the global voice of
the legal profession®

International Bar Association
Banking & Financial Law Committee

Fintech: how is the world shaping the financial innovation industry? (2024)

The International Bar Association (IBA), established in 1947, is the world's leading international organisation of legal practitioners, bar associations, law societies, law firms and in-house legal teams. The IBA influences the development of international law reform and shapes the future of the legal profession throughout the world. It has a membership of more than 80,000 lawyers, 190 bar associations and law societies and 200 group member law firms, spanning over 170 countries. The IBA is headquartered in London, with offices in São Paulo, Seoul, The Hague and Washington, DC.

International Bar Association

Chancery House

53–64 Chancery Lane

London WC2A 1QS

United Kingdom

www.ibanet.org

Table of contents

1. Africa 9

Egypt 10

Ghana 17

Kenya 22

Mauritius 29

Nigeria 34

South Africa 43

2. Asia Pacific 48

Australia 49

China 59

Hong Kong 68

India 80

Indonesia 88

Japan 95

Malaysia 102

New Zealand 110

Singapore 125

South Korea 133

Taiwan 141

3. Central America 148

Costa Rica 149

El Salvador 153

Guatemala 157

Honduras 160

Mexico 164

Nicaragua 171

Panama 174

4. Europe 177

Austria 178

Belgium 183

Denmark 190

Finland 193

France 202

Germany 210

Greece 214

Ireland 219

Italy 227

Lithuania 236

Luxembourg 244

Malta 252

The Netherlands 260

Norway 265

Poland 273

Portugal 281

Spain 293

Sweden 298

Switzerland 302

United Kingdom 308

5. Middle East 312

Iran 313

United Arab Emirates 319

6. North America 329

Canada 330

United States 336

7. South America 343

Argentina 344

Bolivia 353

Brazil 357

Chile 364

Colombia 372

Ecuador 382

Guyana 390

Paraguay 393

Peru 396

Uruguay 401

Venezuela 405

Introduction

In recent years, financial technology (fintech) has rapidly expanded worldwide, forcing traditional financial institutions to evolve in response to this innovative manner of conducting business in the financial industry. Today, we continue to witness the significant impact of fintech on global markets, as it reshapes the financial landscape. Looking ahead, the evolution of fintech promises to further challenge and transform existing frameworks, requiring continuous adaptation and regulatory foresight.

In 2023, the IBA Banking & Financial Law Committee launched an extensive research project aimed at dissecting and understanding the diverse legal frameworks that govern fintech around the globe. This original study covered 39 countries, providing a comprehensive overview of how different jurisdictions are navigating the complexities of fintech regulation.

Through this new edition, the project has been extended to 61 countries across different regions: Africa, Asia-Pacific, Central America, Europe, Latin America and North America. The project contains analysis of how different countries regulate fintech companies and looks at the existence of specific legal frameworks applicable to crypto assets. It also assesses how different jurisdictions around the globe regulate payment service providers and digital wallets and features an overview of special programmes supporting fintech ecosystems. Lastly, the report covers how jurisdictions regulate and deal with matters relating to open banking.

The report has been coordinated by Carlos M Melhem, Treasurer of the IBA Banking & Financial Law Committee and a partner at Allende & Brea in Buenos Aires; Matias Langevin, Young Lawyers' Committee Liaison Officer of the IBA Banking & Financial Law Committee and a partner at HD Legal in Santiago; Lukasz Szgeda, Academic Liaison Officer of the IBA Banking & Financial Law Committee and a partner at Wardynski & Partners in Warsaw; and Rafael Aguilera, Real Estate Section Liaison Officer of the IBA Banking & Financial Law Committee and a partner at Gómez-Acebo & Pombo in Madrid.

Africa

Egypt

Dania El Samad*
Zulficar & Partners, Cairo
drs@zulficarpartners.com

Reem Abu Zahra†
Zulficar & Partners, Cairo
raz@zulficarpartners.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

Financial technology[1] (fintech) was not regulated in Egypt until the issuance of Banking Law No 194 for 2020 (Banking Law). The Banking Law introduced new provisions regulating financial technology in the banking sector which includes electronic payment (e-payment) services, Payment System Operators (PSOs), Payment Service Providers (PSPs) and Systematically Important Payment Systems (SIPS) which are all subject to the regulation and supervision of the Central Bank of Egypt (CBE) as well as any use by any of the banks or companies subject to the Banking Law. Companies conducting these activities must be licensed by the CBE.

This legislative development was furthered by the issuance of Law No 5 for 2022 on the use of financial technology in the conduct of non-banking financial services (NBFS) for the first time in Egypt (the Fintech Law). The Fintech Law puts forward a legal framework with the purpose of facilitating the integration of technology in the conduct of NBFS. The Fintech Law covers services/applications such as roboadvisory,[2] insurtech,[3] artificial intelligence, mobile applications and digital platforms used to provide microfinance, nanofinance and consumer finance.

The conduct of financial services through the use of technology requires prior approval from the Financial Regulatory Authority (FRA). Other applications/services may be authorised provided said applications/services:

---

* Dania is a Partner at Zulficar & Partners. She has been building up her banking and project finance experience since 2007. She specialises in banking and project finance and has experience in acting for government and corporate entities, lenders, borrowers and multinational clients. Dania has worked on a broad range of transactions relating to the development, acquisition, disposal and financing of infrastructure projects. She has over 14 years of experience in Egypt and is recognised as an expert on banking and finance transactions including drafting and negotiating finance documents, loan agreements and security documents, such as pledges, mortgages and corporate guarantees. She has also assisted in major project finance and syndicated lending transactions on behalf of leading real estate developing companies, banking and financial institutions and other local and international clients and has recently acted on behalf of project companies in renewable energy projects under the FiT program and related project financing.

† Reem is a senior associate in Zulficar & Partners' Corporate and Capital Markets Departments. She specialises in providing advice with respect to corporate and commercial legal matters with a special focus on capital market law and Egyptian Exchange (EGX) regulations with extensive experience in initial public offerings (IPOs). She handles general corporate matters, especially corporate governance and compliance for closed as well as public companies listed on EGX. She regularly provides legal advice on a broad range of capital market transactions and topics such as the establishment, licensing and governance of financial companies, investment funds, investigations and inspection by the Financial Regulatory Authority (FRA) inducing insider trading cases, securitisation and MTOs.

1 Means any tools or mechanisms utilising modern and innovative technology in the non-banking financial sector to support and facilitate financial, financing and insurance activities and services using applications, software, digital platforms, artificial intelligence or electronic registers.

2 An innovative system used by licensed entities operating non-banking financial activities to analyse clients' data, financial situations, future objectives and plans to provide them with technical advice through the utilisation of the artificial intelligence platforms.

3 Insurance technology.

- are suitable for the nature of the financial activity in question;
- maintain the necessary software for the protection of personal data from hacking and cyberattacks; and
- comply with the rules issued by the FRA in connection with the verification of digital identity[4] and digital contracts[5] used in non-banking financial activities and anti-money laundering regulations.[6]

Before the promulgation of both laws, some companies informally provided both banking and non-banking financial services through the use of technology (or in line with the CBE circulars issued regularly for banks operating in Egypt). After the issuance of both laws, entities, whether those operating in Egypt or abroad, became expressly prohibited from rendering fintech services to individuals residing in Egypt without obtaining the proper licence from either the CBE and the FRA.

The CBE Board of Directors (BoD) has not yet issued rules in relation to e-payment services. The CBE issued certain circulars and directives regulating electronic payment services (eg, regulations on technical payment aggregators and payment facilitators, payment via mobile phones, payment using QR codes, etc). However, such regulations were addressed to the banks wishing to collaborate with or to benefit from the services of these e-payment service providers. Accordingly, the banks are the ones under the obligation to obtain licences from the CBE to collaborate with e-payment service providers.

In July 2023, the FRA issued three decrees which together regulate the fintech ecosystem governing NBFS companies. Decree No 139 of 2023 describes the basic standards of the technological infrastructure financial companies must meet to conduct financial services through the use of technology, including IT risk and cyber security, as well as basic IT governance requirements. Decree No 140 of 2023 tackles digital identification, digital contracts and e-KYC (know your customer) requirements, and Decree No 141 of 2023 regulates the outsourcing of IT services by NBFS companies and the rules governing the relationship between the financial company and the IT third party. The FRA has verbally advised that it is in the process of issuing further circulars and regulations to cover specific areas and topics.

With respect to e-payment services, the Banking Law provides companies with a grace period of one year (renewable for a maximum of two years) to comply with the licensing rules and obtain the licence; however, the CBE has not yet issued these detailed licensing rules. With respect to NBFS, since the issuance of Decrees No 139,140 and 141 explained above, the FRA has been initiating discussions, preparing workshops and individual meetings with companies to educate them about the new requirements for companies.

The Banking Law regulates e-payment companies in terms of their ownership structure, general conditions for licensing, change of control, violations, and penalties.

---

4 The technically analysed data related to a specific natural or legal person, which is directly or indirectly defined through linking such data with other data such as name, voice, picture, identified numbers and identity, allows the authentication of transactions operated through a digital platform.

5 The contract electronically created to include parties' rights and obligations, and which can be registered in a digital register. This digital contract can also be a 'smart contract' that utilises applications (lines of code) to create a self/auto-execution contract, with auto-control or authentication of its provisions.

6 Article 8, Fintech Law.

Regarding NBFS companies using financial technology, to obtain a licence[7] in accordance with the requirements determined by the FRA BoD, the applicants should meet a number of conditions, including:

- having their activities limited to only the licensed activity;
- disclosing in detail their direct and indirect ownership structure as well as their related parties; and
- having the equipment, technical infrastructure, information systems and means of protection and insurance necessary for carrying out the activity.

Other than the FRA licence, non-banking financial institutions already licensed with the FRA may carry out fintech activities either directly or through an outsourcing agreement with entities registered with the FRA, provided the prior conditional approval of the FRA is obtained.[8]

The CBE in March of 2023 issued new regulations regarding payment card tokenisation on electronic devices applications. Such regulations are intended to effectively pave the way towards a cash-free society by facilitating access to banking services. The CBE Circular applies to all banks operating in Egypt and token service providers licensed by the CBE, and effectively allows for the facilitation of contactless payments utilising tokens formulated through applications on electronic devices, including applications such as Apple Pay and Google Pay.

Tokenisation – ie, the substitution of card details with a unique randomly generated code – entails the circulation of sensitive and confidential data, which is why the CBE has required that appropriate data protection methods and outsourced security services be utilised. Issuer banks must obtain a licence from the CBE for each application whereby tokenisation occurs separately, and in order to obtain such approval must submit, amongst other information, details on the infrastructure of the system to be utilised for tokenisation and a comprehensive three-year business plan of the process.

Furthermore, the CBE has issued in July 2023 the licensing and registration requirements of digital banking. Like non-digital banks, digital banks are required to take the form of either an Egyptian joint-stock company or a branch of a foreign bank. Unlike non-digital banks, however, digital banks are prohibited from providing credit facilities to large companies except under certain conditions. Additionally, digital banks may provide their services via banking agents approved by the CBE.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

The CBE emphasises the importance of adhering to Article (206) of the Banking Law. This article prohibits the establishment or operation of any platforms to issue, trade in or market digital currency or cryptocurrency without the prior CBE approval in accordance with the rules to be issued by the CBE BoD.[9]

The CBE has also issued, and continues to issue, many press releases reiterating its warning against trading in all kinds of cryptocurrencies, mainly Bitcoin, due to the extremely high risk associated

7 Article 4, Fintech Law.

8 Article 5, Fintech Law.

9 Article 206, Banking Law.

with such currencies. Cryptocurrencies are typically characterised by fluctuations and significant price volatility as global speculation is completely unregulated – a fact that makes investments in any of them quite risky and highly speculative, and likely to lead to sudden losses of their whole value.

In the same context, the CBE asserts that trading within the Arab Republic of Egypt is only confined to the official currencies approved by the CBE. In this regard, the CBE calls on all traders in the Egyptian market to use extreme caution and not to engage in any trading in these high-risk currencies.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

Please see Question 1.

The conditions and procedures that PSOs and PSPs must abide by in order to obtain a licence are determined by the CBE BoD; however, as mentioned above, while the Banking Law includes some general principles, the detailed rules have not yet been not issued.

The CBE BoD should issue rules specifying the requirements for the licence applicants, such as:

- minimum capital;
- legal form;
- requirements for technical efficiency;
- financial solvency;
- good reputation;
- disclosure of the ownership structure;
- the technology used;
- quality measures of service provision;
- the rules necessary for operation; and
- fees for examining the licence application.[10]

While the licensing requirements have not yet been issued, the Banking Law stipulates that the PSP or PSO licences may be revoked and the company conducting such activities may be deregistered by virtue of a decision of the BoD of the CBE, if the PSO or PSP:

- commits a gross or recurrent breach of the provisions of the Banking Law or CBE directives and does not remedy such breach within the period and subject to the conditions set forth by the CBE;
- applies a policy that may harm the public economic interest, the monetary policy, or the banking system;
- ceases to practise its activity or submits a request for voluntary liquidation;

10 Article 185, Banking Law.

- becomes financially distressed, and the CBE believes it is not possible to reconcile its position and decides to liquidate it;
- submitted false information to the CBE in order to obtain the CBE licence;
- loses any of the licensing conditions; and
- if a material change occurs to the information based on which the licence was provided.

PSPs and PSOs are required to report any change in the company's information to the CBE; failure to do so is sanctioned by law. The Banking Law also regulates the ownership of PSPs and PSOs and any change in control must be pre-approved before any acquisitions.

Neither PSPs nor PSOs may appoint any of its key managers without obtaining CBE prior approval to ensure that they meet the technical qualification requirements as per the rules set by the CBE. 'Key managers' means the chair and members of the boards of directors, and executive managers who are responsible for the main and supervisory activities determined by a decision of the BoD of the CBE.

The BoD of the CBE has the power to set out necessary rules regulating the supervision and control over the PSPs and the PSOs, and to impose specific standards and rules for such purposes, including:

- the interoperability of the payment systems rules;
- specifications and requirements of the organisational structure, corporate governance procedure and risk management;
- office oversight and field inspection requirements;
- the mechanism for issuing the service performance standards and key performance indicators;
- the rules for protecting the customers' monies;
- disclosure and transparency requirements; and
- the pricing rules for services provided.

PSOs or PSPs are required to provide the CBE with all information or data requested by the CBE and respond to clarifications by the CBE about their operations. The CBE also has the right to inspect and review the records, accounts, meeting minutes of the board of directors and all committees, and the automated systems and electronic media of these companies and their subsidiaries to ensure that they all meet their objectives. The CBE is also entitled to request necessary information from the principal shareholders to ensure they continuously meet the conditions for approval as principal shareholders.

Refraining from providing the CBE with the required information, documents and records would result in the PSO or the PSP being subject to a fine not less than EGP 200,000 and not exceeding EGP 500,000. In all cases, the CBE will be eventually allowed to inspect the company's records and documents.

Such inspections are carried out at the headquarters of the PSP or PSO, its branches and subsidiaries by the CBE inspectors and their assistants who are delegated by the Governor of CBE for this purpose. The CBE's inspectors may obtain copies of any documents necessary to achieve the purposes of such inspections.

As part of its supervisory role, the BoD of the CBE is entitled to take necessary decisions to freeze, cancel, limit, amend or add any of the activities and transactions carried out by the PSOs or PSPs for the purpose of protecting banking stability and customers' rights. It also has the right to take all steps required to settle transactions preceding such decisions.

PSPs may appoint agents to carry out their licensed activities in accordance with the regulations, conditions and procedures to be determined by the BoD of CBE. These agents shall be registered in a special registry at the CBE, and the PSP shall remain liable for all the activities undertaken by such agent(s) on its behalf. The PSPs must ensure that the agent is in compliance with all the applicable laws and regulations related to the payment service activity.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

There are programmes that support fintech in Egypt. In May 2019,[11] before the issuance of the current Banking Law, the CBE launched a regulatory sandbox for the purpose of providing fintech players with a virtual space within which, subject to a specific framework, applicants can experiment with their solutions for a limited period of time on a small scale under well-defined parameters.

Applicants wishing to join the regulatory sandbox must fill in the regulatory sandbox online application form, accessed via the CBE's official website.

Applicants will qualify to enter the regulatory sandbox if the innovative product, service or solution they provide is within the scope of fintech services and is 'genuinely innovative' with a 'clear potential to improve accessibility and efficiency in providing financial services'.

The CBE believes in keeping up with rapid developments in financial technology and striving to achieve an optimal balance between ensuring financial stability and consumer protection while furthering innovation to serve the banking and financial sector in Egypt. To this end, the regulatory sandbox will work as a live testing ground for fintechs which are developing new business models that are currently hindered by stringent authorisation requirements.

The purpose of the regulatory sandbox is to pave the way for faster and easier access to new financial solutions and embed compliance within the fintech ecosystem at an early stage. This will not only allow fintech innovators to focus on their core offering, but also ensure that consumers and other players in the market are not adversely affected by the regulatory uncertainty of the disruptive fintech activities.

Following the issuance of the Banking Law, and consistent with best practices, the CBE is empowered to take the necessary measures to enhance and develop the use of modern technology or financial innovation and banking services or supervision of licensed entities, particularly establishing an ecosystem for testing and supervision of financial and supervisory technology applications.

11 CBE circular dated May 2019.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

Currently, there are no specific laws for open banking in Egypt. However, the CBE recently introduced a set of regulations regarding open banking which govern the instant payments network (IPN) services in Egypt. These new regulations allow people to make electronic payments between bank accounts using their mobile phones via application programming interfaces (APIs). Accordingly, a licence must be obtained from the CBE by banks wishing to provide such services.

In October 2021, the CBE issued the procedures for obtaining such a licence, as well as the general rules regulating banks participating in the IPN. The CBE reserves the right to amend the maximum limits of the transaction values made by banks participating in the IPN and has in fact increased the 2021 limits by virtue of a CBE Circular in March of 2023.

A bank must not launch the service with technical payment aggregators and payment facilitators before furnishing CBE with a penetration test report on the actual work productions, including but not limited to the following:

- merchant plugins;
- software development kits (SDK); and
- application programming interfaces.

This would indicate that there are no weak points with high- or medium-level risks, based on which the CBE approval would be granted to activate the service – provided that the report would be submitted within three months at most as of the issuance of the approval. It is essential to take these tests regularly, and to provide the bank with the penetration test report which is conditional for licence renewal.[12]

12 CBE circular, dated 2019.

Ghana

Rachel Dagadu*
ENSafrica, Accra
rdagadu@ENSafrica.com

Mandy Ofori Sarpong†
ENSafrica, Accra
msarpong@ENSafrica.com

1. Fintech regulatory framework: please provide a description of the most relevant laws and regulations on fintech and financial innovation in your country. Please also refer to any new law or regulation foreseen in the near future or any bill on fintech and financial innovation in your jurisdiction.

The Bank of Ghana (BOG) is the primary institution responsible for regulating fintech business in Ghana. BOG is mandated to grant licences and authorisation to banking and non-banking institutions that offer financial solutions using technology, including payment system services and electronic money issuers. The main laws that regulate fintech in Ghana are as follows:

- *Payment Systems and Services Act, 2019 (Act 987)*: the Payment Systems and Services Act is the main regulatory framework for fintech in Ghana. It sets out the licensing requirements for the payment systems and payment service providers including a minimum of 30 per cent Ghanaian equity participation and minimum capital requirements ranging from GHS800,000 to GHS20m (approximately US$70,000 to US$1.8m) dependent on the licence type.

  A licence is valid for five years and subject to renewal. A fintech company that operates without a licence is liable to a fine ranging from GHS30,000 to GHS84,000 (approximately US$2,600 to US$7,300).

  Payment system providers are required to have a minimum of three directors, two of whom (including the chief executive officer) must be resident in Ghana. The Act also provides for minimum customer due diligence requirements. In addition, fintech companies are required to retain records for a minimum of six years from date of creation of record.

  The constitution of fintech companies should clearly state their respective activity: eg, payment service provider or dedicated electronic money issuer. The constitution of electronic money issuers should include a provision that electronic money owed to customers are held in trust and shall not be encumbered in case of insolvency or liquidation. Electronic money issuers are required to keep 100% of the electronic money float in liquid assets.

- *Electronic Transactions Act, 2008 (Act 772)*: this Act regulates all types of electronic transactions including the activities of fintech companies. The Act prohibits fintech companies from sharing

* Rachel is a partner at ENSafrica in Ghana. She specialises in project finance, banking and finance, capital markets, corporate commercial, M&A, real estate law, mining, oil and gas, and energy and petroleum law.
† Mandy is an associate at ENSafrica in Ghana. Mandy specialises in project finance, banking and finance, tax, energy and petroleum law.

or selling addresses and account numbers of customers without their consent and sending unsolicited electronic communications to a customer without consent. Further, electronic commercial communication sent to a customer must provide the customer with the option to unsubscribe from the mailing list.

For purposes of facilitating proof of authenticity, fintech companies using digital signatures must ensure that: (1) the means of creating the signature is linked to the signatory and not the other party; (2) the means of creating the digital signature is, at the time of signing, under the control of the signatory and not another person without duress or undue influence; and (3) an alteration to the signature after signing is detectable.

- *Electronic Transfer Levy Act, 2022 (Act 1075) as amended by the Electronic Transfer Levy (Amendment) Act, 2022 (Act 1089)*: this Act imposes a 1 per cent electronic transfer levy on electronic transfers above GHS100 (approximately US$9) on a daily basis. Fintech companies are required to charge the levy at the time of transfer and pay the amount charged to the Commissioner-General of the Ghana Revenue Authority (GRA) within 24 hours. Fintech companies are also required to file returns with the Commissioner-General of GRA in respect of the electronic transfer levy. Transactions which are exempt from the imposition of the levy include a transfer for the payment of taxes, fees and charges on any government designated payment system, as well as transfers between accounts owned by the same person or entity.
- *Data Protection Act, 2012 (Act 843)*: fintech companies are required to register with the Data Protection Commission to process the personal data of their customers. Failure to register constitutes an offence and the company will be liable to pay a fine of up to GHS3,000 (approximately US$260).

  In Ghana, the processing of a customer's personal data must be necessary for the purpose of a contract, authorised by law, protect a legitimate interest, necessary for the proper performance of a statutory duty or to pursue the legitimate interest of the company or third party to whom data is supplied. Customers' data cannot be sold or shared without their consent except in relation to credit bureaux, where such data relates to details of a loan which is past due by over 90 days or information on a person involved in financial malpractices.
- *Anti-Money Laundering Act, 2020 (Act 1044)*: under this Act, fintech companies are required to formulate and implement policies to prevent money laundering, the financing of terrorism or the proliferation of weapons of mass destruction, tax evasion or commission of any other unlawful activity, and keep records of customers and transactions. Fintech companies are required to appoint an anti-money laundering reporting officer responsible for liaising with BOG and the Financial Intelligence Centre in filing suspicious transaction reports and in ensuring compliance with the Act and internal policies.

  The Act mandates fintech companies to verify customers' identities through customer due diligence and know your customer (KYC) measures. Fintech companies are also required to (1) put in measures to identify politically exposed persons by exercising enhanced identification, verification and customer due diligence procedures; and (2) take note of and report to the Financial Intelligence Centre within 24 hours all complex, unusually large transactions or an unusual pattern of transactions which do not have an apparent or visible economic or lawful

purpose, and business relationships or transactions with persons or financial businesses, from or in countries which do not sufficiently apply the Financial Action Task Force Recommendations.

- *BOG Guidelines and Notices*: BOG intermittently issues notices and guidelines to govern fintech companies. Guidelines and notices have been introduced in relation to inward remittance payments, crowdfunding and consumer dispute resolution mechanisms, amongst others.

2. Regulations on crypto assets: please provide a summary of the legal framework of crypto assets in your country and how crypto assets are regulated in your jurisdiction.

Cryptocurrency is not recognised under the laws of Ghana. In 2018, BOG issued a notice stating that activities in digital currency remain unlicensed. The Payment Systems and Services Act, which was passed in 2019, does not regulate dealings in crypto assets.

In 2019, the Securities and Exchange Commission issued a notice which stated emphatically that cryptocurrencies are not recognised as currency or legal tender in Ghana. The Commission also stated that it does not regulate crypto assets and their accompanying online trading platforms.

Recently in April 2022, BOG issued cautionary directives to banks and other financial entities in its dealings in cryptocurrency trade and other unregulated investment schemes. The general public was advised to be cautious with regards to trading in cryptocurrencies and other unregulated investment schemes. The Bank further cautioned all regulated institutions, including banks, specialised deposit-taking institutions, dedicated electronic money issuers and payment service providers, to desist from facilitating cryptocurrency transactions and unlicensed investment schemes through their platforms or agent outlets.

However, the Anti-Money Laundering Act enacted in 2020 lists virtual asset service providers as part of accountable institutions. Virtual asset service providers are defined to include persons who engage in the business of exchange, transfer and safekeeping and administration of virtual assets (crypto assets). Thus, crypto assets are subject to the Anti-Money Laundering Act.

3. Payment service providers and digital wallets: please describe how payment service providers and/or digital wallets are regulated in your country. Please mention any foreseen law or regulation in this respect.

The Payment Systems and Services Act is the main regulatory framework for payment service providers (PSPs) and digital wallets. It provides the requirements that need to be met by PSPs and electronic money issuers. The Act provides that no company shall operate a payment system without a PSP licence from BOG. There are currently six categories of PSP licences issued by BOG. These are:

- *Dedicated Electronic Money Issuer Licence*: This license allows a PSP to engage in the issuance of electronic money, the recruitment and management of agents and the creation and management of digital wallets. It also allows the licence holder to engage in wallet-based domestic money transfers, including transfers to and from bank accounts, cash-in and cash-out transactions, investments and savings (in partnership with banks and duly regulated financial institutions).

- *PSP Scheme Licence*: This licence allows a PSP to engage in switching and routing payment transactions and instructions.
- *PSP Standard Licence*: This licence allows a PSP to set up mobile payment applications and solutions for credit, savings and investment products. This is reserved for Ghanaians and wholly owned Ghanaian entities.
- *PSP Medium Licence*: This licence allows a PSP to perform all activities of a standard licence holder. It also permits a PSP to engage in payment aggregation which is connected to an enhanced PSP. In addition, it allows a PSP to engage in the training and support of merchants, printing of non-cash payment instruments and development of market platforms.
- *PSP Enhanced Licence*: This licence allows a PSP to perform all activities of a medium licence holder. It also allows a PSP to engage in the aggregation of merchant and processing services, the provision of hardware and software and the printing and personalisation of Europay, Mastercard and Visa (EMV) cards. It also allows the PSP to provide inward or international remittances services, merchant acquiring, point of sale (POS) deployment and payment aggregation.
- *Payment and Financial Technology Service Provider*: This licence allows a PSP to engage in digital product development, delivery and support services, credit scoring predictive analysis and fraud management services.

PSPs are regulated by the laws discussed in paragraph 1. In addition to these laws, where a PSP has foreign shareholders, the PSP must register with the Ghana Investment Promotion Centre and meet at least 10 per cent Ghanaian equity participation. PSPs also have reporting obligations to BOG and are required to submit reports on liquidity, financial exposure, expenditure, assets, income, liabilities, affairs and any other matter that BOG may require.

4. Special Support to fintechs: does your jurisdiction provide any special programme supporting fintech ecosystems, in particular fintech startups (eg regulatory sandboxes, accelerator programmes). Are such programmes supported by the regulator in your country?

On 19 August 2022, BOG launched a regulatory and innovation sandbox developed in collaboration with EMTECH Service LLC. The regulatory and innovative sandbox seeks to encourage fintech initiatives by allowing startups to conduct live experiments under regulatory supervision prior to launching a product or service on the market. To be eligible, innovations must satisfy one of the following categories:

- new digital business models not currently covered explicitly or implicitly, under any regulation;
- new and immature digital financial service technology; and
- innovative digital financial services products that have the potential of addressing a persistent financial inclusion challenge.

The regulatory and innovative sandbox excludes solutions that do not provide additional or material value to existing payment and financial service solutions, and for which regulatory status can be determined without live testing in the marketplace.

It is open to all licensed financial institutions including payment service providers and dedicated electronic money issuers. To benefit from the regulatory sandbox, the applicant must complete and submit an application online to BOG (at no fee) detailing the nature of the innovative product, service or business model, its readiness to be tested and an exit plan. After assessment, a successful applicant is issued with a letter of approval permitting testing for typically six months, subject to extension. Testing is monitored and evaluated periodically by the sandbox technical team and the applicant exits the sandbox after submission of a final testing report.

To facilitate testing, BOG may issue restricted authorisation exclusive to the sandbox entity, waive or modify an unduly difficult rule or issue a 'no enforcement action letter' where there is uncertainty as to which regulatory requirements could be breached during the testing. Foreign companies must incorporate a subsidiary in Ghana and satisfy the 30 per cent Ghanaian equity requirement to be eligible to participate in the regulatory sandbox.

The BOG opened the regulatory and innovative sandbox from 13 February 2023 to 14 March 2023 to admit the first cohort of participants. The first cohort window largely accepted innovations from certain priority areas including payments, remittances, crowdfunding and micro-lending.

5. Open banking: please advise whether in your jurisdiction there are regulations on open banking. If the response is no, please provide any reference to regulations that may directly or indirectly affect open banking. Please include any foreseen laws and regulations on open banking.

There are no specific regulations for open banking in Ghana. However, the National Payment Systems Strategic Plan includes an open banking policy and BOG is set to develop guidelines for open banking by the end of 2023.

Currently, fintech companies and financial institutions have individual IT systems and software for clients' data and financial records. Each institution has its own procedures for data sharing and granting access to other institutions in accordance with the law.

The Data Protection Act provides that a person who processes personal data should ensure that the personal data is processed without infringing the privacy rights of the data subject including sharing data without consent. Personal data should also be processed in a lawful and reasonable manner. The Cybersecurity Act 2020 (Act 1,038), also requires owners of critical information infrastructure to report any incident of cybersecurity to the relevant sectorial computer emergency response team or to the National Computer Emergency Response Team within 24 hours.

The Payment Systems and Services Act encourages PSPs to have a system capable of interoperating with other payment systems under the Act. PSPs are required to put in place appropriate security policies and measures, intended to safeguard the authenticity and confidentiality of data and operating processes that are shared with third parties. The Act also enjoins PSPs to desist from engaging in any act which would result in systemic risk or affect the integrity, effectiveness or security of their respective payment systems.

Kenya

Belinda Ongong'a[1]
ENS, Nairobi
bongonga@ENSafrica.com

Duane Wekesa[2]
ENS, Nairobi
dwekesa@ENSafrica.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

In Kenya, there are no specific regulations for fintech. However, there are various statutes and regulations that directly or indirectly apply to fintech and innovation in the financial services sector. The most relevant of these laws and regulations are set out below.

Central Bank of Kenya Act, Cap 491 (CBK Act)

The CBK Act establishes the Central Bank of Kenya (CBK), whose responsibility includes formulating financial policies and regulating the provision of financial services. The CBK licenses and supervises banks, financial institutions, foreign exchange dealers, payment service providers (PSPs), money remittance operators (MROs) and digital credit providers (DCPs).

Additionally, under section 4A of the CBK Act, the CBK has the power to authorise the use of new financial models to operate in the absence of a governing framework or regulation. In these instances, the CBK may issue a letter of no objection to any entity seeking to provide financial services including fintech where there is no regulatory framework. The CBK also has in place various guidelines and policies including on corporate governance, consumer protection and cybersecurity that aim to provide guidance to sector players.

National Payment System Act, No 39 of 2011 (NPS Act) and National Payment System Regulations (NPS Regulations)

The NPS Act defines the services offered by a PSP to include:

- sending, receiving, storing or processing of payments, or the provision of other services in relation to payment services through any electronic system;
- possessing, operating, managing or controlling a public switched network for the provision of payment services; or
- the processing or storing of data on behalf of such PSPs or users of such payment services.

1 Belinda is a senior associate at ENS Kenya with seven years' experience. She specialises in corporate commercial, M&A, TMT, fintech and has also taken a keen interest in project finance, energy, and infrastructure.

2 Duane is a junior associate at ENS Kenya specialising in corporate and commercial law, M&A, fintech, TMT and data protection.

The NPS Regulations set out the application fees and the licensing/authorisation procedures that must be followed by any person intending to offer payment services in Kenya. The NPS Regulations provide that in addition to getting a CBK authorisation, a mobile PSP must obtain a licence from the Communications Authority of Kenya (CA).

The NPS Act and the NPS Regulations prohibit the conduct of business as a PSP without CBK authorisation. Failure to have the requisite authorisation is an offence attracting penalties of up to KES 500,000 or imprisonment for up to three years, or both. The NPS Regulations allows a PSP to appoint agents whose responsibility includes sending, receiving, and processing payments.

Money Remittance Regulations 2013 (MR Regulations)

The MR Regulations provide for the licensing and regulation of MROs. An authorised MRO is allowed to deal in inbound and outbound international money transfer transactions. Once authorised as an MRO, an MRO is required not to engage in any other business other than what is authorised by the CBK. The MR Regulations exempt banks and microfinance institutions from applying for and obtaining an MRO licence.

In terms of forex inflows and outflows, the CBK requires that MROs ensure that these must be done through bank accounts: therefore, there are no wallet-to-wallet remittances. A person who provides money remittance services in Kenya without a licence commits an offence, and on conviction is liable to a fine not exceeding KES 500,000 or to imprisonment for a term not exceeding three years, or both.

CBK Digital Credit Providers Regulations 2022 (the Regulations)

The CBK (Amendment) Act 2021 (Amendment Act) and the Regulations operationalise the licensing of digital credit providers (DCPs). Engaging in digital credit business without a licence constitutes an offence under the CBK Act and the Regulations. Under the CBK Act, a person operating without a licence is liable on conviction to imprisonment for a term not exceeding three years, to a fine not exceeding KES 5m or both.

The Regulations define 'digital credit business' to mean the business of providing credit facilities or loan services through a digital channel, while 'digital channels' include (1) the internet, (2) mobile devices, (3) computer devices, (4) applications and any other digital systems as may be prescribed by the CBK. DCPs are allowed to engage in digital credit business and may not undertake deposit-taking business or take cash collateral for loans. The Regulations provide that any investment in a licensed DCP requires prior approval of or notification to the CBK.

Capital Markets Act, Cap 485A (the Act)

The Act establishes the Capital Markets Authority (CMA), whose role includes regulating public offering of securities. The Act defines the term 'security' and identifies various securities including (1) debt instruments, (2) depository receipts, (3) shares, (4) futures relating to assets or property and (5) asset-backed securities and any other security defined by the CMA under the Act.

In a decision issued by the High Court of Kenya (High Court) (*re Wiseman Talent Ventures vs the CMA*) the High Court held that the CMA has the residual jurisdiction to regulate cryptocurrencies in Kenya, and the absence of a specific regime does not ouster the jurisdiction of the CMA to regulate cryptocurrencies and associated financial products. The High Court also directed the CMA to designate cryptocurrencies as securities; however no such designation has been provided as at the date of this survey.

The CMA has issued various warnings to the public, especially touching on initial coin offerings and cryptocurrency transactions which lack regulatory sanctions. The CMA in March 2019 published the Regulatory Sandbox Policy Guidance Note ('Sandbox Policy') to allow for testing of innovative products, solutions and services including fintech products. The Sandbox Review Committee (SRC) has a mandate to provide regulatory support and review, consider sandbox applications and to implement test plans to allow sandbox entrants to transition to licensing categories. The Sandbox Policy is only applicable to servicing fintechs and financial services that are directly within the regulatory parameters of the CMA.

Capital Markets (Investment-Based Crowdfunding) Regulations 2022 (Crowdfunding Regulations)

Under the Crowdfunding Regulations, the establishment, maintenance, or operation of an investment-based crowdfunding platform requires a licence from the CMA. The Crowdfunding Regulations extend to platforms within Kenya, those targeting Kenyan investors from abroad, or those with key components physically located in Kenya.

Operating such a platform without a licence is considered an offence, with potential penalties including fines up to KES 5m or imprisonment for two years, along with restitution. Unlicensed crowdfunding platforms face even higher penalties, up to KES 10m and restitution. Micro, small and medium enterprises meeting certain criteria, including a minimum two-year operating track record and good corporate governance, can raise funds up to KES 100m within a 12-month period through licensed crowdfunding platforms. These platforms can apply to the CMA for approval to exceed this limit. Eligible investors, including sophisticated and retail investors, are subject to investment limits set by crowdfunding operators, with a cap at KES 100,000 for retail investors.

Capital Markets (Online Foreign Exchange Trading) Regulations 2017 (Online Trading Regulations)

Under the Online Trading Regulations, a person shall not carry on a business as a dealing online foreign exchange broker, non-dealing online foreign exchange broker or a money manager unless that person is licensed by the CMA. Online foreign exchange trading means internet-based trading of foreign exchange and includes trading in contracts for difference based on a foreign underlying asset. In this regard, the CMA issued warnings to Kenyans against engaging in online foreign exchange trading through unlicensed entities, as they risk losing their investments and may not be protected by law.

Kenya Information and Communications Act, Cap 411A (KICA)

KICA establishes the Communications Authority of Kenya (CA), which regulates the information, communications, media and broadcasting industries, including e-commerce, in Kenya. The CA has a licensing framework that is technology neutral. The CA may license a fintech where its operating model incorporates a technological aspect, and the implementation of the innovation requires the fintech to establish its own telecommunications infrastructure or results in content creation. In such cases, the CA issues an approval or licence, a letter of no objection, or a confirmation that an entity does not require a telecommunications licence. Mobile money service providers (MMSPs) and mobile virtual network operators (MVNOs) usually fall under the regulatory ambit of the CA.

The various regulators, including the CBK and CMA, also rely on other laws and regulations that have an impact either directly or indirectly to fintech companies. These include (1) data protection laws, (2) anti-money laundering laws, (3) consumer protection laws, (4) cybersecurity laws, (5) competition laws and (6) access to information laws.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

Cryptocurrencies, including any form of crypto assets and stablecoins, are not regulated in Kenya. Some regulators, including the CBK and the CMA, have expressed concerns about cryptocurrencies. These concerns are discussed below in detail.

CBK

The CBK does not issue any licence to operate any payment or remittance business that utilises cryptocurrencies and similar products. The CBK has further stated that cryptocurrencies are not regulated and are not considered legal tender in Kenya. Despite Kenyans having interest in cryptocurrencies, the CBK has issued various notices to the public warning against the use of virtual currencies. The notice issued by CBK in 2015 stated that cryptocurrencies such as Bitcoin are unregulated digital currencies that are not issued and guaranteed by the government. As such, the CBK recommended that the public should desist from transacting in Bitcoin and similar products.

Furthermore, the CBK issued Banking Circular No 14 of 2015 (Circular) to all chief executives of commercial banks, mortgage finance companies and microfinance banks on virtual currencies such as Bitcoin. The circular informed banks that virtual currencies are a form of unregulated digital currency that are not issued or guaranteed by any government or central bank. As such, the circular sought to caution all financial institutions against dealing or transacting in virtual currencies. It is unclear how the directions contained in the Circular are enforced, especially where Kenyan customers utilise peer-to-peer marketplaces to allow them to buy cryptocurrencies directly from other users, using their preferred payment method and local currencies.

Nonetheless, there has been slight progress on the CBK's view of digital currencies. The CBK, for instance, published a Discussion Paper on Central Bank Digital Currency (CBDC) for public comments. The discussion paper examines the applicability of a potential CBDC in Kenya and

received 119 responses from various stakeholders across nine countries. It is part of CBK's initiatives to ensure informed policy decisions regarding financial innovations.

CMA

The Capital Markets Act defines the term 'security' and identifies some types of securities, such as (1) shares; (2) debt instruments; (3) rights or options relating to other securities; (4) futures relating to assets or property; (5) rights under depositary receipts in respect of other securities; and (6) asset-backed securities. The definition of securities also includes interests, rights or property commonly known as securities. Further, the Capital Markets Act provides that securities include any other instrument prescribed by the CMA to be a security. This allows the CMA to prescribe cryptocurrencies as securities. However, as at the date of this survey, no such designation has been given.

Similar to the CBK's approach, the CMA has issued public warnings stating that it has not issued or approved any initial coin offerings and any crypto-related assets. Currently, there is no licensing regime in existence as both the CBK and the CMA have held that cryptocurrencies are: (1) not a legal tender; (2) not considered as assets; and (3) are not licensed. The CMA has recently announced that it will commence the development of a framework for the regulation of digital currencies and designation of cryptocurrencies as securities. Despite that, there is no indication as to when this planned framework could become law.

As part of the efforts, The Capital Markets (Amendment) Bill 2023 ('Amendment Bill'), seeks to amend the Capital Markets Act to define digital currency. Consequently, cryptocurrencies will be regulated under CMA. The Amendment Bill proposes that, for a licence to be granted for the introduction of a new cryptocurrency product in Kenya, the CMA must be satisfied that the product has undergone product development for not less than two years and that the product was tested on a customer base of not fewer than 10,000 customers. The Amendment Bill is pending parliamentary approval before it comes into effect.

From a tax perspective, the Finance Act 2023 introduced Digital Asset Tax which is applicable on the income derived from the transfer or exchange of digital assets such as cryptocurrencies at a rate of 3 per cent.

That notwithstanding, the financial regulators recently expressed interest in developing guidelines for regulating digital assets. A communique from the 13th Joint Financial Sector Regulators Forum (JFSRF) stated that the regulators agreed to consider the recommendation of the National Treasury and Economic Planning for the formation of a technical working group of concerned regulators to develop recommendations for regulatory framework covering digital assets.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

As discussed in Question 1, PSPs are regulated by the CBK under the framework established by the NPS Act and NPS Regulations. The NPS Act provides for the regulation and supervision of payment systems and PSPs. PSPs must be authorised by the CBK, and any person who provides payment services without a licence is guilty of an offence. The CBK's National Payments Strategy

2022–2025 (CBK NPS Strategy) classifies PSPs to include mobile money providers, payment switches and international money remittance providers/operators. The CBK may authorise a PSP as (1) an electronic retail transfer provider, (2) a small money issuer, (3) an e-money issuer and (4) a designation of payment instrument. The core capital requirement for a PSP is KES 5m and is dependent on the licence applied for.

As discussed in Question 1, if a PSP also offers money remittance services, the PSP must apply for authorisation as an MRO, and the MRO must be registered separately with the CBK. Money remittance business is defined to mean a service for the transmission of money or any representation of monetary value without any payment accounts being created in the name of the payer or the payee, where:

- funds are received from a payer for the sole purpose of transferring a corresponding amount to a payee or to another payment service operator acting on behalf of the payee; or
- funds are received on behalf of and made available to the payee.

The minimum core capital requirement for an MRO is KES 20m.

There are no specific regulations regulating digital wallets. Nevertheless, digital wallets are regulated within the auspices of the NPS Act, NPS Regulations and MR Regulations. Digital wallet services in Kenya are mostly offered through a mobile app or web browser, which allows immediate payments, and/or debit, credit or prepaid card transactions. The CBK requires that PSPs and banks eliminate charges for transfers between mobile money wallets and bank accounts. There is interoperability of mobile wallets and only limited to peer-to-peer payments. As part of the CBK's future commitments, the CBK NPS Strategy intends to ensure that there is full interoperability across mobile wallets, channels, and providers under a unified scheme.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

Startups in Kenya receive a great deal of support both locally and internationally, with many accelerators, incubators and venture capitalists targeting startups in the country. Some key accelerators/incubators that accept fintech startups include the Baobab Network, Growth Africa, Sinapis, NaiLab, iBizAfrica, 88mph and the Catalyst Fund.

The CBK recognises the importance of regulatory support for innovation, and takes an approach labelled the 'test and learn' approach. Under the CBK NPS Strategy, the CBK promises to continue to facilitate this approach with the main objective of building on its legacy of supporting innovation that is consistent with the CBK's policy and regulatory mandate.

The Sandbox Policy discussed in Question 1 offers the CMA the opportunity to accelerate understanding of emerging technologies, support the adoption of an evidence-based approach to regulation, and facilitate deepening and broadening of Kenya's capital markets. Companies and startups are invited to apply to join the sandbox, and if successful, they have a 12-month period to

deploy their product and conduct live testing. Upon exit from the sandbox, they become eligible for grant of an existing applicable licence or grant of permission to operate in Kenya subject to specified terms. The CBK has hinted at the possibility of establishing a similar regulatory sandbox that will explore ways of providing guidance on how players with innovative services can apply for licensing.

The Startup Bill 2022 is undergoing the legislative process in the Kenyan Senate. This Bill aims to create an innovative environment for entrepreneurs. If passed, the Bill proposes to establish the Kenya National Innovation Agency to: (1) create partnerships among local and international business incubators; (2) create online directories of startups and incubators; and (3) register and certify startups and incubators if certain conditions are met. The Bill allows for the establishment of credit guarantee schemes intended to provide accessible financial support and act as a guarantee for investors in startups.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

There are currently no regulations or prescribed requirements for open banking in Kenya, but the CBK has recognised the possibility of moving to open architecture in the CBK NPS Strategy.

The CBK strategy contains provisions relating to development on standards for open but secure application program interfaces (APIs). These standards will include API specifications for:

- identification, verification, and authentication;
- customer account information/data access;
- transaction initiation; and
- formats and coding languages for APIs.

Due to the risk associated with opening up data from financial institutions to third parties, CBK intends to develop clear risk management frameworks and standards, including providing clarity on liability and consumer protection. The CBK seeks to review open but secure APIs standards as a medium-term goal by 2023 or 2024. The Ministry of Treasury and Planning is also finalising a Digital Finance Policy, one of whose strategic objectives is to include open infrastructure. Any investor seeking to provide initiatives in open banking must therefore seek direction from the CBK.

Mauritius

Shianee Calcutteea[1]
Bowmans, Mauritius
shianee.calcuttea@bowmanslaw.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

The Fintech legal framework in Mauritius is mainly administered by the Financial Services Commission (FSC) set up under the Financial Services Act 2007 (FSA) and the Bank of Mauritius (BoM) under the Bank of Mauritius Act 2004 (BMA).

The legislators in Mauritius have been actively ensuring that Mauritius becomes a competent fintech hub. Accordingly, several amendments were made and/or introduced recently.

Fintech hubs

In 2021, the FSA was amended to authorise the FSC to set up fintech innovation hubs and digital labs, and to regulate and supervise financial institutions or startups providing relevant services under the fintech umbrella.

Digital banking

The Banking Act 2004 of Mauritius was amended in 2020 to introduce a digital banking licence. Digital banking business is defined in the Banking Act as 'banking business carried on exclusively through digital means or electronically'.

In December 2021, the BoM issued guidelines for digital banks setting out the regulatory and supervisory framework for operating a digital bank in Mauritius along with the application process for a digital banking licence. The guidelines also specify additional requirements to, or exemptions from, the framework generally applicable to traditional banks.

Digital currencies

The BMA was amended to allow the BoM to issue digital currencies. The BoM is now also authorised to open accounts for, and accept deposits of, digital currencies from such persons as determined by the bank, and to make rules to establish the framework under which digital currency may be issued by the bank and may be held or used by the public. It has been recently communicated that the BoM is working towards the introduction of a retail central bank digital currency (CBDC), which will be called the 'digital rupee'.

1 Shianee is a partner in our Mauritius office who specialises in corporate law, banking law, mergers and acquisitions, employment, compliance and regulatory issues. Her experience has included advising on various sizeable M&A transactions and corporate restructurings, both local and cross-border.

In order to finalise the design attributes of the digital rupee, the BoM requested technical assistance from the International Monetary Fund (IMF). The BoM is the first central bank to have benefitted from such technical assistance from the IMF. The BoM has to date begun a pilot project starting with one commercial bank in Mauritius to further its research for the potential implementation of the digital rupee.

Virtual assets

A framework regulating business activities involving virtual assets was introduced through the Virtual Asset and Initial Token Offering Services Act 2021 (VAITOS), which is further detailed in Question 2.

Non-fungible tokens

The FSC has recently clarified its stance in relation to non-fungible tokens (NFTs). The FSC acknowledges that NFTs may taken different forms and warrant different regulatory treatment. To the extent that an NFT is issued and marketed as a unique digital collectible and is not used for payment or investment purposes, it will not fall within the purview of the FSC.

However, if an NFT constitutes a transferrable financial asset such as a share or an interest in a collective investment scheme or if it falls under a category of virtual assets, any trading or offer of such NFTs will require an applicable license by the FSC.

Peer-to-peer lending

In August 2020, the FSC introduced the licensing criteria for peer-to-peer (P2P) lending. Prior to this, P2P operators were operating under regulatory sandbox licensing issued by the FSC. P2P lending is an emerging fintech practice that enables a person to lend funds through an online portal or electronic platform, whereby a P2P operator facilitates the access to finance by matching borrowers and lenders on its online platform.

Robotic and artificial intelligence-enabled advisory services

Mauritius has introduced the robotic and artificial intelligence-enabled advisory services (RAIEAS) licence to encourage companies in Mauritius to put in place emerging technologies. In June 2021, the FSC issued The Robotic and Artificial Intelligence Enabled Advisory Services Rules 2021 to regulate the conduct of these services. RAIEAS is defined as the provision of digital and personalised advisory services through a computer program and/or artificial intelligence-enabled algorithms with limited human intervention. No person can carry out RAIEAS without a licence issued by the FSC.

Crowdfunding

The Financial Services (Crowdfunding) Rules 2021 came into operation on 4 September 2021, bringing a legal framework to crowdfunding platforms. As per the Rules, a crowdfunding activity involves the solicitation of funds from investors for a specific investment purpose through an

online portal or electronic platform. The Rules further confirm the requirement to apply for a crowdfunding licence issued by the FSC in order to operate a crowdfunding platform.

Mauritius Central Automated Switch (MauCAS)

The MauCAS was launched by the BoM in August 2019. It is fully owned and operated by the BoM for routing payments among operators on a 24/7 basis. The goal of MauCAS is to create an enabling environment for digital payments to support the development of Mauritius as a digital economy. In September 2021, the national MauCas QR code was also launched. The QR code, which is hosted on the Bank's MauCAS platform, allows swift and secure digital and mobile payments when making bank transfers, including international transactions.

Cloud services

The BoM issued guidance in September 2022 in relation to the use of cloud services by its licensees so that the risks are duly identified and managed. The guidelines especially provide for the level of governance to be applied, the risk assessment, the information security requirements, the types of controls to be deployed, contingency plans and exit strategies, as well as the level of the initial and ongoing due diligence and assurance to be performed in respect of cloud services.

The BoM defines 'cloud services' as services provided using a model enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

In 2021, VAITOS was introduced to provide a legal framework in sync with international standards in relation to virtual assets like cryptocurrencies as well as to safeguard against money laundering and terrorist financing associated with such virtual assets. VAITOS defines a virtual asset (which includes cryptocurrencies) as:

> 'a digital representation of value which may be digitally traded or transferred, and may be used for payment or investment purposes, but does not include a digital representation of fiat currencies, securities and other financial assets that fall under the purview of the Securities Act of Mauritius'.

In Mauritius, the FSC regulates and supervises the non-banking cryptocurrency environment, especially in relation to virtual asset service providers (VASPs) and issuers of virtual asset offerings to the public (ITOs).

VAITOS regulates VASPs and ITOs by setting out rules in relation to technical requirements, governance structures, risk management, disclosure of information requirements, and the protection of the rights of clients of virtual assets. The following activities are licensed under VAITOS:

- Class M (Virtual Asset Broker-Dealer) licence to carry out activities such as exchange between virtual assets and fiat currencies;
- Class O (Virtual Asset Wallet Services) licence pertaining to the transfer of virtual assets;
- Class R (Virtual Asset Custodian) licence for safekeeping or administration of virtual assets or instruments enabling control over virtual assets;
- Class I (Virtual Asset Advisory Services) licence for the participation in and provision of financial services related to an issuer's offer and/or sale of virtual assets; and
- Class S (Virtual Asset Market Place) for setting up and running a virtual asset exchange.

Pursuant to VAITOS, holders of the above licences are also subject to a local anti-money laundering and prevention of terrorism financing (AML/CFT) legal framework, which includes the Financial Intelligence and Anti-Money Laundering Act among others.

The BoM is expected to soon issue a guideline setting out the principles to be followed by banks involved in activities related to virtual assets, in which the BoM is expected to embrace the principles set out in the second consultative document of the Basel Committee in relation to the prudential treatment of crypto asset exposures.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

The framework for the regulation, oversight, and supervision of payment systems in Mauritius (other than banks or companies who wish to provide payment intermediary services exclusively outside Mauritius) is governed by the National Payment Services Act 2018.

Any party who wishes to act as a payment service provider can apply for a licence to do so from the BoM, along with the payment of a non-refundable fee. A successful applicant must:

- have a principal place of business in Mauritius, and the staffing requirement and estimated operating costs must be commensurate with the size and complexity of its business;
- have an adequate number of suitably qualified full-time officers, including a CEO and other senior officers; and
- have in place an AML/CFT policy and monitoring system, as well as such other monitoring systems as are commensurate with the identified risks and the size and complexity of its business.

Further, with respect to digital wallets, VAITOS has introduced the Class R (Virtual Asset Custodian) licence which is regulated and issued by the FSC. This licence allows a licensee to conduct the business of safekeeping and administration of virtual assets or other instruments enabling control over virtual assets.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

The BoM (in respect of banking-related services) or the FSC (in respect of non-banking-related services) operate a regulatory sandbox authorisation for business activities for which there exists no legal framework or adequate provisions under existing local legislation. The authorisation creates a controlled 'safe space' where innovative products and business models can be tested without immediately being subject to all the regulatory requirements; applicants can conduct live experiments with fintech or other innovation-driven financial services under the supervision to test the viability of innovative business models.

Any corporate body can apply for a regulatory sandbox authorisation. All applications must be made to the BoM in respect of banking-related services or the FSC in respect of its non-banking-related services.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

While to date there are no regulations or framework regarding open banking in Mauritius, during the Budget Brief 2021 on 11 June 2021, it was proposed that the BoM will issue a guideline in respect of the usage of APIs to support open banking initiatives. A relevant framework is therefore in the pipeline.

Nigeria

Yinka Edu[1]
Udo Udoma & Belo-Osagie, Lagos
Yinka.Edu@uubo.org

Joseph Eimunjeze[2]
Udo Udoma & Belo-Osagie, Lagos
Joseph.Eimunjeze@uubo.org

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

Depending on the nature of their business, fintech operators in Nigeria are subject to different laws and regulated by various institutions. Such laws include the Companies and Allied Matters Act 2020 (CAMA), the Central Bank of Nigeria Act 2007 (CBN Act), the Banks and Other Financial Institutions Act 2020 (BOFIA), moneylenders laws applicable in the various states in Nigeria, and regulations, guidelines and circulars issued pursuant to these laws.

The Central Bank of Nigeria (CBN) is the principal regulator of the Nigerian fintech space. The CBN derives its powers from the CBN Act and the BOFIA. BOFIA requires that any entity carrying on the business as a financial institution must obtain a licence from the CBN.

Regarding moneylending, any entity not licensed by the CBN, but which wishes to carry on the business of moneylending is required to obtain a moneylender's licence from the state government in the state in which it intends to carry on its business.

Lastly, every entity wishing to do business in Nigeria is required to be incorporated with the companies' registry and comply with the requirements of CAMA. For fintech companies, CAMA prescribes the minimum requirements for incorporation, share capital, operations, management, meetings, directors, shareholding and other related matters.

There are other laws which apply to fintech companies in varying degrees not discussed in this update. We have set out below a summary of some of the most important regulations with respect to fintech and financial innovation in Nigeria.

New licence categorisations for the Nigerian payments system

The CBN issued the *New Licence Categorizations for the Nigerian Payments System, 2020* (NPS Circular) in 2020 to provide for the different categories of licences and requirements for carrying on business as a payment operator in Nigeria. Furthermore, the CBN subsequently issued the approved new licence

1 Yinka is a partner in the firm's banking and finance team and heads the firm's capital markets and fintech teams. Yinka is ranked as a Tier 1 Lawyer in the *Chambers Global Fintech Guide 2021* as well as in *Chambers Global* for her expertise in banking & finance and corporate/commercial practice. She has also been commended for her banking & finance and capital markets work in the current edition of *Who's Who Legal*.

2 Joseph is a partner in the firm's banking and finance, fintech, corporate advisory, capital markets and tax teams. His specialisation also includes mergers and acquisitions, insolvency and corporate restructuring, foreign investments and banking regulatory compliance. He has been recognised by the IFLR1000 2022 Nigeria jurisdiction reviews as a Highly Regarded Lawyer in the practice areas of banking & finance and M&A.

categorisations in 2021 to provide for the specific requirements to be satisfied by an applicant before being issued each of the payments-related licences. Some of the payments-related licences in Nigeria are discussed in Table 1.

Guidelines on operations of electronic payment channels

These guidelines were introduced with the aim of promoting and facilitating the development of an efficient and effective payments system for the settlement of transactions in Nigeria, including the development of electronic payment systems. The guidelines have various sub-parts which cover the following operations:

- automated teller machine (ATM) operations;
- point of sale (POS) card acceptance services;
- mobile point of sale (MPOS) acceptance services; and
- web acceptance services.

Each fintech operator is required to comply with the parts of the guidelines which applies to its operations.

Regulatory framework and guidelines for mobile money services

The Regulatory Framework for Mobile Money Services in Nigeria and the Guidelines on Mobile Money Services in Nigeria 2021, cover the licensing regime, capital requirements and rules of operation for mobile payment transactions.

The regulations identified the following two models for the implementation of mobile money services:

- the bank-led model (with a bank and/or consortium of banks as lead initiator); and
- the non-bank led model (with a corporate organisation duly licensed by the CBN as lead initiator).

In addition, the regulations prescribe the permissible and non-permissible activities for mobile money operators in Nigeria.

Guidelines on transactions switching

The Guidelines on Transactions Switching in Nigeria 2016 set out the procedure for the operation of switching companies and the provision of switching services in Nigeria. It also covers the rights and obligations of the parties to a switching contract, prohibits exclusivity arrangements, prescribes operational modalities and the mandatory minimum standards required for providing switching services in Nigeria, as approved by the CBN.

Supervisory Framework for Payment Service Banks 2021

Payment service banks (PSBs) are financial service providers who leverage the use of technology to provide limited banking and financial services to persons in Nigeria. This regulation provides for the permissible and non-permissible activities of PSBs, ownership and licensing requirements, and the corporate governance structure for PSBs.

PSBs have in recent years gained popularity in Nigeria following the CBN's issuance of the Supervisory Framework for Payment Service Banks in 2021: one of the key objectives of the regulations is to improve the access of everyday Nigerians to financial services.

Regulatory Framework for Non-Bank Acquiring in Nigeria 2021

The Regulatory Framework for Non-Bank Acquiring in Nigeria 2021 sets out the procedure for the operation of non-bank merchant acquirers in Nigeria including the rights and obligations of parties involved in the acquiring process and business.

According to the CBN, a merchant acquirer is an institution responsible for processing and settling credit and debit card transactions on behalf of merchants or other businesses. Merchant acquirers play an integral role in the electronic payment system and transaction processing as they enable merchants to accept card payments by acting as a link between merchants, financial institutions and card schemes. Their functions typically include transaction authorisation, processing, and settlement of electronic payment transactions.

The Nigeria Startup Act

The Nigeria Startup Act was a joint initiative of the Presidency and stakeholders in the Nigerian fintech space. The Act defines a startup based on certain criteria, some of which include:

- the nationality of the company;
- objects of the company;
- shareholding of the company;
- goods/services provided by the company; and
- expenses of the company.

The Act establishes the Council for Digital Innovation and Entrepreneurship (the Council) which has, as one of its principal functions, the responsibility to support digital and technological development through grants to persons, research institutions and universities pursuing postgraduate programmes in the areas of science, technology and innovation. The Act also seeks to harness Nigeria's ever-growing fintech space by providing tax and fiscal incentives for qualified startups. Some of the incentives include exemption from payment of income tax for a period of about four years and access to export initiatives and financial assistance to qualified entities involved in the exportation of products and services.

It is expected that the Act will further help to increase investments in the Nigerian fintech space by incentivising potential investors and creating an enabling environment for startups, and by extension, fintech and financial innovation.

In relation to new laws or regulations that may be enacted or issued in the near future, or any bill on fintech and financial innovation in Nigeria, we have provided a high-level overview of some proposed laws and regulations below.

Operational Guidelines for Open Banking in Nigeria 2023

In March 2023, the CBN issued the Operational Guidelines for Open Banking in Nigeria (the Guidelines) which apply to banking and other related financial services. Organisations that use customers' data for the purpose of providing innovative financial services within Nigeria are eligible participants in the open banking ecosystem. Participants are required to, amongst other things, adhere to security standards when accessing and storing customers' data, subject to compliance with minimum privacy, operational, customer experience and risk management standards as prescribed by the CBN.

The Guidelines categorise participants into API providers (APs), API consumers (ACs), and customers, depending on the roles the participants play in the open banking sector. The CBN, through the Guidelines, stipulates the clear responsibilities and expectations for the various participants.

The APs and ACs are required to establish and implement a data governance policy, data ethics framework, data breach policy, etc. APs and ACs, in dealing with customers' data, are also required to comply with the Nigeria Data Protection Act 2023 and other data privacy and protection regulations issued by the regulators, including any data protection regulations issued by the CBN.

The Guidelines require that the intellectual property, including proprietary and protectable software source and object codes, aggregate data, aggregate services and other protectable information, will be protected under the applicable laws in Nigeria.

To maintain the highest standards of integrity and security within the open banking system, the Guidelines also mandate APs and ACs to comply with the Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) in Banks and Other Financial Institutions in Nigeria Regulations.

The Nigeria Data Protection Act 2023

On 12 June 2023, the President of the Federal Republic of Nigeria, Bola Ahmed Tinubu, signed the Nigeria Data Protection Act 2023 (NDPA) into law. The NDPA was enacted to regulate the protection of personal data and establish the Nigeria Data Protection Commission (the Commission). The NDPA has notable provisions that significantly impact how organisations (such as financial services companies) collect and process customers' personal data. Before the enactment of the NDPA, data privacy in Nigeria was primarily regulated by the Nigeria Data Protection Regulation 2019 (NDPR) and the NDPR Implementation Framework 2020 (Implementation Framework). The NDPA did not repeal the NDPR and the Implementation Framework, which means that these instruments are still

in force. Where there is a conflict between the provisions of the NDPA, the NDPR and the NDPR Implementation Framework, the provisions of the NDPA will prevail in such circumstances.

Applicability

The provisions of the NDPA apply in circumstances where (1) a data controller or processor is domiciled in, resident in, or operating in Nigeria; (2) the processing of personal data occurs within Nigeria; or (3) the data controller or processor is not domiciled in, resident in, or operating in Nigeria, but is processing the personal data of a data subject in Nigeria. Data controllers and data processors are required to comply with the principles of data processing set out in the NDPA.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

Cryptocurrency

Generally speaking, crypto assets are not statutorily defined or regulated in Nigeria. As a result, parties are generally free to engage in crypto transactions on a bilateral basis. The Securities and Exchange Commission (SEC) has, however, issued the Rules on Issuance, Offering Platforms, and Custody of Digital Assets (the Rules) in which the SEC defines virtual assets and digital assets. Under the Rules, digital assets are defined as digital tokens that represent assets such as a debt or equity claim on the issuer, while virtual assets are defined as a digital representation of value that can be transferred, digitally traded and used for payment or investment purposes excluding digital representations of fiat currencies, securities, and other digital assets. Under the Rules, the SEC seeks to regulate the offering of virtual and digital assets, which may include cryptos targeted at the general public in the country.

In relation to CBN-regulated entities, the CBN has taken an entirely different approach regarding crypto transactions by its regulated entities. The CBN released a circular dated 5 February 2021, titled *Letter to All Deposit Money Banks, Non-Bank Financial Institutions and Other Financial Institutions* (CBN Circular). The CBN Circular applies to all deposit money banks, non-bank financial institutions and other financial institutions (together, regulated institutions). Pursuant to the circular, the CBN prohibits the regulated institutions from dealing in cryptocurrencies or facilitating payments for cryptocurrency exchanges. The CBN also mandated regulated institutions to ensure that they do not hold, trade, use or transact in cryptocurrencies and virtual currencies in any way.

The above diverging positions of the CBN and the SEC has been clarified by the SEC, which has issued a press release stating that there are no inconsistencies between the CBN circular and the Rules. It adds that, in recognition of the fact that digital assets may have the full features of investments as defined in the Investments and Securities Act 2007 (the legislation governing investments and securities in Nigeria), the trading of such assets falls under the purview of the SEC unless proven otherwise. Notwithstanding the position of the SEC, it is currently unclear how entities engaging in crypto business can comply with the Rules if such entities cannot operate bank accounts from the settlement of transactions in cryptos.

Blockchain

In May 2023, the Federal Ministry of Communications and Digital Economy released the National Blockchain Policy for Nigeria (the Blockchain Policy), which is a comprehensive framework aimed at promoting the responsible adoption and utilisation of blockchain technology in the country. It encourages collaboration, talent development, and ethical practices in the blockchain industry. The Blockchain Policy seeks to drive innovation through research and development support, partnerships with industry experts, and incentives for startups. Nigeria aims to leverage blockchain to transform financial services, enhance security, and digitise government and corporate services such as identity management and supply chain management. Overall, the Blockchain Policy sets the stage for the adoption and responsible utilisation of blockchain technology in Nigeria, geared towards driving economic growth, enhancing security, and fostering innovation.

The National Information Technology Development Agency (NITDA), an agency supervised by the Ministry, has been tasked with responsibility for the coordination of the Blockchain Policy. In addition, a multi-sectoral Steering Committee (comprising key agencies pivotal to the widespread adoption of blockchain technology) has been established to oversee the policy's execution. Prominent members of the committee include the CBN, the NITDA, the National Universities Commission, the SEC, and the Nigerian Communications Commission. Their primary task is to create an all-encompassing framework for implementing blockchain technology across different sectors of the economy.

Tax on gains from crypto assets

The Finance Act of 2023, which became effective on 1 September 2023, introduces amendments to the Capital Gains Tax Act 2004 (as amended). One notable change is the inclusion of digital assets as chargeable assets for capital gains tax purposes. Based on this amendment, gains (less any applicable deductions) realised from the disposal of digital assets are now liable to capital gains tax in Nigeria at the rate of 10 per cent. While the Finance Act does not specifically define 'digital asset', the SEC Rules offer a definition for virtual and digital assets, potentially encompassing cryptocurrencies accessible to the general public within the country.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

In order to operate as a payment service provider or provide services relating to a digital wallet in Nigeria, an entity is required to obtain a licence from the CBN. Payment service providers in Nigeria are classified into various categories. We have provided a high-level overview of each category and the permissible activities as stipulated by the CBN in Table 1.

No	Category/licence	Permissible activities
1.	Payment Solution Services	All activities permitted under the Payment Solutions Service Provider (PSSP), Payment Terminal Service Provider (PTSP) and Super-Agent categories.
2.	Payment Solutions Service Provider	Payment processing gateway and portals, payment solutions/application development, merchant service aggregation and collections.
3.	Payment Terminal Service Provider	Point of sale (POS) terminal deployment and services, POS terminal ownership, payments terminal application development, merchant/agent training and support.
4.	Super-Agent	Agent recruitment and management, bills payment (utilities, taxes, tenement rates, subscriptions, etc), payment of salaries; funds transfer services (local money value transfer), balance enquiry, generation and issuance of mini-statements, collection and submission of account opening and other related documentation, agent mobile payments/banking services, cash disbursement, cash repayment of loans and cash payment of retirement benefits, cheque book request and collection, and collection of bank mail/correspondence for customers.
5.	Mobile Money Operator (MMO)	E-money issuing, wallet creation and management, pool account management, bill payment, agent recruitment and management, pool account management, non-bank acquiring as stipulated in the regulatory requirements for non-bank merchant acquiring in Nigeria, any other activities that may be permitted by the CBN from time to time and all activities permitted under the Super-Agent category.
6.	Switching and Processing	Switching, card processing, transaction clearing and settlement agent services, non-bank acquiring services.
7.	Payment Service Banks	Accepting deposits, payments, and remittance (inbound), operation of electronic wallets, issuance of debit and pre-paid cards, financial advisory and investment in Federal Government of Nigeria and CBN securities.

Table 1: Payment service provider categories

In relation to the question on the regulatory framework for mobile wallet creation, one of the permissible activities for MMOs includes the creation and management of e-wallets. Therefore, entities which intend to provide digital wallet-related services to persons in Nigeria will be required to obtain an MMO licence or PSB licence from the CBN.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

The CBN, as the primary regulator of the Nigerian financial and payment system, plays a major role in determining the ease of entry or otherwise into the financial services space.

As part of its efforts to support fintechs, the CBN in 2021 released the Framework for Regulatory Sandbox Operations (Sandbox Regulations). According to the Sandbox Regulations, the sandbox encourages innovation that can improve the design and delivery of payment services and is, therefore, also suitable for proposed products, services, or solutions that are either not contemplated under the prevailing laws and regulations or do not precisely align with existing regulations.

The sandbox application process is open to both existing CBN licensees (financial institutions with fintech initiatives) and other local companies. The latter may include financial sector companies, as well as technology and telecom companies intending to test an innovative payments product, or service industry deemed acceptable by the CBN. The CBN also has the power to review an approval granted to any participant before the end of the testing period of the participant in the sandbox.

Similarly, the SEC has adopted a 'Three-Pronged Objective' to regulate and facilitate innovations in the Nigerian fintech landscape. This includes: safety; market/financial deepening; and providing solutions to existing problems. In furtherance of these objectives, the SEC released the Regulatory Incubation Guidelines for Specific Category of Fintech Entrepreneurs (Incubation Guidelines) and created a Fintech & Innovation Office (FINO) to facilitate its communication with fintech innovators, regulate fintech businesses and constantly engage with innovation hubs around the country.

The Incubation Guidelines allow the SEC to supervise some new models of providing capital market services in limited form before it becomes fully established. Interested participants are required to show, among other things, that they are using innovative technology to offer a new type of product or service or apply innovative financial technology to an existing product or service.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

Nigeria currently has regulations on open banking. In February 2021, the CBN released the Regulatory Framework for Open Banking in Nigeria (Open Banking Framework) which establishes the principles for data sharing across the banking and payment system to promote innovations and broaden the range of financial products and services available to bank customers.

The Open Banking Framework applies to the following financial services: deposit taking, credit, credit ratings and scoring, payment and remittance services, leasing and hire purchase mortgage, collection and disbursement services and treasury management. Prior to the issuance of the Open Banking Framework, Nigerian banks enjoyed exclusive access to customers' information, thereby locking out innovators and forcing customers to rely solely on the digital channel offerings of their respective banks. With the issuance of the Open Banking Framework, financial services are expected to experience better growth and invention of innovative products.

Further to, and in line with, the Open Banking Framework, the CBN released the exposure draft of the Operational Guidelines for Open Banking in Nigeria which sets out, among other things, detailed provisions on the roles, minimum requirements, responsibilities, and expectations for the participants in the open banking system. As explained in Question 1, in March 2023 the CBN issued the Guidelines on open banking in Nigeria. The Guidelines apply to banking and other related financial services. Organisations that use customers' data for the purpose of providing innovative financial services within Nigeria are eligible participants in the open banking ecosystem. Participants are required to, among other things, adhere to security standards when accessing and storing customers' data, subject to compliance with minimum privacy, operational, customer experience and risk management standards as prescribed by the CBN.

Contactless Payments

On 27 June 2023, the CBN issued the Guidelines on Contactless Payments (the Contactless Guidelines) in a bid to foster innovation and standardise operations in the payments systems in Nigeria. Contactless payment enables the consummation of financial transactions without the need

for physical touch: that is, it eliminates the need to hand over credit/debit cards or manually swipe them through machines. The purpose of the Contactless Guidelines is to:

- define the minimum requirements and standards for contactless payment operations in Nigeria;
- to outline the roles and responsibilities of all stakeholders involved in those operations; and
- to ensure that the stakeholders implement the necessary risk management procedures and safeguards while adhering to the highest industry standards.

All industry stakeholders who participate in contactless payments are to comply with the provisions of the Contactless Guidelines. These stakeholders include acquirers, issuers, payment schemes, card schemes, switching companies, payment schemes, payment terminal service providers, payment terminal service aggregators, merchants, terminal owners, customers, and any other stakeholder/participant that the CBN may designate. Stakeholders that process and/or store customers' information must also ensure their terminals, applications, and processing systems comply with the minimum standards.

South Africa

Bright Tibane[1]
Bowmans, Johannesburg
bright.tibane@bowmanslaw.com

Kirsten Paulo[2]
Bowmans, Johannesburg
kirsten.paulo@bowmanslaw.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

There is currently no specific regulatory framework regulating fintech or financial innovation in South Africa. Notwithstanding, certain fintech products and services may fall within the scope and ambit of the traditional financial sector regulatory frameworks, as the frameworks are generally activity-based.

The most relevant laws applied to fintech products or service offerings (ie, the legislation that fintech products and services are tested against prior to their roll out) are as follows:

- the Financial Advisory and Intermediary Services Act 2002 (FAIS), which regulates the provision of financial services (ie, investment advice and intermediary services) in relation to financial products, including 'robo-advice' or automated investment advice. Notably, in October 2022 crypto assets were declared a financial product under FAIS, bringing crypto asset service providers (CASPs) within the FAIS regulatory framework. This has empowered the FSCA to regulate the advisory and intermediary component of crypto assets as an interim measure, pending the commencement of the Conduct of Financial Institutions (CoFI) Bill (discussed below);
- the Financial Markets Act 2012 (FMA), which regulates the capital/financial markets, particularly securities trading infrastructures and their participants;
- the National Credit Act 2005, which regulates the provision of credit and lending activities, including peer-to-peer (P2P) lending, crowdfunding and buy now pay later (BNPL) platforms;
- the Banks Act 1990 (Banks Act), which regulates banking business and deposit-taking related activities. The issuance of e-money or electronic money is considered to be regulated under the Banks Act;

1 Bright is a Partner in Bowmans' Banking & Finance department in Johannesburg and a member of the Banking and Financial Services Regulatory practice. Bright is a financial sector-focused regulatory lawyer who specialises in financial services, financial technology (fintech) services, securities, fund management, domestic and international payment services, regulated lending, exchange control, banking services and anti-money laundering and counter-terrorist financing.

2 Kirsten Paulo is a senior associate in Bowmans' Banking & Finance department in Johannesburg and a member of the Banking and Financial Services Regulatory practice. Kirsten specialises in all aspects of financial services (including fintech services), banking, payment services and investment management regulatory law, and advises local and foreign clients on the content and implications of the Financial Sector Regulation Act 2017, the Financial Advisory and Intermediary Services Act 2002, the Collective Investment Schemes Control Act 2002, the Banks Act 1990, the Financial Intelligence Centre Act 2001, the National Payment Systems Act 1998, the Financial Markets Act 2012, and the National Credit Act, 2005 (along with the regulations to and host of subordinate legislation promulgated under this legislation).

- the National Payment Systems Act 1998 (NPSA), which regulates the domestic payment system and role-players in the payment system, both banks and non-banks (such as payment aggregators and payment service providers / payment gateway providers); and
- the Exchange Control Regulations 1961 issued under the Currency and Exchanges Act 1933, which regulate cross-border flow of capital (including money) and institutions that facilitate cross-border flow of capital.

In terms of new law foreseen in the near future on fintech and financial innovation, the enactment of the CoFI Bill is anticipated in 2024, which will seek to enable open finance. It is envisaged that the CoFI Bill, once enacted, will repeal FAIS and regulate crypto asset-related financial advice and intermediary services.

Once in effect, CoFI will materially change the regulatory regime currently applicable to financial institutions and parties seeking to carry out regulated financial services activities in or in relation to South Africa.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

In October 2022, the Financial Sector Conduct Authority (FSCA) declared crypto assets as a financial product in terms of FAIS. In turn, a CASP, being any person furnishing advice or rendering intermediary services in relation to crypto assets, is required to be appropriately licensed as a financial services provider with the FSCA in terms of FAIS (subject to certain transitional provisions). In addition, in December 2022, CASPs were also declared as accountable institutions in terms of FICA (subjecting them to the provisions of South Africa's chief anti-money laundering legislation, including reporting obligations and customer due diligence).

In addition to FAIS, the characteristic of a crypto asset must be borne in mind in terms of how it may potentially otherwise be regulated in South Africa. By way of example, some crypto assets (such as stablecoins) have the potential to be seen as derivative instruments which are regulated by both the FMA and FAIS. Similarly, while the regulation of securities generally does not extend to crypto assets (as they are not regarded as securities), those that meet the functional definition of securities may be regulated under the FMA and FAIS.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

Payment service providers

In South Africa, payment service providers are regulated by the NPSA. Non-bank payment service providers are specifically regulated by Directive 1 of 2007 (which regulates payment aggregators/ non-bank acquirers) and Directive 2 of 2007 (which regulates system operators) issued by the South African Reserve Bank (SARB). Payment service providers are required to be authorised by

the Payments Association of South Africa (PASA), as the body mandated by the SARB to organise, manage, and regulate the participation of its members in the national payment system.

The South African regulated payment system encompasses the entire payment process from payer to beneficiary and 'includes all the tools, systems, mechanisms, institutions, agreements, procedures, rules or laws applied or utilized to effect payment'.

Digital wallets

Digital wallets usually have the potential to be regulated either under the Banks Act or FAIS.

Some digital wallet services have the potential to qualify as 'the business of a bank', as regulated by the Banks Act. The Banks Act defines 'the business of a bank' as:

> '(a) the acceptance of deposits from the general public (including persons in the employ of the person so accepting deposits) as a regular feature of the business in question;
>
> (b) the soliciting of or advertising for deposits;
>
> (c) the utilization of money, or of the interest or other income earned on money, accepted by way of deposit as contemplated in paragraph (a)–
>
> (i) for the granting by any person, acting as lender in such person's own name or through the medium of a trust or a nominee, of loans to other persons;
>
> (ii) for investment by any person, acting as investor in such person's own name or through the medium of a trust or a nominee; or
>
> (iii) for the financing, wholly or to any material extent, by any person of any other business activity conducted by such person in his or her own name or through the medium of a trust or a nominee;
>
> (d) the obtaining, as a regular feature of the business in question, of money through the sale of an asset, to any person other than a bank, subject to an agreement in terms of which the seller undertakes to purchase from the buyer at a future date the asset so sold or any other asset.'

The Banks Act defines a 'deposit' to mean an amount of money paid by one person to another person, subject to an agreement in terms of which:

> 'a) an equal amount or any part thereof will be conditionally or unconditionally repaid, either by the person to whom the money has been so paid or by any other person, with or without a premium, on demand or at specified or unspecified dates or in circumstances agreed to by or on behalf of the person making the payment and the person receiving it; and
>
> b) no interest will be payable on the amount so paid or interest will be payable thereon at specified intervals or otherwise, notwithstanding that such payment is limited to a fixed amount or that a transferable or non-transferable certificate or other instrument providing for the repayment of such amount mutatis mutandis as contemplated in sub-paragraph a) or for the payment of interest on such amount mutatis mutandis as contemplated in this sub-paragraph b) is issued in respect of such amount.'

Some digital wallets have the potential to qualify as electronic money/e-money, which is provided for under a position paper published by the SARB in November 2009, entitled the *Position Paper on Electronic Money* (E-Money Position Paper). Only registered South African banks are permitted to issue e-money. This requirement often means that fintech companies will need to partner with a bank to provide certain services within South Africa.

The E-Money Position Paper defines e-money as 'monetary value represented by a claim on the issuer. This money is stored electronically and issued on receipt of funds, is generally accepted as a means of payment by persons other than the issuer and is redeemable for physical cash or a deposit into a bank account on demand'.

In order for any business activity or representation of value to qualify as e-money for the purposes of the E-Money Position Paper, all aspects/elements of the definition of e-money must be present or apply. As such, depending on their structure, digital wallets may meet the definition of e-money.

There is currently no e-money licensing framework in South Africa. According to the E-Money Position Paper, the SARB currently allows only South African registered banks to issue e-money. The E-Money Position Paper does, however, refer to section 52 of the Banks Act, which allows for non- banks to enter into arrangements with banks which may permit them to offer banking- related services in conjunction with registered banks. As such, if a digital wallet constitutes e-money, the issuer can rely on section 52 of the Banks Act and have a formal alliance with a licensed bank for purposes of issuing e-money.

Digital wallet services could also constitute financial services regulated by FAIS.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

In 2016, the Intergovernmental FinTech Working Group (IFWG) was established (comprising members from the SARB, National Treasury, the FSCA, the Financial Intelligence Centre and the South African Revenue Services), with the purpose of developing a common understanding among regulators and policymakers of financial technology developments, and policy and regulatory implications for the financial sector and economy.

The IFWG has established a regulatory guidance unit, a regulatory sandbox and an innovation accelerator initiative, all of which form part of the IFWG Innovation Hub. The regulatory sandbox gives participants an opportunity to test innovative products or services against existing legislation and regulations while the innovation accelerator initiatives provide a collaborative, exploratory environment for financial sector regulators to learn from and work with each other (and the broader financial sector ecosystem) on emerging innovations in the industry.

In October 2022, the IFWG published a report providing feedback on the work of its inaugural regulatory sandbox initiative which commenced with a cohort-based application process in April 2020. The inaugural cohort proceeded with nine sandbox tests from eight participants. The test cases covering a variety themes, including:

- cross-border crypto payments;
- CASP safe custody service;
- tokenisation of assets; and
- credit data (non-traditional).

The IFWG has resolved to move from a cohort approach (where regulators only receive applications during an open application window) to an adjusted rolling approach, under which the regulatory sandbox will generally remain open for applications and allow relevant regulators to provide an indication of their areas of focus, regulatory appetite, and capacity and resource constraints in assessing applications throughout the regulatory sandbox period.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

There are currently no open banking regulations in South Africa. The sharing of consumer financial data, including any personal information by any service provider and participating bank, is currently subject to the Protection of Personal Information Act 2013, which regulates the processing of personal information, provides for the rights of data subjects, and prescribes the obligations of data controllers and data processors.

In November 2020, the SARB issued a consultation paper on open banking activities in the national payment system, which makes various policy proposals regarding open banking, including:

- a new class of third-party providers should be introduced, and access to customers' financial information should be promoted to improve product and service offerings for customers;
- such third-party providers should be regulated by the SARB and the FSCA;
- banks should provide access to customers' financial information, subject to customer consent, to such third-party providers;
- technical standards for open banking should be developed and implemented; and
- consumer education or awareness should be conducted.

In May 2023, the SARB (through its National Payment System Department) released Draft Directive No 1 of 2023 for public comment regarding the issuing of electronic funds transfer (EFT) credit payment instructions on behalf of a payer in South Africa's national payment system. The purpose of the directive is to impose requirements on persons issuing EFT credit payment instructions on behalf of a payer, using screen scraping or any other tool in the national payment system, to mitigate risks associated with such payments. These risks include (but are not limited to) lack of data privacy, exposure to fraud and lack of informed consent.

The requirements intended to be imposed on issuers of EFT credit payment instructions include certain registration requirements (including conditions) and numerous ongoing obligations (including obligations relating to compliance, reporting, risk management, etc).

Asia Pacific

Australia

Peter Reeves
Gilbert + Tobin, Sydney
preeves@gtlaw.com.au*

Anthony Basa
Gilbert + Tobin, Sydney
abasa@gtlaw.com.au†

Meg Dalco
Gilbert + Tobin, Sydney
mdalco@gtlaw.com.au‡

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

In Australia, the regulatory regimes are technology agnostic, with the same regulatory concepts applying to fintech businesses and other types of financial service providers. The regulatory framework that applies to fintech businesses includes:

- financial services and consumer credit licensing;
- registration and disclosure obligations;
- consumer law requirements;
- privacy; and
- anti-money laundering and counter-terrorism financing (AML/CTF) requirements.

Financial services and consumer credit laws

The Corporations Act 2001 (Cth) (Corporations Act) is the principal legislation that regulates the provision of financial services.

Fintech businesses that carry on a financial services business in Australia must hold an Australian financial services licence (AFSL) or be exempt from the requirement to be licensed. Financial services are broadly defined under the Corporations Act to include the provision of financial product advice, dealing in financial products (as principal or agent), making a market for financial products, operating registered schemes and providing custodial or depository services. There are specific things that are listed as financial products (eg, securities, derivatives and managed investment schemes). Financial products are also defined generally as a facility through which, or through the

* Peter is a partner in Gilbert + Tobin's Corporate Advisory team and leads the Fintech + Web3 practice at G+T. He is an expert and market-leading practitioner in fintech and financial services regulation.

† Anthony is a senior lawyer in Gilbert + Tobin's Corporate Advisory team focusing on fintech, crypto assets and financial services.

‡ Meg is a lawyer in Gilbert + Tobin's Corporate Advisory team with a focus on fintech, crypto assets and financial services.

acquisition of which, a person makes a financial investment, manages a financial risk or makes a non-cash payment. The definitions of financial service and financial product will generally capture any investment or wealth management business, payment service (ie, non-cash payment facility), advisory business (including robo-advice), trading platform, or crowdfunding platform.

Fintech businesses may also need to hold an Australian market licence where they operate a facility through which offers to buy and sell financial products are regularly made and accepted (eg, an exchange). In addition, if an entity operates a clearing and settlement mechanism (CS) which enables parties transacting in financial products to meet obligations to each other, the entity must hold a CS facility licence, or be exempt from the requirement to be licensed.

Similarly, the National Consumer Credit Protection Act 2009 (Cth) (Credit Act) imposes a licensing obligation on entities that engage in consumer credit activities. Fintech businesses that provide marketplace lending products and related services will generally constitute consumer credit activities that trigger the requirement to hold an Australian credit licence (ACL) or be exempt from the requirement to be licensed.

Adjacent to the Corporations Act and the Credit Act, the Australian Securities and Investments Commission Act 2001 (Cth) (ASIC Act) contains prohibitions on engaging in unconscionable conduct, and misleading and deceptive conduct, that will apply to fintech businesses that supply financial services or consumer credit.

The Australian Securities and Investments Commission (ASIC) is Australia's financial markets conduct regulator and is responsible for regulating the financial services and consumer credit regimes.

Australian consumer law

Fintech businesses may also be subject to prohibitions in the Australian Consumer Law under the Competition and Consumer Act 2010 (Cth) (Competition Act) which is enforced by the Australian Competition and Consumer Commission (ACCC).

The Australian Consumer Law applies to Australian businesses that engage or contract with consumers and small businesses. Obligations include a general prohibition on misleading and deceptive conduct, false or misleading representations, unconscionable conduct and unfair contract terms in relation to the offer of services or products.

Notably, from 10 November 2023 changes to the prohibition on unfair contract terms came into effect. Previously the unfair contract term regime only captured small business contracts that employed fewer than 20 persons. The regime now captures small business contracts with businesses that employ fewer than 100 persons or generate less than A$10m (in the last income year). Other changes include expanding the powers of Australian courts to enforce contraventions, while a civil penalty regime now applies.

While the Australian Consumer Law does not apply to financial products or services, many of these protections are enforced by ASIC either through mirrored provisions in the ASIC Act or through delegated powers.

Anti-money laundering and counter-terrorism financing laws

The Anti-money Laundering and Counter-terrorism Financing Act 2006 (Cth) (AML/CTF Act) applies to entities that provide 'designated services' and have a geographical link to Australia. Generally, the AML/CTF Act applies to any entity that engages in financial services, credit (ie, consumer or business) and payment activities, and the operation of digital currency exchanges. Obligations include enrolment with the Australian Transaction Reports and Analysis Centre (AUSTRAC), reports and customer due diligence.

On 20 April 2023, the Attorney General released proposed reforms to the AML/CTF Act which would result in lawyers, accountants, trust and company service providers, real estate agents and dealers in precious metals and stones coming within the scope and operation of the AML/CTF Act. The proposed reform also recommends expanding the current regulation of services provided by digital currency exchanges (being the exchange of crypto currency for fiat currency and vice versa) to include:

1. exchanges between one or more other forms of digital currency;
2. transfers of digital currency on behalf of a customer;
3. safekeeping or administration of digital currency; and
4. the provision of financial services related to an issuer's offer and/or sale of a digital currency (eg, initial coin offerings where companies sell investors a new digital token or cryptocurrency to raise money for projects).

The proposed reforms also recommend expanding the travel rule to remittance service providers and digital currency exchange providers in line with international standards (capturing information about the originator and beneficiary of a transfer).

On 2 May 2024 the Attorney General commenced a second consultation on the proposed reforms to the AML/CTF Act with the release of five consultation papers. The first four consultation papers contain further detail about the proposed reforms affecting real estate professionals, professional services providers, dealers in precious metals and stones, digital currency exchange providers, remittance services providers and financial institutions. The fifth consultation paper details broader reforms to simplify, clarify and modernise the AML/CTF regime.

Notably, the fourth consultation paper details reform relevant to payment service providers, digital currency exchange providers and financial institutions. If accepted, the changes would broaden the remit of designated service providers to include digital currency exchanges that 'make arrangements' for the exchange of digital assets, and remittance providers that provide 'value transfer' services. The fourth consultation paper also contains a proposal to introduce a suitability test for 'fit and proper persons' of registrable designated service providers (eg, remittance service providers and digital currency exchanges). The second stage of consultation closed on 13 June 2024. An update on the outcome of the consultation is expected in 2024.

From a regulatory guidance perspective, on 27 June 2023 AUSTRAC issued guidance that seeks to clarify the role of financial institutions and business sectors that are increasingly being 'debanked'

because they are considered high risk. Debanking refers to financial institutions restricting, rejecting or terminating banking services to customers from certain industries. AUSTRAC's guidance is not enforceable but provides a risk-based approach for financial institutions to follow when evaluating the legitimacy of customers from 'high risk' industries to minimise debanking.

Banking laws and prudential regulation

The Banking Act 1959 (Cth) requires those engaged in the business of banking to be authorised by the Australian Prudential Regulatory Authority (APRA) (ie, be an 'authorised deposit-taking institution' or ADI) before engaging in such business. It also contains the Financial Accountability Regime (FAR) which replaced the Banking Executive Accountability Regime (BEAR) on 14 September 2023.

BEAR is administered by APRA and establishes, among other things, accountability obligations for ADIs and their senior executives and directors, deferred remuneration, key personnel and notification obligations for ADIs. FAR will be administered jointly by APRA and ASIC and has a wider remit than BEAR to include general insurers, life insurers, private health insurers, registrable superannuation entity licensees, and significant related entities. FAR is now applicable to the banking industry after a six-month transition period. The insurance and superannuation industries have an 18-month transition period, after which they must comply with FAR.

The Financial Sector Collection of Data Act 2001 (Cth) (FSCODA) is designed to assist APRA in the collection of information relevant to financial sector entities. FSCODA generally applies to any corporation engaging in the provision of finance in the course of carrying on business in Australia. APRA collects data from registered financial corporations under FSCODA. Generally, registered financial corporations with assets greater than AU$50m need to regularly report statements of financial position to APRA.

The Financial Sector (Shareholdings) Act 1998 (Cth) imposes an ownership limit of 20 per cent in a financial sector company without approval from the Treasurer. A financial sector company includes authorised deposit taking institutions, certain types of insurance companies and a holding company of either of those things.

Privacy laws

The Privacy Act 1988 (Cth) (Privacy Act) regulates the handling of personal information by government agencies and private sector organisations that have an aggregate group revenue of at least AU$3m. In some instances, the Privacy Act will apply to businesses (ie, credit providers and credit reporting bodies) regardless of turnover. The Privacy Act includes 13 Australian Privacy Principles which impose obligations on the collection, use, disclosure, retention and destruction of personal information.

On 16 February 2023 the Attorney General released a report detailing 116 proposals at a principles level on how the Privacy Act can be uplifted to best fit consumer privacy needs (Privacy Report). The principles are aimed at strengthening the protection of individual personal information and enhancing individuals' control over their data. The government published its response to the

Privacy Report on 28 September 2023 and accepted (either in whole, or in principle) all but ten of the proposals. Draft legislation is expected in 2024.

In addition, the Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) contains the Notifiable Data Breaches (NDB) scheme which requires entities that are regulated under the Privacy Act to notify any affected individuals and the Office of the Australian Information Commissioner (OAIC) in the event of a data breach (ie, unauthorised access to or disclosure of information), which is likely to result in serious harm to those individuals.

The OAIC is Australia's privacy and freedom of information regulator and is responsible for administering the Privacy Act and the NDB scheme.

Payment system laws

Fintech businesses that provide payment services must operate in accordance with various laws that regulate the infrastructure of Australia's payments system and may be subject to direct regulation for certain activities. See Question 3 for further information regarding the regulation of payment service providers.

The Reserve Bank of Australia (RBA) is Australia's central bank and provides a range of banking services to the government and its agencies, overseas central banks and official institutions. It is also responsible for maintaining the stability of the financial system through monetary policy and regulating payment systems.

In 2021 the RBA completed a framework review of the regulatory regime supporting various payment methods. A key outcome of the review was the creation of a policy framework designed to encourage the deployment of least-cost routing, also known as merchant-choice routing, which is functionality that allows contactless (tap-and-go) dual-network debit card transactions at the point-of-sale to be processed through whichever network on the card is less costly for the merchant.

On 7 June 2023 the government released its Strategic Plan for Australia's Payment System (Strategic Plan) outlining the policy objectives and priorities to reform the payments system. The Strategic Plan follows several reviews in recent years and a government consultation on proposed priorities and reform objectives, focusing its agenda on:

1. *Promoting a safe and resilient system*: through reducing the prevalence of scams and frauds, supervising systematically important payment systems and strengthening defences against cyber attacks.

2. *Updating the payments regulatory framework*: by establishing a new payments licensing framework, enabling greater collaboration between payment system regulators, reducing small business transaction costs, implementing changes to the Payments Systems Act and promoting competition by facilitating transparent access to payment systems.

3. *Modernising payments infrastructure*: by upgrading the electronic funds transfer system that facilitates processing of direct entry payments (eg, direct debits and credits between individual accounts at different financial institutions), maintaining adequate access to cash and phasing out cheques.

4. *Uplifting competition, productivity and innovation across the economy*: through aligning payment system objectives and the Consumer Data Right framework, supporting the broader use of the government's Digital ID solution, uplifting digital and technological skills and building public trust and confidence in artificial intelligence.

5. *Keeping Australia as the leader in the global payments landscape*: through creating an environment that attracts and enables innovation, exploring the policy rationale for a central bank digital currency in Australia and supporting international efforts to facilitate cross-border payments.

The focus areas are underpinned by the government's key principles relating to the payments system: trustworthiness, accessibility, innovation and efficiency. The Strategic Plan was released alongside two consultations, the first on reforming the Payment Systems (Regulation) Act 1998 (Cth) (Payment Systems Act) and the second on modernising the licensing framework for payment services providers (PSPs).

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

At the time of writing, there are no laws in Australia that have been implemented to specifically regulate crypto assets. Generally, the predominant focus on the regulation of crypto assets has revolved around applying the established financial services regulatory framework. The only formal monitoring of crypto asset activity in Australia is in relation to AML/CTF. Digital currency exchange providers have obligations under the AML/CTF Act: they must register with AUSTRAC and are required to keep certain records relating to customer identification and transactions for up to seven years.

There have been numerous government reviews that are either ongoing or have recently been completed in connection with how crypto asset and crypto asset-adjacent services should be regulated. In particular, on 3 February 2023 the government released a consultation paper into token mapping, which seeks to identify the key activities and functions of crypto assets and map them against existing regulatory frameworks. The consultation closed on 3 March 2023. As at the time of writing, the government has not released its findings from the consultation.

The government has also indicated that it will release a licensing and custody paper for crypto asset service providers. It is expected that the recommendations from these reviews will have significant effects on the current regulatory regimes relevant to cryptocurrency.

On 29 March 2023 a private members bill was introduced to the Australian Parliament which proposes to regulate digital assets, including by introducing licensing requirements for digital asset exchanges, digital asset custody service providers and stablecoin issuers (Digital Assets Bill). The Digital Assets Bill also proposes to introduce disclosure requirements for facilitators of central bank digital currencies in Australia. The proposed licensing framework draws on familiar processes and requirements that already exist for AFSL and ACL holders. The Digital Assets Bill was introduced by a member of the opposing party to the current government and has not progressed through the Australian Parliament.

On 16 October 2023, the Treasury commenced a consultation on a proposed reform to regulate digital asset platforms under the existing financial services regime. The proposed reform includes introducing a requirement for 'digital asset facilities' (ie, multi-function platforms that hold client assets and allow clients to transact in platform entitlements) to be regulated as a financial product, and for certain providers of related services to be required to hold an AFSL. Enhanced conduct obligations and consumer protections are also expected to be imposed in respect of digital asset facilities. The proposed reform also includes a proposal to introduce minimum standards for facility contracts and entities that provide 'financialised functions' for non-financial product tokens (ie, entities that conduct token trading, staking, asset tokenisation and funding tokenisation). The consultation closed on 1 December 2023 and draft legislation is expected in 2024.

From a regulatory guidance perspective, ASIC has released *Information Sheet 255 Crypto-assets* (INFO 225) to assist businesses involved with cryptocurrency or providing cryptocurrency-adjacent services. INFO 225 covers regulatory considerations for cryptocurrency offerings, misleading and deceptive conduct, trading platforms and cryptocurrency offered via a regulated investment vehicle.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

The provision of payment services is regulated by ASIC, APRA, the RBA and AUSTRAC under certain regulatory regimes as set out in Question 1.

Financial services

Under the financial services regulatory regime, a facility through which (or through the acquisition of which) a person makes a non-cash payment (ie, other than through the delivery of physical currency) (NCP) is a financial product (NCP facility). When delivering payment services, the provider will generally be dealing in the NCP facility and providing advice in respect of the same. Both activities constitute the provision of financial services and require the provider to hold an AFSL or rely on an exemption.

ASIC has outlined numerous AFSL exemptions from this requirement, including NCP-specific exemptions related to gift vouchers and loyalty schemes. Payment services providers often provide these financial services under licensing exemptions which apply when the services are provided on behalf of an AFSL holder.

Whether a digital wallet comprises an NCP facility will largely depend on the functionality of the wallet. A digital wallet may be a part of an NCP facility if it allows users to make payments to a number of payees or enables a payment to be initiated in a digital asset which is converted into fiat to enable completion of the payment.

Banking laws and prudential regulation

Generally, service providers that operate as holders of stored value in relation to purchased payment facilities under the Payment Systems Act are required to be an ADI unless an exemption applies.

A holder of stored value must also apply to the RBA for an authority under the Payments System Act, unless a declaration which exempts the holder applies.

A purchased payment facility is a facility (other than cash) where the same is purchased and can be used to make payments up to the amount available for use under the facility, and the payments are made by the provider or a person acting under an arrangement with the provider, rather than the user of the facility.

A digital wallet may constitute a purchased payment facility. This is possible where the digital wallet also allows deposits of fiat currency and the provider of the facility is the holder of stored value.

AML/CTF

Many payment service providers also provide a designated service under the AML/CTF Act through a designated remittance arrangement. A designated remittance arrangement is where an instruction is accepted for the transfer of money or property, or where money or property is made available or arranged to be made available. Property includes digital assets (but not digital currency). Payment providers that provide designated services and have a geographical link to Australia must enrol and register with AUSTRAC before providing those services and comply with various AML/CTF obligations. AML/CTF obligations include adopting and implementing a risk-based AML/CTF program, undertaking 'know your client' due diligence on their customers and complying with various reporting requirements.

Upcoming reform

In parallel with the release of the Strategic Plan noted in Question 1, the Government released a consultation that proposes a tiered, risk-based licensing framework to be incorporated in the existing financial services regime. Regulation will be based on the relevant payment function provided, with corresponding regulatory obligations balanced against the level of risk posed to end customers. The consultation proposes to regulate two main payments categories: stored value facilities (SVF) and payment facilitation services (PFS), which are further broken down into seven defined payment functions.

On 8 December 2023, the Treasury released a second consultation paper proposing AFSL requirement and corresponding obligations for PSPs. The consultation paper proposes to replace the financial product definition of a 'non cash payment facility' with a new 'payment product' definition and inserts a new type of financial service, being a 'payment service', to be regulated under the financial services regime. The consultation paper also proposes introducing a range of exemptions from the requirement to hold an AFSL for certain types of products and PSPs. The consultation closed on 2 February 2024, with draft legislation expected to follow. The requirement for captured PSPs to hold an AFSL are expected to be enforced 18 months after the passage of legislation.

At the time of writing, buy-now pay later (BNPL) service providers are (only) required to comply with the product design and distribution obligations (DDO) under the Corporations Act. The DDO impose disclosure, reporting and product governance obligations on product issuers and distributors. BNPL providers are also able to voluntarily subscribe to the Australian Financial

Industry Association's BNPL Code of Practice which was developed in conjunction with the BNPL industry. The BNPL Code of Practice is not law and is not enforceable by regulators.

Following public consultation, on 22 May 2023 the government announced its plan to regulate the BNPL industry. BNPL providers will be required to obtain an ACL and comply with a reduced set of obligations under the Credit Act, including in relation to responsible lending, dispute resolution and hardship. On 12 March 2024, the Treasury commenced a further consultation with the release of draft legislation containing proposals to regulate certain BNPL arrangements as 'low cost credit contracts' under the existing regulatory regime for consumer credit products. The consultation closed on 9 April 2024 and draft legislation is expected by the end of 2024.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

ASIC and AUSTRAC have established 'innovation hubs' designed to assist fintech businesses in understanding their obligations under Australian law.

The ASIC innovation hub is designed to foster innovation that could benefit consumers by helping Australian fintech startups navigate the Australian regulatory system. The Innovation Hub provides tailored information and access to informal assistance intended to streamline the AFSL application process for innovative fintech startups.

AUSTRAC's Fintel Alliance has an innovation hub targeted at combatting money laundering and terrorism financing, and improving the fintech sector's relationship with the government and regulators. The innovation hub also assesses the impact of emerging technologies such as blockchain and crypto assets.

Since 2016, ASIC has made certain legislative instruments establishing a fintech licensing exemption which allows fintech businesses to test certain financial services, financial products and credit activities without holding an AFSL or ACL by relying on the legislative instrument (referred to as the regulatory sandbox). Since September 2020, this has been further developed into an enhanced regulatory sandbox, which allows testing for a broader range of financial services and credit activities for up to two years. There are strict eligibility requirements for both the type of businesses that can enter the regulatory sandbox and the products and services that qualify for the licensing exemption. There are restrictions on how many people can be provided with a financial product or service, and caps on the value of the financial products or services which can be provided.

Regulators in Australia have been generally receptive to the entrance of fintechs and technology-focused businesses. The financial services regulatory regime adopts a technology-neutral approach, whereby services will be regulated equally, irrespective of the method of delivery. However, further concessions have been made by regulators in order to support technology-focused startups entering the market.

ASIC has also entered into a number of cooperation agreements with overseas regulators under which there is a cross-sharing of information on fintech market trends, encouraging referrals of

fintech companies and sharing insights from proofs of concepts and innovation competitions. It is also the intention of a number of these agreements to further understand the approach to regulation of fintech businesses in other jurisdictions, in an attempt to better align the treatment of these businesses across jurisdictions.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

On 12 August 2019, the Treasury Laws Amendment (Consumer Data Right) Act 2019 (Cth) (CDR Act) amended the Competition Act, the Privacy Act and the Australian Information Commissioner Act 2010 (Cth) (AIC Act) to establish the Consumer Data Right (CDR).

The CDR gives customers a right to require banks and other data holders to share their data with accredited service providers (including banks, comparison services, fintechs or third parties), encouraging the flow of information in the economy and competition within the market. The CDR also contemplates the introduction of action initiation which would allow accredited data recipients to transact and transfer accounts on the customer's behalf. Accredited data recipients are accredited by the ACCC to receive consumer data to provide a product or service.

The CDR framework is being rolled out across a number of economic sectors as determined by the Minister. Each designated sector will be subject to the Competition and Consumer (Consumer Data Right) Rules 2020 (Cth) (CDR Rules) and technical data standards for that sector as made by the ACCC and Data Standards Chair respectively. Consumers will be able to exercise greater access and control over their data. These data sharing arrangements are intended to facilitate easier swapping of service providers, enhancement of customer experience based on personal and aggregated data, and more personalised offerings.

The banking sector was the first sector to be designated under the open banking regime. The CDR rules for data sharing in the banking sector came into force on 6 February 2020, and consumers were able to consent to their bank sharing data with accredited data recipients from July 2020.

The open banking regime has been implemented in a phased approach, having regard to both the types of banking entities and the products they offer. From 1 July 2022, individual Australian bank customers can allow accredited third parties to access data across a full suite of banking products. The major ADIs must also facilitate data shared by business consumers, partnerships, and secondary users and joint accounts, with non-major ADIs required to deliver the same from 1 November 2022. The intention to implement action initiation in open banking has been confirmed by the Inquiry into Future Directions for the CDR. However, there has not been a designation or legislative change to require banks or other data holders to allow accredited data recipients action initiation.

On 25 August 2023, the government commenced two consultations which propose changes to the CDR Rules, including in relation to consent requirements and operational improvements. The proposals include expanding the CDR to the non-bank lenders sector. Both consultations closed on 6 October 2023.

China

Laurence Yuan*
Fangda Partners, Hong Kong
laurence.yuan@fangdalaw.com

Jason Zhao†
Fangda Partners, Shanghai
jason.zhao@fangdalaw.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

One principle of fintech regulation in the People's Republic of China (China or the PRC)[1] is that all financial business should operate on a licensed basis. Therefore, fintech and any financial innovation (depending on the nature of financial services involved) are also subject to numerous existing laws and regulations that apply to the traditional financial sector, such as those in relation to banking, securities, funds, insurances, trusts and foreign exchanges, etc. Meanwhile, the People's Bank of China (PBOC – the central bank of the PRC), together with various other PRC authorities, has been introducing specific rules and regulations in respect of the fintech industry.

China's current fintech regulations can be understood in two ways: one is from the perspective of the regulated subjects, while the other categorises the types of financial business – current fintech-specific regulations cover a wide range of financial businesses such as mobile payment, online banking, online lending, online insurance, asset management, credit references, crypto assets, crowdfunding, etc.

Key regulations, organised by the regulated subjects

Financial holding companies

The Interim Measures for the Supervision and Administration of Financial Holding Companies (金融控股公司监督管理试行办法) were issued by PBOC on 11 September 2020. The companies that meet the criteria as a financial holding company (through equity investment in financial institutions or otherwise) must apply for the relevant financial licence and be fully supervised by the financial regulators. The measures also impose detailed requirements on sufficiency of capital, risk management systems and corporate governance of financial holding companies.

---

* Laurence works at Fangda's Hong Kong office and is admitted to practice in Hong Kong, the PRC and New York. He specialises in banking and distributed ledger technology (blockchain). Laurence is a pioneering lawyer in blockchain in the greater China region. He has been providing blockchain-related legal service since 2016. Laurence has gained vast experience in the area and built up good connections with the cryptocurrency/blockchain technology community in the region.

† Jason works at Fangda's Shanghai office and is admitted to practice in the PRC. He specialises in banking and financing, debt restructuring and regulatory matters for financial institutions. Jason has been working at Fangda since 2015 and has advised various financial institutions and corporate clients on their compliance and regulatory issues as well as fintech-related transactions, including the cross-border debt restructuring of a cryptocurrency lending company based offshore. Jason has been closely following the development of fintech regulation in China.

1 Answers to the questions here are based on the laws, regulations and rules of the People's Republic of China (for the purpose of these answers only, not including those of Hong Kong, Macau or Taiwan).

Internet platforms

The Guidelines of the Anti-monopoly Commission of the State Council for Anti-Monopoly in the Field of Platform Economy (国务院反垄断委员会关于平台经济领域的反垄断指南) were issued on 7 February 2021 for the purpose of preventing and curbing monopolistic conducts in the field of internet platform economy.

Regarding payment services in particular, on 20 January 2021, PBOC circulated an exposure draft of Regulations on Non-Bank Payment Institutions (非银行支付机构条例) which, among other things, strengthened PBOC's power to supervise the digital payment sector through robust antitrust enforcement. See more in Question 3.

Personal data protection

The Law of the People's Republic of China on Personal Information Protection (中华人民共和国个人信息保护法), which came into effect on 1 November 2021 (Personal Information Protection Law) is the fundamental law in the field of personal information protection covering the full lifecycle of personal data in the PRC.

In addition, PBOC issued a preliminary draft of Interim Measures on Protection of Personal Financial Information (Data) (个人金融信息（数据）保护试行办法) in late 2019 for comments from banks. The draft addresses issues in collection, processing, use and provision of personal financial information by financial institutions.

The Law of the People's Republic of China on Cybersecurity (中华人民共和国网络安全法), which came into effect upon 1 June 2017 (Cybersecurity Law, with an exposure draft of its amendment recently circulated on 12 September 2022) provides that network operators must only collect or use personal data based on the principles of legality, legitimacy and necessity, and must obtain the data subject's consent to do so.

As an important supplement to the Cybersecurity Law, national standards such as the Personal Information Protection Specifications (GB/T 35273) and the Personal Financial Information Protection Technical Specification (JR/T0171-2020) provide detailed recommendations for financial companies to follow.

The Law of the People's Republic of China on Data Security (中华人民共和国数据安全法) which came into effect on 1 September 2021 (Data Security Law) aims to regulate data activities from the perspective of national security and to formulate a tiered data security system echoing the multiple-level protection schemes of the Cybersecurity Law. As fintechs typically rely heavily on personal data to develop their businesses, such as through precision marketing, online ads and personal profiling, such data protection laws and regulations mentioned above can potentially apply to most fintech businesses.

Consumer protection

The Implementation Measures of the People's Bank of China for Protecting Financial Consumers' Rights and Interests (中国人民银行金融消费者权益保护实施办法) were issued by PBOC on 15 September 2020, which substantially increases the cost of financial institutions that infringe on financial consumers' rights.

The Administrative Measures for Protection of Consumers Rights and Interests by Banking and Insurance Institutions (银行保险机构消费者权益保护管理办法) were issued by CBIRC on 12 December 2022 and came into effect upon 1 March 2023, which is the basic regulation in respect of consumer rights protection in the banking and insurance industry, with a dedicated chapter on protection of consumers' personal information.

Key regulations, organised by the types of financial business

Payment services

The Administrative Measures on Payment Services Provided by Non-financial Institutions (非金融机构支付服务管理办法) were issued by PBOC on 14 June 2010, and the exposure draft of Regulations on Non-Bank Payment Institutions (非银行支付机构条例) was circulated by PBOC on 20 January 2021. See more in Question 3.

Online lending

The Guidance on Transformation of Online Lending Information Intermediaries into Microlending Companies on a Trial Basis (关于网络借贷信息中介机构转型为小额贷款公司试点的指导意见) was issued in November 2019. As peer-to-peer (P2P) lending is essentially prohibited in the PRC, intermediaries like P2P lending platforms are encouraged to be transformed into microlending companies pursuant to this guidance.

In addition, on 2 November 2020, PBOC and the China Banking and Insurance Regulatory Commission (CBIRC) jointly issued an exposure draft of the Interim Measures for the Administration of Online Microlending Business (网络小额贷款业务管理暂行办法) which aimed to subject microlending business to regulation by reference to bank loans.

Online microlending business refers to the businesses that use technical means (such as big data, cloud computing, mobile internet, etc) and data accumulated via internet platforms to analyse and assess the credit risk of borrowers, determine the method and amount of loans and conduct the loan-related process online.

Online banking

The Interim Measures for Administration of Internet Lending by Commercial Banks (商业银行互联网贷款管理暂行办法), promulgated by CBIRC on 12 July 2020, provides that banks shall have their own risk control decision models even using third-party network platforms.

The Notice on Issues Concerning Regulating Personal Deposit Services Provided by Commercial Banks on the Internet (关于规范商业银行通过互联网开展个人存款业务有关事项的通知), announced by CBIRC and PBOC on 13 January 2021, provides that commercial banks shall not violate or circumvent regulatory requirements by means of the internet, and shall not carry out fixed deposit business or fixed & call deposit business through third-party network platforms.

The Notice on Further Regulating the Internet Loan Business of Commercial Banks (关于进一步规范商业银行互联网贷款业务的通知), issued by CBIRC on 19 February 2021 sets out the regulatory requirements for the proportion of capital contribution where commercial banks and their partner institutions jointly fund the loans.

Online insurance

The Measures for Administration of Internet Insurance Business (互联网保险业务监管办法), promulgated by CBIRC on 7 December2020, emphasises that internet insurance business shall be carried out by duly established insurance institutions.

Insurance companies and brokers must be CBIRC-licensed to carry out their business. They are allowed to conduct internet insurance business on their own online platforms or through third-party online platforms. Individual insurance agents and other types of sideline insurance agents remain prohibited from conducting internet insurance business.

Credit references and credit information services

The Measures for Administration of Credit Reporting Business (征信业务管理办法) issued by PBOC on 27 September 2021, defines 'credit information' and delineates the boundaries of regulation on credit reporting business.

According to the measures, providers of corporate credit information services are subject to filing requirements with PBOC, while the providers of personal credit information services are subject to prior approval from PBOC and stricter qualification requirements; financial institutions shall not obtain services from unqualified credit service providers.

Investment/asset management

The Guiding Opinions on Regulating Asset Management Business of Financial Institutions (关于规范金融机构资产管理业务的指导意见) jointly formulated by PBOC, CBIRC, the China Securities Regulatory Commission (CSRC) and the State Administration of Foreign Exchange (SAFE) on 27 April 2018 (the AMB Opinions), are the first rules related to robo-advisers in the PRC.

The AMB Opinions require an investment adviser to have appropriate qualifications when using artificial intelligence technology to carry out investment advice business. Non-financial institutions cannot use robo-advisers to carry out asset management business beyond their business scope or carry out such business in disguised forms. Financial institutions that use artificial intelligence technology to carry out asset management business must strictly follow the general provisions under the AMB Opinions on (1) investor appropriateness; (2) investment scope; (3) information disclosure; and (4) risk isolation.

In addition, depending on the product investment strategy, such institutions must study and develop corresponding artificial intelligence algorithms or programmatic transactions in order to avoid homogenisation of the algorithm, and must formulate responsive plans for market fluctuation risks that may arise because of these factors. If artificial intelligence algorithm model defects or system abnormalities

affect the stable operation of the financial market, financial institutions must promptly adopt manual intervention measures to force adjustments or terminate relevant business.

The Guiding Opinions on Further Regulating the Services Relating to Internet Sales and Redemption of Money Market Funds (关于进一步规范货币市场基金互联网销售、赎回相关服务的指导意见), issued on 30 May 2018 by PBOC and CSRC (the MMF Opinions), provides that:

- non-licensed institutions are strictly prohibited from carrying out fund sales activities;
- except for commercial banks qualified for fund sales, other institutions or individuals are prohibited from providing advances for 'T+0 redemption and withdrawal' business in any way; and
- non-bank payment institutions are not allowed to provide value-added services to direct payment with shares of money market funds and are not allowed to engage in sales of money market funds.

Crowdfunding

The Guideline Opinion on Promoting the Healthy Development of Internet Finance (关于促进互联网金融健康发展的指导意见), jointly issued by PBOC, CSRC, CBIRC and several other PRC authorities on 18 July 2015, has defined equity-based crowdfunding as public equity financing in small amounts through an internet-based platform. The opinion provides that equity crowdfunding shall be conducted through an agency platform such as a website or other digital medium, and that the CSRC will be the regulatory authority for equity crowdfunding business.

On 3 August 2015, CSRC published a Notice on Special Inspection of Institutions Carrying Out Equity Financing Activities through the Internet (关于对通过互联网开展股权融资活动的机构进行专项检查的通知), which clarifies that equity-based crowdfunding is an open and public equity offering for a small amount and shall not be conducted unless with prior regulatory approval.

On 14 April 2016, CSRC issued an Action Plan for the Special Rectification of Risks in Equity Crowdfunding (股权众筹风险专项整治工作实施方案), prohibiting internet equity financing platforms from public offering of securities or establishing private equity funds in the name of 'equity crowdfunding'. To date, there is no regulation specifically addressing crowdfunding financing in the PRC.

Crypto assets

See Question 2.

Government initiatives supporting fintech

See Question 4.

Open banking

See Question 5.

In addition to the above, fintech development plans issued by the PBOC every couple of years, as the roadmap for China's development of fintech and financial innovation in the given period, are also of good reference value as they often indicate how the government will administer or guide the development of the sector.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

There is no specific law or regulation regarding crypto assets in the PRC. Several 'ministry notices/announcements' issued by various PRC authorities (mainly ministries/departments under the State Council) constitute the most important legal source in the PRC with respect to crypto assets (or cryptocurrencies). At the same time, crypto assets transactions are subject to numerous PRC laws of general application, such as the PRC Civil Code and the PRC Criminal Law.

China's current regulatory stance on cryptocurrencies, as reflected in the 'ministry notices/announcements', is a comprehensive crackdown. Crypto assets do not have the legal status as fiat currencies and cannot be circulated and used in the market as such in the PRC. The following cryptocurrency-related activities are strictly prohibited:

- exchanging between currencies and cryptocurrencies or between different cryptocurrencies;
- trading cryptocurrencies as a central counterparty;
- providing intermediary services or pricing services for cryptocurrency transactions;
- fundraising via initial coin offerings (ICO); and
- cryptocurrency-related derivatives trading.

The blanket ban is also applicable to offshore cryptocurrency exchanges offering services to PRC residents via the internet. Onshore entities and individuals are prohibited from supporting cryptocurrency transactions or providing relevant services, especially banks, payment institutions, and internet platforms. Crypto mining has also been banned recently in the PRC.

Regarding crypto assets-related transactions, according to the Notice on Further Preventing and Handling the Risk of Speculation in Virtual Currency Transactions (关于进一步防范和处置虚拟货币交易炒作风险的通知) jointly issued by PBOC, the Supreme People's Court, the Supreme People's Procuratorate, the Ministry of Public Security, SAFE and other authorities of the PRC on 15 September 2021, any investment into cryptocurrencies or relevant derivatives that contravenes the public order or good social morals has no legal effect, and any losses incurred as a result will not be remedied. It further provides that if such investment could potentially disturb the financial order or endanger financial security, the people involved may be subject to relevant administrative or even criminal liabilities. In judicial practice, the PRC courts seem not hesitant in finding cryptocurrency transactions (typically cryptocurrency-related investments) void or unlawful, though they are divided on how to address or enforce the parties' resulting losses or claims and have manifested large discretion case by case. That said, the PRC courts generally acknowledge property rights in crypto assets. In some cases, crypto assets could be protected in the PRC as property with economic value.

In addition, certain cryptocurrency transactions may even constitute crimes under the PRC Criminal Law. Criminal charges under the PRC Criminal Law commonly associated with cryptocurrency transactions include (1) illegally absorbing public deposits, (2) fundraising fraud, (3) illegal business operations, (4) organising or leading pyramid schemes, and (5) money laundering, etc. If held as a crime, the punishments for the crime will include fines and imprisonment for several years.

With the blockchain technology commonly used for crypto assets, PBOC has also issued 'Digital CNY' as the lawful digital form of CNY, but it remains subject to centralised management of PBOC and is still in the trial phase. The exposure draft of the amended Law of the People's Republic of China on the People's Bank of China (中华人民共和国中国人民银行法) circulated on 23 October 2020, stipulates that CNY includes both physical and digital forms, intending to provide the legal basis for issuing Digital CNY.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

In the PRC, payment services by non-financial institutions (payment services providers) are primarily regulated by PBOC under the Administrative Measures on Payment Services Provided by Non-financial Institutions (非金融机构支付服务管理办法) and its implementation rules and affiliated regulations.

Payment services by non-financial institutions is defined as fund transfer services provided by them as the intermediary between the payer and the payee, which are categorised as follows:

- payments through networks;
- issuance and acceptance of prepaid cards;
- acceptance of bank card payments (ie collection of funds for the franchised merchants via POS terminals, etc); and
- other payment services as specified by PBOC.

A payment service provider is required to obtain a licence from PBOC in order to provide payment services. On 13 April 2016, PBOC issued the Implementation Plan of Special Risk Remediation for Non-bank Payment Institutions (非银行支付机构风险专项整治工作实施方案), stating that PBOC would, in principle, no longer accept applications for the establishment of new payment institutions.

Under PBOC's current regulatory regime, payment services providers are regulated in a similar way as banks. In particular, they must:

- deposit customer reserve funds in accounts with PBOC or qualified commercial banks held in escrow in order to protect the funds;
- establish a sound client identification system under know your customer (KYC) guidelines; and
- not engage in business such as securities, insurance, financing, trust, wealth management, currency exchange or withdrawal services.

On 20 January 2021, PBOC circulated an exposure draft of the Regulations on Non-Bank Payment Institutions (非银行支付机构条例), aiming to replace the current administrative measures issued over 10 years ago and strengthen its supervision over payment institutions in several respects. In respect of the antitrust issue that has been hotly debated in recent years, the regulations set the thresholds in terms of market share that trigger PBOC's consultation with antitrust authorities on whether to give a warning to or to verify the dominant market position of the payment institution. In addition, PBOC may recommend antitrust authorities intervene and stop abusive practices or implementation of concentrations or, where there is an adverse impact on market competition, even to split such institutions. Once enacted, these measures will strengthen PBOC's power to supervise the digital payment sector through robust antitrust enforcement.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

The operation of the 'regulatory sandbox' in the PRC is still in the trial stage. Following the release of the Fintech Development Plan (2019–2021), PBOC has rolled out a number of initiatives to promote a safe environment for fintech innovation, aiming to transform financial regulatory compliance from reactive to proactive. Fintech pilot sandbox projects were kicked off in Beijing in December 2019 and were further extended to Shanghai, Chongqing, Shenzhen, Hangzhou, Suzhou and Xiong'an New District in April 2020.

In April 2020, PBOC, CBIRC, CSRC and SAFE jointly issued their Opinions on Financial Support for Development of the Guangdong–Hong Kong–Macao Greater Bay Area (关于金融支持粤港澳大湾区建设的意见) where a mechanism to 'study and establish a cross-border financial innovation regulatory sandbox' was proposed and the concept of 'sandbox regulation' was expressly mentioned. These sandboxes test regulatory approaches in a centralised manner, aiming to find the right balance between innovation and regulation. Credit, operation management and payment services are the key areas covered by the sandbox regulation.

In October 2021, PBOC and the Hong Kong Monetary Authority entered into a Memorandum of Understanding on Fintech Innovation Supervisory Cooperation in the Guangdong–Hong Kong–Macao Greater Bay Area (关于在粤港澳大湾区开展金融科技创新监管合作的谅解备忘录). The two authorities agreed to link up the PBOC's Fintech Innovation Regulatory Facility with the HKMA's Fintech Supervisory Sandbox in the form of a 'network'. Initiatives under this cross-border regulatory sandbox could include cross-border market access mirroring the EU 'single passport' regime, and promoting capital account convertibility utilising Digital CNY.

At the local level, cities including Beijing, Shanghai, Shenzhen and Hangzhou have introduced their own policies supporting and encouraging local development of fintech industry, offering tax incentives, simplified administrative procedures and even cash rewards.

Also, the recent Fintech Development Plan (2022–2025) by PBOC sets out goals in relation to supporting the fintech ecosystem, including:

- fostering an open and innovative industrial ecosystem;
- bringing in cutting-edge technologies and advance management experiences;
- building an agile innovation system by exploring flat and network management models; and
- exploring and promoting new innovation models, such as digital factories and innovation labs.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

Currently, there are no specific regulations for open banking in the PRC. The PRC does not have an open banking law like the European model developed in the recent years. However, in practice, many banks in the PRC have been making attempts at open banking.

Regarding the open bankers to which data protection laws apply (see Question 1) and the following technical standards, the most relevant are:

1. Specifications for Security Administration of Commercial Banks' Application Program Interface (商业银行应用程序接口安全管理规范), which refines security assurance techniques and requirements of the different types, security levels, design, deployment, integration, operation and maintenance, etc, of bank interfaces, providing clear technical standards for open banking.
2. Technical Specifications for Protection of Personal Financial Information (个人金融信息保护技术规范), which specifies the security protection requirements for collection, transmission, storage, use, deletion and destruction, etc of personal financial information.

Moreover, the FinTech Development Plan (2019–2021) has expressed support for cross-business cooperation on a compliant basis through application programming interfaces (APIs) and software development kits (SDKs), etc, integrating and deconstructing financial business and encapsulating modules that can be combined and applied in different scenarios, thereby establishing new business paradigms and building up an open, cooperative and win-win financial service ecosystem.

Hong Kong

Laurence Yuan*
Fangda Partners, Hong Kong
laurence.yuan@fangdalaw.com

Cecilia Li†
Fangda Partners, Hong Kong
Cecilia.Li@fangdalaw.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

Currently, there is no specific regulatory framework for fintech and financial innovation in Hong Kong. Fintech businesses are however subject to the existing laws and regulations in Hong Kong relating to financial activities. The relevant regulatory regimes are summarised as follows.

Securities and Futures Ordinance (SFO)

Fintech companies which carry out 'regulated activities' in Hong Kong need to be licensed by, or registered with, the Securities and Futures Commission (SFC) unless there is an exemption. Under the SFO, 'regulated activities' include, among others, dealing in securities or future contracts, advising on securities, future contracts or corporate finance, providing automated trading services and asset management. Fintech companies should consider whether their business activities fall within the definition of 'regulated activities' under the SFO. (Please also see Question 2 relating to the implication of the SFO on crypto assets.)

Companies (Winding Up and Miscellaneous Provisions) Ordinance (CWUMPO)

Unless an exemption applies, a document offering shares in, debentures of, a company, or securities to, the public is subject to prospectus registrations under CWUMPO as well as the authorisation requirements under the SFO. Fintech companies should evaluate whether their business activities would trigger any obligations under CWUMPO or the SFO.

Banking Ordinance (BO)

The BO provides that:

---

* Laurence works at Fangda's Hong Kong office and is admitted to practice in Hong Kong, the PRC and New York. He specialises in banking and distributed ledger technology (blockchain). Laurence is a pioneering lawyer in blockchain in the greater China region. He has been providing blockchain-related legal service since 2016. Laurence has gained vast experience in the area and built up good connections with the crypto currency/blockchain technology community in the region.

† Cecilia works at Fangda's Hong Kong. She specialises in banking and distributed ledger technology (blockchain).

- no person shall act as a 'money broker', being an entity that negotiates, arranges or facilitates the entry by clients into arrangement with banks, unless approved by the Hong Kong Monetary Authority (HKMA);
- no 'banking business' (which includes receiving from the general public money on current, deposit, savings or other similar accounts repayable on demand or within less than a specific period) shall be carried out in Hong Kong except by a licensed bank; and
- no business of taking deposits can be carried on in Hong Kong except by an authorised institution.

Fintech companies should evaluate whether their business activities fall under the ambit of the BO.

Money Lenders Ordinance (MLO)

The MLO provides that a 'money lender', being a person whose business is that of making loans or who holds themselves out in any way as carrying on such a business, requires a money lender licence unless there is an exemption. Such licensed money lenders must also comply with the licensing conditions and requirements which are set out in the MLO. Fintech companies should evaluate whether their business activities fall under the ambit of the MLO.

Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO)

The AMLO imposes customer due diligence and record keeping obligations on financial institutions.

Under the AMLO, any person operating a 'money service' requires a money service operator licence.

The definition of 'money service' includes (1) a service for exchanging currencies that is operated in Hong Kong as a business and (2) a service for sending money to a place outside Hong Kong, receiving money from outside Hong Kong or arranging for the receipt of money outside Hong Kong.

Fintech companies should evaluate whether their business activities would trigger any obligations under the AMLO. Please also see Question 2 below in relation to the amendment to the AMLO.

Payment Systems and Store Value Facilities Ordinance (PSSVFO)

PSSVGO provides a licensing regime for the issue of 'stored value facilities'. This licensing regime covers both device-based and network-based facilities. Under the PSSVFO, 'stored value facilities' are facilities which can be used to store the value of an amount of money that is paid into the facility from time to time as a means of making payment for goods and services. Fintech companies should evaluate whether their business activities fall under the ambit of the PSSVFO.

Insurance Ordinance (IO)

The IO provides that no person shall carry on any class of insurance business in or from Hong Kong unless authorised to do so. Fintech companies should evaluate whether their businesses fall under the ambit of the IO.

Competition Ordinance (CO)

The CO prohibits certain behaviours which harm competition in Hong Kong. Fintech companies should consider whether their business operations comply with the requirements set out in the CO.

Personal Data Privacy Ordinance (PDPO)

Fintech companies which are 'data users' – being persons who control the collection, holding, processing and use of personal data in Hong Kong – are regulated by the PDPO and should be aware of the data protection requirements in Hong Kong.

Organised and Serious Crime Ordinance (OSCO)

The OSCO provides a universal obligation to report suspicious transactions in relation to suspected or known crime proceeds.

Drug Trafficking (Recovery of Proceeds) Ordinance (DTROP)

The DTROP establishes offences relating to the proceeds of drug trafficking which will be applicable to all businesses (including fintech businesses).

United Nations (Anti-Terrorism Measures) Ordinance (UNATMO)

The UNATMO establishes offences related to specified terrorist property which will be applicable to all businesses (including fintech businesses).

United Nations Sanctions Ordinance (UNSO)

The UNSO implements United Nations sanctions which will be applicable to all businesses (including fintech businesses).

2. Regulations on virtual assets: a dual licensing regime.

The amended Hong Kong Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO) defines virtual assets (VA) as cryptographically secured digital representations of value, but the definition excludes tokens that constitute securities and futures contracts, thus marking a difference between virtual assets (which are not securities) and tokenised securities (which are considered securities under the existing SFO).

Following the amendments to the AMLO in December 2022 (effective on 1 June 2023), Hong Kong now has a dual licensing regime for cryptocurrency: the new VASP regime in respect of non-security tokens and the existing SFO regime with respect to security tokens. As a new regime, the VASP regime only applies to virtual assets trading platforms (VATPs), but not other VA related services.

The object of the new VASP licensing regime is to fill in the regulatory gaps in the regulations of cryptocurrency trading. Previously, only centralised platforms providing trading services for security tokens were regulated by the SFC under the SFO, resulting in the trading of non-security tokens falling outside the SFC's purview. With the new VASP licensing regime coming into effect, trading of non-security tokens is now also subject to regulation.

The new VASP regime operates in parallel with the existing SFO regime: ie, platforms trading security tokens will be regulated under the SFO, while those trading non-security tokens will fall under the VASP regime. Notwithstanding the differentiation between security and non-security tokens, the SFC encourages platforms to apply for dual licences under both regimes to ensure business continuity and to avoid potential licensing non-compliance issues, given that the nature and characteristics of a virtual asset may evolve over time, resulting in changes to its classification (eg, from a non-security to security token or vice versa).

Key aspects of the new VASP licensing regime

The SFC is the key regulator for VASPs. With the amendments to the AMLO, the SFC was granted additional supervisory powers over the VASPs with respect to their businesses involving the non-security tokens, in addition to their existing supervision powers over security tokens or other virtual assets deemed 'securities' and their associated 'regulated activities' under the existing SFO regime.

Under the new VASP regime, a person needs to obtain an SFC licence if (1) it carries on, or holds out as carrying on, a business of providing any virtual asset service (ie, operating a virtual asset exchange) (VA Service) in Hong Kong, or if (2) it actively markets any VA Service to the public of Hong Kong (whether in Hong Kong or elsewhere). Non-compliance with the licensing requirements will lead to monetary and criminal sanctions. It is also noteworthy that the new AMLO introduces new criminal offences for fraudulent activities involving virtual assets which apply to any person, rather than just VASPs.

As part of VASPs, VATP operators must also comply with the Guidelines for Virtual Asset Trading Platform Operators (VATP Guidelines) published by the SFC, which provides for the important criteria that platform operators must meet, from the establishment requirements (fitness and properness, competency, and financial soundness) to the ongoing obligations (in areas such as client take-on procedures, information disclosure, custody of client assets, due diligence, cybersecurity, operational controls, recordkeeping and auditing, etc).

While the SFC limits the trading of the derivatives of virtual assets to institutional investors, it allows licensed VATPs to offer trading services of certain virtual assets to retail investors, subject to a range of additional investor protection requirements covering onboarding, governance, disclosure, token due diligence and admission criteria.

- *Onboarding*: VATP operators should assess whether it is suitable for a client to trade virtual assets by assessing a client's risk tolerance, and their understanding of the nature and risks of virtual assets. Similar assessments also apply to intermediaries engaging in virtual asset- related activites.
- *Governance*: VATP operators shall establish a token admission and review committee.

- *Disclosure*: when publishing any information or materials on its platform or providing information to clients, a VATP operator must exercise due skill, care and diligence, and ensure all information is accurate and presented in an easily comprehensible manner.
- *Token due diligence and admission criteria*: The VATP Guidelines provide for a non-exhaustive list of factors for VATP operators to consider when admitting virtual assets for trading. For special tokens to be offered to retail investors, the VATP operators must ensure the virtual assets are an eligible large-cap virtual asset (ie, the virtual assets are included in at least two acceptable indices issued by separate index providers which are independent of the VA issuers and the VATP operator).

The SFC clarified that stablecoins will not be permitted for retail trading until they are subject to regulation in Hong Kong. The HKMA concluded the public consultation on the proposed stablecoin regulation earlier in 2024 but the specific timetable for the proposed regulation has not been provided. We will discuss the proposed stablecoin regime in the later part of this Question.

Certain activities by VATPs are prohibited under the VATP licensing regime, such as establishing arrangements that generate returns for clients through the use of client virtual assets (eg, staking products), or permitting third-party custodians to hold client assets. The client assets must be held by a wholly owned subsidiary of the licensed VATP.

The VATP Guidelines also require VATP operators to establish compensation arrangements covering 50 per cent of client virtual assets held in cold storage and 100 per cent of client virtual assets held in hot and other storages kept by the VATP and its associated entities. The compensation arrangement should include any or a combination of (1) third party insurance, (2) funds or VAs of the VATP operator or a corporation within its group put into trust specially for the required compensation, and (3) bank guarantees provided by an authorised financial institution in Hong Kong.

The new Chapter 12 of the AMLO sets out VA-specific AML/CFT requirements governing the conduct of VASPs and associated entities when carrying out activities associated with VA or businesses which give rise to money laundering and terrorist financing risk in relation to VAs. The VA-specific AML/CFT requirements cover areas like:

- additional customer due diligence;
- compliance with the 'travel rule' (which requires the licensed VATPs to (1) as the ordering institution, obtain, hold and submit required information about the originator and recipient to the beneficiary institution immediately and securely; and (2) as the beneficiary institution, obtain and hold the required information from the ordering institution);
- conducting counterparty due diligence for VA transfers;
- handling transfers involving unhosted wallets;
- managing cross-border correspondent relationships; and
- screening VA transactions and associated wallet addresses.

There is a transition period for VATPs that provided services prior to the commencement of the VASP regime. To qualify for the transitional arrangements, a VATP must have already been providing virtual asset services with a genuine presence in Hong Kong before 1 June 2023. Note that the

transitional arrangements only apply to the trading of non-security tokens by VATPs. VATPs which aim to provide trading involving security tokens must obtain the required licence(s) from the SFC before commencing the businesses. Deemed eligible platforms for the transitional arrangements can continue to provide its VA service in Hong Kong from 1 June 2023 to 31 May 2024.

Other VA-related activities by financial intermediaries

In addition to regulating VASPs in Hong Kong, the SFC also regulates the VA-related activities conducted by financial intermediaries.

On 20 October 2023, the SFC and the HKMA issued a joint circular on intermediaries' virtual asset-related activities (Circular) for intermediaries (ie, a licensed corporation or a registered institution under the SFO) which intended to engage in VA-related activities, setting out regulatory guidelines for intermediaries to follow when they are:

- distributing VA-related products (VA-related product distribution);
- providing VA-dealing services (VA dealing services);
- providing VA advisory services (VA advisory services); and
- providing VA-related asset management services (VA asset management services).

The 2023 Circular revises a joint circular previously issued by the SFC and the HKMA on 28 January 2022. The 2023 Circular permits the intermediaries to provide more VA-related services to retail investors, subject to compliance with relevant requirements and the enhanced investor protection measures.

VA-related product distribution

- *Selling restrictions*: except for a limited suite of products (those traded on regulated exchanges specified by the SFC), VA-related products that are considered as complex products should only be offered to professional investors.
- *Virtual asset knowledge test*: except for institutional professional investors and qualified corporate professional investors, intermediaries should assess whether clients have knowledge of investing in virtual assets or VA-related products prior to effecting a transaction in VA-related products.

VA dealing services

- *Partner with SFC licensed platforms only*: to ensure sufficient investor protection, the SFC and the HKMA consider it appropriate and necessary to require intermediaries to partner only with SFC-licensed VA trading platforms for the provision of VA dealing services. Since SFC-licensed VATPs are now allowed to service retail clients, the intermediaries are permitted to provide VA dealing services, on an introducing agent or omnibus account basis with the licensed VATPs, to retail investors.

- *Account segregation*: Intermediaries which allow clients to deposit or withdraw virtual assets from their accounts should only receive or withdraw such client virtual assets through the segregated account(s) established and maintained with (1) their partnered licensed VATPs; or (2) authorised financial institutions (or their subsidiaries) which meet the expected standards of VA custody issued by the HKMA from time to time.

VA advisory services

- *High liquidity VAs*: when recommending any virtual assets to retail clients, intermediaries shall take all reasonable steps to ensure that the VA is of high liquidity (and at minimum, an eligible large-cap VA) and made available by VATPs for trading by retail investors.
- *Advising tokenised securities*: intermediaries which provide advisory services in tokenised securities should comply with the existing requirements governing advising on securities and the expected standards of conduct and guidance on tokenised securities issued by the SFC from time to time.

VA asset management services

- *Additional requirements if meeting* de minimis *threshold*: intermediaries providing virtual asset portfolio management or discretionary account management services must adhere to additional requirements if they exceed the *de minimis* threshold (10 per cent or more of the gross asset value of a portfolio in virtual assets) for virtual assest investments. These requirements will be imposed by the SFC (and in consultation with the HKMA, where applicable) as licensing or registration conditions.
- *Cap on percentage of VAs in client's portfolio*: the SFC and the HKMA reiterates that if a Type 1 intermediary is authorised by its clients to provide ancillary VA dealing services on a discretionary basis, the intermediary should only invest less than 10 per cent of the gross asset value (ie, below the *de minimis* threshold) of the client's portfolio in VAs.

Intermediaries wishing to offer VA services following the 2023 Circular should notify the SFC (and the HKMA, if applicable) to start discussions on the services they intend to provide and how they can comply with the requirements in the 2023 Circular.

HKMA's proposed stablecoins regime

On 27 December 2023, the Hong Kong Financial Services and the Treasury Bureau ('FSTB') and the HKMA jointly published a public consultation paper on the legislative proposal for implementing the regulatory regime for stablecoin issuers (the 'Proposal'). The Proposal outlined the FSTB and the HKMA's approach in regulating financial activities with respect to stablecoins.

As a kind of special virtual assets, stablecoins refer to cryptographically-secured digital representations of value that, among other things, aim to maintain a stable value relative to a specified asset, or a pool or basket of assets, such as fiat currencies or commodities. Under the Proposal, the FSTB and the HKMA will initially focus their regulation on fiat-referenced stablecoins (FRS), ie, where the specified asset is one or more fiat currencies, as these stablecoins are more

likely to be used for payment or storage of value, thereby presenting more imminent monetary and financial stability risks than other types of stablecoins or virtual assets. Notably, the FSTB and the HKMA proposed that tokenised deposits, certain securities or futures contracts, float stored in SVFs or SVF deposits, ditigal fiat currencies issued by central banks and digital representation of value that can only be used for payment of goods or services, do not fall under the definition of a 'stablecoin'.

The HKMA's proposed stablecoins scheme encompasses the following key aspects:

- Licensing regime and requirements for FRS issuers:
    - Persons/entities that will require an FRS issuer licence from the HKMA:
        - any person who issues or holds themselves out as issuing an FRS in Hong Kong;
        - any person who issues or holds themselves out as issuing a stablecoin that purports to maintain a stable value with reference to the value of the Hong Kong dollar; or
        - any person who actively markets their issuance of FRS to the public of Hong Kong.
    - In order to be licensed, the FRS issuer must demonstrate that it can meet certain licensing requirements. Key licensing requirements include:
        - management of reserves and stabilisation mechanism: the FRS issuer shall ensure that the value of reserve assets must be at least equal to the par value of the FRS (at a minimum) at all times. Reserve assets must be of high-quality and high-liquidity and be held in the reference currency. FRS issuers must store reserve assets in segregated accounts with licensed banks or other custodians as approved by the HKMA. Regular publication by the FRS issuer of the total amount of FRS in circulation, the value and composition of reserve asset value is mandatory;
        - redemption requirements: FRS users are expected to have the right to redeem their stablecoins at par value and FRS issuers are expected to timely process the redemption requests without undue costs and/or unreasonable conditions;
        - restrictions on business activities: FRS issuers must obtain approval from the HKMA before commencing any new lines of business. However, FRS issuers can conduct activities that are ancillary or incidental to their FRS issuance activities, such as providing wallet services for their own FRS, provided that they have adequate systems for the segregation and safekeep of FRS and handling of deposit and withdrawal requests for FPS. FRS issuers are prohibited from engaging in lending, financial intermediation or other regulated activities;
        - financial resources and governance: an FRS issuer is expected to maintain a minimum paid-up share capital to be HKD 25,000,000 or two per cent of the par value of FRS in circulation, whichever is higher. Controllers, chief executives and directors of an FRS issuer must be fit and proper and their appointment and any changes to their appointment are subject to HKMA approval;
        - risk management and anti-money laundering and counter-financing of terrorism (AML/CFT) requirements: the FRS issuers must implement appropriate risk management

processes and measures, such as adequate security and internal controls, effective fraud monitoring and detection, as well as adequate systems of control for preventing or combatting possible AMT/CFT;

    - physical presence in Hong Kong: an FRS issuer must be a company incorporated in Hong Kong with a registered office in Hong Kong. Key personnel and senior management of the FRS issuer must be based in Hong Kong. They must have effective management and control over FRS issuance and related activities.

- Custody and offering of FRS:
    - regarding the offering of FRS, the FSTB and the HKMA are of the view that FRS issued by unlicensed entities are not suitable for use by the public. As a result, their intention is that only licensed FRS issuers, authorised institutions, licensed corporations and licensed VATPs can offer FRS in Hong Kong or actively market such offerings to the Hong Kong public. Meanwhile, authorised institutions, licensed corporations and licensed VATPs can offer FRS issued by unlicensed entities to professional investors only;
    - regarding the custody of FRS, the FSTB and the HKMA have indicated that they will examine the appropriate regulatory approach for the custody of FRS with relevant stakeholders. Further regulatory guidance on this topic is underway but no specific timeframe for its publication was indicated.

Under the Proposal, all entities would be eligible to apply for an FRS issuer licence as long as they can satisfy the same set of licensing and regulatory requirements. Considering that authorised institutions are already subject to stringent prudential requirements and ongoing holistic supervision by the HKMA, it is proposed that the licensing criteria related to restrictions on business activities, physical presence in Hong Kong and financial resources requirements do not apply to FRS issuers that are authorised institutions.

The public consultation on the Proposal was concluded on 29 February 2024. The HKMA announced on 12 March 2024 the launch of the stablecoin issuer sandbox arrangement. The HKMA wishes to leverage the sandbox arrangement to communicate supervisory expectations to parties interested in issuing FRS in Hong Kong, and to obtain feedback from the sandbox participants on the Proposal. As of now, no timetable for the proposed regulation has been provided. Reference to international standards and the stablecoin regulations of major foreign jurisdictions will also be made when formulating the final regulatory regime.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

HKMA is the main regulatory body for payment systems. In Hong Kong, the major types of payment systems would be retail payment systems (RPS) and stored value facilities (SVF) which are regulated by PSSVFO.

Retail payment systems

The PSSVFO defines an RPS as a system or arrangement for the transfer, clearing or settlement of payment obligations related to retail activities (whether the activities take place in Hong Kong or elsewhere), principally by individuals, that involve purchases or payments; and includes related instruments and procedures. Examples of RPSs may be payment card systems, electronic funds transfer systems, transaction acquiring systems or payment gateways. The PSSVFO stipulates criteria and relevant factors based on which the HKMA may determine whether an RPS should be designated, and the requirements that designated RPSs are required to comply with. The HKMA's Explanatory Note on Designation of Retail Payment Systems explains the relevant policies and procedures adopted by the HKMA with respect to the designation of RPS. So far, the HMA has designated the RPSs operated by Visa, Mastercard, UnionPay International, American Express, Joint Electronic Teller Services Limited (JETCO), and EPS Company (Hong Kong) Limited (EPSCO) for the processing of payment transactions.

Stored value facilities

Digital wallets and prepaid cards, on the other hand, are classified as SVFs under the PSSVFO. SVF covers any facility used for storing monetary value and can be used as a means of payment for goods and services and/or to another person. It is an offence to issue or operate an SVF without a licence. An SVF licence is not required if it is used for the following purposes:

- for certain cash reward schemes;
- for purchasing certain digital products;
- for certain bonus point schemes;
- within limited groups of goods or services providers; and
- within certain premises.

Below are certain criteria to be fulfilled by an applicant applying for an SVF licence:

- the main business must be the issue of SVF under an SVF licence;
- the paid-up share capital of the applicant must be not less than HK$25m;
- each chief executive, director and controller of the applicant must be a fit and proper person;
- the applicant must have in place appropriate risk management policies and procedures for managing the risk arising from the operation of its SVF business;
- the applicant must have in place adequate measures to ensure the confidentiality and integrity of databases and to protect the data privacy of users in compliance with the Personal Data (Privacy) Ordinance;
- the applicant must have in place in the SVF scheme adequate and appropriate systems of control for preventing or combatting possible money laundering or terrorist financing;

- the applicant must have in place adequate risk management policies and procedures for managing the float and SVF deposit to ensure that there will always be sufficient funds for the redemption of the stored value that remains on the facility;
- the applicant must redeem in full the total of the stored value that remains on the facility as soon as practicable after being requested by the user; and
- the operation rules of the SVF scheme must be prudent and sound.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

The regulators in Hong Kong have been active in providing special programmes supporting the fintech ecosystem.

In this regard, HKMA, the SFC and the Insurance Authority (IA) has each set up a regulatory sandbox.

The Fintech Supervisory Sandbox (FSS)

The HKMA has set up a Fintech Supervisory Sandbox which allows banks and their partnering technology companies to conduct pilot trials of their fintech initiatives involving a limited number of participating customers without the need to comply fully with HKMA's supervisory requirements. To date, HKMA has launched several of its own initiatives such as the Faster Payment System and iAM Smart which encourages banks and SVF providers to participate in the fintech ecosystem. HKMA also participated in the Global Financial Innovation Network on cross-border testing of pilot schemes. As mentioned above, the HKMA also plans to roll out a sandbox to facilitate communications of its supervisory expectations with entities that are interested in issuing stablecoins in Hong Kong.

The SFC sandbox

The SFC Regulatory Sandbox invites licensed corporations and startups that wish to carry out a regulated activity under the SFO to operate such regulated activity within a limited scale. All participating companies must be fit and proper, use innovative technologies and be able to demonstrate a genuine and serious commitment to carry on such regulated activity through the use of fintech. The SFC may also impose licensing conditions to limit the scope of a participating company's business or to put in place reporting requirements.

The InsurTech Sandbox

The IA launched the InsurTech Sandbox to facilitate innovative applications of insurance technology. Authorised insurers and licensed insurance brokers may apply for a pilot trial under the InsurTech Sandbox to test new insurtech initiatives and collect market data as well as user experience before making any such technology available to the general market.

It is also worthwhile to note that, in September 2017, the IA launched a fast-track pilot scheme to expedite applications for new authorisations to carry on insurance business in or from Hong Kong using solely digital distribution channels to promote the development of insurance technology in Hong Kong.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

Currently, there are no specific regulations on open banking in Hong Kong. Nonetheless, in July 2018, the HKMA published the Open Application Programming Interface (Open API) Framework which seeks to enable collaboration between banks and third-party service providers (TSP). The Open API Framework adopts the following four-phase approach to implement various Open API functions, and recommends prevailing international technical and security standards to ensure fast and safe adoption:

- Phase I: Production information (deposit rates, credit card offerings, service charges and other public information).
- Phase II: Customer acquisition (new applications for credit cards, loans and other products).
- Phase III: Account information (account balance, credit card outstanding balance, transaction records, credit limit change and others).
- Phase IV: Transactions (payment and transfers).

The banking sector in Hong Kong launched Phases I and II of the Open APIs framework in January 2019 and October 2019 respectively. Furthermore, Phases III and IV of the framework began in December 2021. As of May 2024, of the 28 participating banks, 25 banks have launched the Phase III API functions for retail customers, 23 banks have launched the Phase III API functions for corporate and SME customers and 26 banks have launched the Phase IV API functions.

India

Sajai Singh*[1]
JSA, Bengaluru
sajai@jsalaw.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

Some of the notifications and regulations that relate to financial technology offerings in India are listed below.

Payment aggregators and payment gateways

Intermediaries that facilitate online payments such as payment aggregators are regulated primarily under the Guidelines on Regulation of Payment Aggregators and Payment Gateways 2020 (Guidelines). Payment aggregators are entities that facilitate e-commerce sites and merchants to accept various payment instruments from customers, pools the same and transfers to the merchants after a specific time period.

Payment gateways do not handle any funds on behalf of merchants and provide technology infrastructure to route and facilitate processing of an online payment transaction. The Guidelines are applicable to payment aggregators. Payment gateways may choose to adhere to the baseline technology-related recommendations contained in the Guidelines. Non-bank payment aggregators are required to obtain authorisation from the Reserve Bank of India and are required to be incorporated in India.

Digital lending

On 2 September 2022, the Reserve Bank of India issued the Guidelines on Digital Lending (Guidelines). Digital Lending has been defined as a 'remote and automated lending process, largely by use of seamless digital technologies for customer acquisition, credit assessment, loan approval, disbursement, recovery and associated customer service'. It applies to digital lending applications and platforms operated by banks and non-banking financial companies, as well as to those operated by lending service providers engaged by banks and non-banking financial companies.

The Reserve Bank of India also issued the Guidelines on Default Loss Guarantee in Digital Lending (DLG Guidelines) to govern the DLG model, bringing in clarity and permissibility to loss-sharing arrangements in digital lending, which are termed as default loss guarantee (DLG) or first loss default guarantee (FLDG). The DLG Guidelines recognise and permit regulated entities (REs) to enter into arrangements with lending service providers or other REs, under which the latter

* Sajai is the Co-Chair of JSA's Corporate Practice and the Chair of the IBA Technology Law Committee. He is an expert on information technology and financial technology-related laws, and regularly advises clients on their product initiatives and technology-based service offerings.

guarantees to compensate the RE's loss due to default (up to a certain percentage) of the loans provided by the RE.

The most crucial aspect of these regulations is the imposition of a 5 per cent cap on the maximum loan coverage a third party can offer for the entire loan portfolio. This effectively means that most credit risk will still be borne by the lending institution (or RE). Additionally, the DLG amount cannot be used to offset losses on specific individual loans; REs also must activate the DLG within a maximum of 120 days of a loan becoming overdue, unless the borrower pays off the loan before this period elapses.

National Payments Corporation of India (NPCI)

The NPCI was set up as a joint initiative of the Reserve Bank of India and the Indian Banks Association under the Payment and Settlement Systems Act 2007 to operate retail payments and settlement systems in India. The NPCI has launched many payment systems in India such as the Unified Payments Interface (UPI), RuPay (domestic card network), etc. NPCI is not a statutory body and has been set up as a not-for-profit. The payment systems operated by NPCI have many third-party participants which are regulated by various notifications issued from time to time by the NPCI. The UPI is a system that enables multiple bank accounts (of participating banks) to be accessed using a single mobile application, quick routing of funds and merchant payments.

Data localisation

Pursuant to its notification dated 6 April 2018, the Reserve Bank of India requires all system providers to store data (including end-to-end transaction details) in India relating to payment systems operated by them. For the foreign part of a transaction, the data may also be stored in the respective foreign country if required.

Outsourcing

The Reserve Bank issued Guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks on 3 November 2006. These restrict banks from outsourcing any 'core management functions' such as decision-making functions, including determining compliance with know your customer (KYC) norms. Similar guidelines have also been enabled for non-banking financial companies and payment system operators.

The Reserve Bank of India issued the Master Direction on Outsourcing of Information Technology Services on 10 April 2023 (Master Directions on IT Outsourcing), which came into effect on 1 October 2023. The Master Directions on IT Outsourcing were issued to ensure that the responsibility of regulated entities (such as banks, credit information companies, non-banking financial companies, etc) towards their customers does not diminish on account of engaging third-party service providers for information technology services, nor does it hinder effective supervision by the Reserve Bank of India. In pursuance of that, the Master Directions on IT Outsourcing impose extensive requirements on regulated entities, including the necessity for a board-approved policy (including an exit strategy), the establishment of a risk management framework, a mechanism for handling complaints, and legally binding agreements.

Credit information

The Credit Information Companies (Regulation) Act 2005 provides for regulation of credit information companies and defines the term 'credit information' to include, amongst other things, information relating to the amount and the nature of loans, amounts outstanding under credit cards and other credit facilities granted by a credit institution, and the creditworthiness of any borrower.

It further provides that only a duly registered 'credit information company' may, amongst other things, collect, process and disseminate information on trade, credit and financial standing of bank customers, and provide a credit score in respect thereof.

Recurring mandates

The Reserve Bank of India issued a framework on the processing of e-mandates on cards for recurring transactions made through card transactions, prepaid instruments and UPI. A customer is required to register and process the first transaction using additional factor authentication. Thereafter, for recurring transactions above INR 15,000, card issuers are required to authenticate the transaction through additional factor authentication.

Storage of card data

The Reserve Bank of India required all entities in a payment chain, other than card networks and card issuers, to cease storage of card data and purge any previously stored data before 1 October 2022. Entities may store the last four digits of a card number and the card issuer's name for the limited purposes of transaction tracking and reconciliation.

The Reserve Bank has been encouraging card holders to tokenise their cards to reduce incidents of fraudulent use and misuse of card data, and released a framework for card on file tokenisation services. The framework envisages the creation of unique codes, or 'tokens', which will replace card details. These tokens may be stored by merchants for future processing. The token creation process involves a one-time registration for each card, at each merchant's website, through additional factor authentication.

Anti-money laundering

The Prevention of Money Laundering Act 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules 2005 require every banking company, financial institution (which includes the operator of a payment system) and intermediary to keep certain records and report certain questionable/suspicious transactions.

Notably, the High Court of Delhi in *PayPal Payments Pvt. Ltd. (PayPal) v Financial Intelligence Unit India & Anr* (W.P. (C) 138/2021]), has recently held that an online payment gateway service provider such as PayPal would be classified as a payment system operator under the Prevention of Money Laundering Act 2002 (PMLA). Therefore, PayPal would be mandated to adhere to the obligations falling upon a reporting entity under PMLA.

The Ministry of Finance notified and expanded the scope of the Prevention of Money Laundering Act 2002 to include specific activities related to virtual digital assets (VDAs) under its purview. The definition of VDA will be the same as in the Income-tax Act 1961. This definition is broad in nature and includes any information, code, number, or token generated in digital form through cryptographic means, providing a digital representation of value exchanged with or without consideration that can be transferred, stored, or traded electronically. This definition also includes non-fungible tokens (NFTs) in its ambit. The Ministry of Finance has notified that the following activities will be subject to the provisions of the PMLA:

- exchange between VDAs and fiat currencies;
- exchange between one or more forms of VDAs;
- transfer of VDAs;
- safekeeping or administration of VDAs or instruments enabling control over VDAs; and
- participation in and provision of financial services related to an issuer's offer and sale of a VDA.

Know your customer directions

The Master Direction – Know Your Customer Direction 2016 – issued by the Reserve Bank of India, imposes customer due diligence and KYC obligations on entities such as non-banking financial companies, payment system providers and issuers of prepaid payment instruments. These include the obligation to frame KYC policies, types of data to be collected, retention periods, etc.

Please see responses below for regulations governing payment systems, prepaid instruments (including wallets), open banking and crypto assets.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

In 2018, the Reserve Bank of India had cautioned against dealing in virtual currencies due to the risks involved and the lack of regulation, and had restricted regulated entities from dealing in or providing services in respect of virtual currencies.

In 2020, this notification was struck down by the Supreme Court of India in *Internet and Mobile Association of India v Reserve Bank of India (2020)* on the grounds of unreasonableness of restrictions imposed upon the exercise of freedom guaranteed under Article 19 (i)(g) of the Constitution of India. Subsequently, the Reserve Bank of India acknowledged that banks may process cryptocurrency-related transactions, subject to their customer due diligence procedures.

Since then, India has witnessed the introduction of some regulations which regulate cryptocurrencies and other crypto assets to a certain extent:

- amendments to taxation laws have been introduced, which inter alia tax any income from the transfer of virtual digital assets at 30 per cent and which mandate a withholding tax of 1 per cent at the time of payment of consideration for transfer of a virtual digital asset;

- the Advertising Standards Council of India, which is a voluntary, non-statutory council in advertising, has published guidelines on the advertisement of virtual digital assets and linked services;
- the Ministry of Corporate Affairs has mandated all companies to include disclosures in their financial statements on virtual currency and cryptocurrency transactions undertaken by them in a financial year; and
- pursuant to a notification by the Ministry of Electronics and Information Technology, the Indian Computer Emergency Response Team specifically requires virtual asset service providers, virtual asset exchange providers and custodian wallet providers to keep all the information obtained as part of KYC and certain records of financial transactions for a period of five years.

The Government of India has announced the introduction of the Cryptocurrency and Regulation of Official Digital Currency Bill, 2021. The draft of this bill is not publicly available and has not been tabled before the Parliament of India yet. The Government of India had announced that the bill would seek to prohibit all private cryptocurrencies, while creating a facilitative framework for the introduction of an official digital currency issued by the Reserve Bank of India and still allowing certain exemptions to promote the underlying technology and its uses.

The Government of India has also announced that the Reserve Bank of India would launch its own digital currency based on blockchain – the Central Bank Digital Currency – which would be exchangeable one-to-one with fiat currency (as described below).

Central Bank Digital Currency (CBDC)

The Reserve Bank of India proposes to introduce CBDC or the 'digital rupee' as a legal tender that coexists with and complements existing forms of money in a digital format. It envisages two categories of CBDC: iretail CBDC (CBDC-R) and wholesale CBDC (CBDC-W). CBDC-R is intended to be a general-purpose digital currency which would be available for use by private sector, non-financial consumers and businesses, while CBDC-W is intended to be made available only to financial institutions specifically for the purpose of inter-bank transfers and settlement of transactions. The Reserve Bank of India has launched pilots for both categories with selective banking entities.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

In India, payment services are primarily regulated by the Reserve Bank of India, pursuant to the Payment and Settlement Systems Act 2007 (Act) and the regulations thereunder. Under the Act, a 'payment system' is defined as a 'system that enables payment to be effected between a payer and a beneficiary, involving clearing, payment or settlement service or all of them, but does not include a stock exchange'. All systems (except for stock exchanges and clearing corporations set up under stock exchanges) carrying out either clearing, settlement or payment operations (or all of them) are regarded as payment systems. Payment systems include systems enabling credit card operations, debit card operations, smart card operations, money transfer operations or similar operations. Any entity

operating a payment system is a 'system provider'. An entity that wishes to begin to operate a payment system is required to be authorised to do so by the Reserve Bank of India.

In India, digital wallets are regulated as prepaid payment instruments (PPIs) by the Reserve Bank of India, pursuant to the Master Directions on Prepaid Payment Instruments 2021. PPIs are broadly categorised as follows:

- *Closed system PPIs*: these PPIs facilitate the purchase of goods and services from the entity issuing the PPI only. No cash withdrawals are allowed. These are not currently regulated or supervised by the Reserve Bank of India.
- *Small PPIs*: these PPIs require minimal details of the PPI holders to be set up and may only be used for the purchase of goods and services. Fund transfers and cash withdrawals for such PPIs are not allowed. Issuance of small PPIs requires authorisation from the Reserve Bank of India.
- *Full KYC PPIs*: these PPIs are issued after full KYC processes are conducted for the holder of the PPI and may be used for purchase of goods and services, fund transfers and cash withdrawals. Issuance of full KYC PPIs requires authorisation from the Reserve Bank of India.

In its Payments Vision 2025 statement, the Reserve Bank of India has stated that it proposes to revisit the framework on PPIs, including closed system PPIs.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

There have been several initiatives to facilitate and support the fintech ecosystem and startups in India, including regulatory sandboxes and innovation hubs. Regulatory sandboxes have been set up in financial, securities and insurance sectors by each of the respective regulators.

The Reserve Bank of India launched regulatory sandboxes in three cohorts: on retail payments (tested products that engage feature phones and offline payments), cross-border payments (tested platforms facilitating purchase of assets listed on foreign exchanges, blockchain-based cross-border payment systems, etc) and micro, small and medium enterprises lending. The fourth cohort is being conducted on prevention and mitigation of financial fraud for which the Reserve Bank of India has selected six entities to test their fintech products from February 2023 onwards.

The Reserve Bank of India has recently launched the Reserve Bank Innovation Hub to create an ecosystem that focuses on promoting access to financial services by identifying and mentoring startups. The hub has been set up though a wholly owned subsidiary of the Reserve Bank of India and its board comprises independent industry and academic experts. The Reserve Bank also set up a dedicated department to oversee and supervise the financial technology sector.

Furthermore, the Ministry of Electronics and Information Technology has announced the Digital India Startup Hub (DISH) initiative that is aimed to enable startups around the country by facilitating fact time engagements between startups and government on a regular basis.

The government has launched a regulatory framework to establish international financial services centres (IFSC) in India, under the purview of the International Financial Services Centres Authority (IFSCA). The IFSCA is a single regulator for the centre and is aimed at the development and regulation of financial products, financial services and financial institutions in the international financial centres in India. Currently, the Gujarat International Finance Tec-City (GIFT) is the only IFSC in India.

The IFSCA has launched a Framework for FinTech Entity in the IFSCs, which provides for a regulatory sandbox – ie, the IFSCA Fintech Regulatory Sandbox for fintech products and solutions (which would enable such players to avail grants under the IFSCA Fintech Incentive Scheme 2022) and the Interoperable Regulatory Sandbox, which tests fintech products and solutions that would typically fall within the regulatory purview of multiple financial sector regulators.

The Government of India has also approved an incentive scheme of INR 2,600 crore (approximately US$360m) for promoting RuPay debit cards (a domestic card scheme developed by the National Payments Corporation of India (NPCI)) and low value UPI transactions. It is expected to facilitate the construction of a robust digital payment ecosystem in India.

The Reserve Bank of India has launched the pilot project for Public Tech Platform for Frictionless Credit, that would enable delivery of frictionless credit by facilitating a seamless flow of required digital information to lenders and optimising the lending process, cutting operational costs, expediting disbursements, and enabling scalability. The initial phase of the project would prioritise products such as Kisan credit card loans, dairy loans, collateral-free loans for micro, small and medium enterprises, personal loans and home loans.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

The primary regulation in India's open banking regime is the Master Direction – Non-Banking Financial Company – Account Aggregator (Reserve Bank) Directions 2016, (Master Directions) which were issued to regulate non-banking financial companies undertaking the business of an account aggregator for a fee or otherwise.

Further, the Reserve Bank of India has also issued the *Technical Specifications for all participants of the Account Aggregator ecosystem*, which spells out the technical infrastructure requirements applicable to the actors in the Indian open banking regime.

The open banking framework in India is in its first stage and facilitates limited use cases.

Under the Master Directions, account aggregators are allowed to only carry on the business of account aggregation. A registration process has been set out for an account aggregator. The Master Directions define the business of an account aggregator as the business of providing under a contract, retrieval or collection services in respect of such financial information pertaining to its customers, as may be specified by the Reserve Bank of India from time to time; and consolidating, organising and presenting such information to the customer or any other user of financial information as may be specified by the Reserve Bank of India. Other than this, an account aggregator

is not allowed to undertake any other business activity, including but not limited to supporting transactions by customers, storing of financial information, etc.

Account aggregators are envisaged to be data blind. Their limited role is to manage the consent artefact and act as a conduit for information sharing between financial information providers (FIPs) and financial information users (FIUs). Notably, the Securities and Exchange Board of India (SEBI) has joined the account aggregator framework in India for customers to share information about their mutual fund and stock holdings with financial service providers or FIUs. SEBI also requires FIPs engaged in the securities market to enter into a contractual framework with the account aggregators.

To date, only regulated FIPs and FIUs that are registered with financial sector regulators may have access to the account aggregator ecosystem. Account aggregators are required to collect the explicit consent of customers to retrieve, share and transfer their financial information. The consent is required to be collected in a standardised consent artefact.

The account aggregator framework in India was enabled on 2 September 2021. Based on information available in the public domain, at least six entities have received licences and have launched customer facing applications, and at least eight entities have received in-principle approval. Several banks and financial technology companies have also appeared on the network as financial information providers and financial information users. A voluntary, self-organised and self-regulating body has been set up for the account aggregator ecosystem (the DigiSahamati Foundation).

Indonesia

Freddy Karyadi*
ABNR, Jakarta
fkaryadi@abnrlaw.com

Anastasia Irawati†
ABNR, Jakarta
airawati@abnrlaw.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

The following are the key regulations on fintech and financial innovation in Indonesia.

Securities crowdfunding

On 11 December 2020, Indonesia's financial services authority, Otoritas Jasa Keuangan (OJK) enacted OJK Regulation No 57 on securities crowdfunding (POJK 57). This revoked a previous regulation from 2018 on equity crowdfunding. POJK 57 was later amended by OJK Regulation No 16/POJK.04/2021. Despite sharing some fundamental principles, securities crowdfunding differs from classic public offerings undertaken through the Indonesian Stock Exchange. Securities crowdfunding typically involves the offering of small amounts of securities by the relevant issuers to retail investors.

Unlike the previous regulations, that focused only on equity securities, POJK 57 expands the scope of crowdfunding to include equity securities in shares and other types of securities, such as debt securities and *sukuk*,[1] or other convertible equity.

Significantly, POJK 57 now allows Indonesian non-legal entities to participate as issuers – unlike the 2018 regulation that allowed only Indonesian limited liability companies to do so. It brings small and medium-sized enterprises and startups an opportunity to acquire a new source of income.

Peer-to-peer (P2P) lending

The country's P2P business is covered in OJK Regulation No 10/POJK.05/2022 (POJK 10). POJK 10 is the newest P2P regulation in Indonesia and revokes the previous legislation. It sets the scope of P2P lending practice, including:

- business activities;
- registration and licensing procedures;
- the relationship between the P2P lending providers and users;

* Freddy has practised law and tax in Indonesia for more than 25 years. He has been heavily involved in numerous complex cross-border deals and is one of the pioneers who focused on the digital industry.

† Anastasia is a senior associate at ABNR. Her focus of expertise includes M&A, tech law and competition law. She has been involved in many cross-border deals concerning her expertise.

1 Islamic bonds.

- risk mitigation;
- IT system maintenance;
- prohibitions in P2P lending; and
- the minimum requirements concerning agreements between the lender–borrower and lender–service provider.

POJK 10 provides some stricter requirements compared to the previous regulations, which we believe were adopted from the existing OJK regulations in other heavily regulated business sectors such as insurance, securities and multi-finance, including a higher amount of capital requirement. The POJK 10 also introduces the Sharia[2] concept to the P2P business.

Payment system

On 29 December 2020, the central bank, Bank Indonesia, issued Peraturan Bank Indonesia (PBI) Regulation No 22 on the payment system (PBI 22), effective from 1 July 2021. The regulation differentiates payment system providers into (1) payment services providers and (2) payment system infrastructure providers. For more on this subject, see Question 3.

Crypto assets

Crypto assets were first acknowledged as a commodity in Indonesia in 2018 through Regulation No 99 of 2018, General Policy on Crypto Asset Trading, issued by the Ministry of Trade. As a follow-up on this, the Commodity Futures Trading Regulatory Agency (Bappebti) issued several renditions of a regulation to regulate the trading mechanism for crypto assets. The prevailing regulation is Bappebti Regulation No 8 of 2021, which has been amended by Bappebti Regulation No 13 of 2022. Bappebti recently appointed PT Bursa Komoditi Nusantara to act as the crypto asset exchanges (crypto bourse) in Indonesia. Following this appointment, the Bappebti is in the process of drafting more regulations concerning crypto assets in Indonesia. For more on this subject, see Question 2.

Digital gold

The trading of digital gold in Indonesia was first legalised through Ministry of Trade Regulation No 119, 2018. The trading process was further regulated by the Bappebti through Bappebti Regulation No 4 of 2019, Technical Provisions on Implementation of Digital Gold Physical Market in Futures Exchange, as amended by Bappebti Regulation No 13, 2019 (Reg 4).

Regulation 4 requires a digital gold trader to fulfil some requirements, including (1) being a licensed futures exchange and clearing house member, and (2) placing the physical gold with a designated gold storage manager. The digital gold transactions allowed under Reg 4 are:

- sale and/or purchase;
- buying up to a specified amount of the gold that can be printed for collection;

2 Islamic law.

- fixed instalments with later delivery;
- deposit;
- printing; and
- other transactions based on the innovations, developments and needs in digital gold trading.

Mutual funds

In Indonesia, a mutual fund in the form of a collective investment fund or KIK Mutual Fund can only be offered and sold to investors by an investment manager. This is regulated under OJK Regulation No 23/POJK.04/2016, as amended by OJK Regulation No 4 of 2023 on Mutual Fund in the Form of Collective Investment Contract (POJK 23). Nevertheless, the POJK 23 opens an opportunity for the investment manager to cooperate with other parties who have (1) wide networks in their business activities to provide a point of sale or sales outlets, and/or (2) a credible electronic system.

POJK 23 also provides that the transaction of a mutual fund participation unit can be conducted electronically, either through an electronic system built by the investment managers themselves or by cooperation with a third party. This electronic system may be in the form of a virtual account provided by an authorised payment gateway service company, or other payment mechanism innovation related to mutual funds.

IT-based expert advisory services

Bappebti recently issued a regulation to outlaw rogue robot trading, but to allow and indeed facilitate the provision of online advisory services to help retail investors make informed choices. The regulation is issued under Bappebti Regulation 12 of 2022 on the Provision of Information Technology-based Expert Advisory Services in Commodity Futures Trading.[3]

The regulation allows futures advisers (FA) that have been approved by Bappebti to carry out IT-based advisory services (AS). AS is an automated service related to market monitoring, calculating market entry and exit opportunities, placing of reasonable transactions, and managing risk as appropriate to client needs.

In this scheme, the FA will only provide the advice but the final decision on whether or not to invest would be taken by the customer.

Fintech taxation

The government recently issued Minister of Finance Regulation No 69/PMK.03/2022 on Income Tax and VAT on the Implementation of Financial Technology.[4] The focus of this regulation is the imposition of (1) income tax for the interest earnings in a P2P transaction and (2) VAT for the services provided in the financial technology market.

3 Peraturan Bappebti No 12 Tahun 2022 tentang Penyelenggaraan Penyampaian Nasihat Berbasis Teknologi Informasi Berupa Expert Advisor di Bidang Perdagangan Berjangka Komoditi.

4 PMK No 69/PMK.03/2022 tentang Pajak Penghasilan dan Pajak Pertambahan Nilai atas Penyelenggaraan Teknologi Finansial.

The regulation requires the financial technology operator who has been appointed as a taxable entrepreneur to collect the VAT over the fee, commission, merchant discount rate or other consideration obtained from the services provided to the consumer. The tariff would be 11 per cent.

Regarding the first imposition, the interest earned by the lender in a P2P transaction will be deemed as earnings of the lender which would be subject to income tax and must be reported in the annual tax return of the lender. The interest would be subject to:

- Article 23 of the Income Tax Law in the case of domestic taxpayers or permanent establishments. The income tax rate would be 15 per cent of the gross interest amount; and
- Article 26 of the Income Tax Law in the case of foreign taxpayers. The income tax rate would be 20 per cent of the gross interest amount or in accordance with the amount agreed in the tax treaty.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

Crypto assets have been acknowledged as a commodity in Indonesia in 2018 through the issuance of Ministry of Trade Regulation No 99 of 2018 on General Policy on crypto asset trading. However, the first crypto asset trading regulation in Indonesia was Bappebti Regulation No 5, issued in 2019. The regulation has since been revoked and replaced by Bappebti Regulation No 8 of 2021 on Guidelines for the Physical Trading of crypto assets on the Futures Exchange, as amended by Bappebti Regulation No 13 of 2022 (Reg 8).[5]

Crypto assets characteristics under Indonesian Law

Under Indonesian law, crypto assets are categorised as a commodity that can be traded in the market. However, crypto assets cannot be used as a method of payment in Indonesia. The prevailing laws and regulations in Indonesia only allow the use of the Indonesian rupiah as the currency and method of payment for transactions performed within the territory of the Republic of Indonesia.

Crypto assets can only be traded in the physical market if they are approved by and registered with Bappebti. Bappebti has recently updated the list of crypto assets that are allowed for trading on the local crypto assets market. After the updates, there are 383 approved crypto assets to be traded in Indonesia. Some of the notable new members of the list are Secret (SCRT), Axie Infinity (AXS), Ethereum Name Service (ENS), and PancakeSwap (CAKE).

Key market players

Some of the key players in the physical crypto asset futures that are regulated under Reg 8 are crypto asset exchanges, crypto asset clearing agencies, crypto asset traders, crypto asset clients, and crypto asset storage providers.

5 Peraturan Badan Pengawas Perdagangan Berjangka Komoditi No 8 Tahun 2021 tentang Pedoman Penyelenggaraan Perdagangan Pasar Fisik Aset Kripto di Bursa Berjangka sebagaimana telah diubah dengan Peraturan Badan Pengawas Perdagangan Berjangka Komoditi No 13 Tahun 2022.

To be appointed as a crypto asset exchange, crypto asset clearing agency, crypto asset trader, crypto asset client or crypto asset storage provider, each party must fulfil a number of requirements from the Bappebti, including but not limited to:

- minimum issued and paid-up capital;
- equity maintenance;
- engaging an employee with specific qualifications; and
- having the members of the board of directors, board of commissioners, shareholders and controller/beneficial owner passing the suitability and competence test requirement.[6]

There are also additional requirements that must be fulfilled specifically by crypto asset traders, which, among others, include the obligation to have Indonesian nationals as directors and members of the board of commissioners, as well as having a physical office in Indonesia. Following the recent appointment of crypto asset exchanges (crypto bourses) in Indonesia, the current prospective physical crypto assets traders must convert their license to be registered as crypto asset traders.

Tax obligations

The Indonesian government imposes VAT and income tax on the crypto assets transaction, as regulated under Minister of Finance (MoF) Regulation No 68/PMK.03/2022.

VAT

The MoF will impose VAT on:

- Intangible taxable goods in the form of crypto assets by the crypto assets' sellers: this includes (1) sale and purchase of crypto assets with fiat money; (2) swap of crypto assets; and/or (3) swap of crypto assets with other goods and/or services.
- Taxable services in the form of the provision of electronic facilities for crypto assets trading by the Trade Organiser through the Electronic System (PPMSE). This includes the provision of services for (1) sale and purchase of crypto assets with fiat money; (2) swap of crypto assets; (3) e-wallet services for the deposit, withdrawal; (4) transfer of one crypto asset to the other party's account; and (5) the management of the media for the storage of the crypto assets.
- Taxable services in the form of verification of crypto assets transactions and/or management services of the mining pool of crypto assets.

Income Tax

Any income received by the (1) crypto assets trader; (2) trade organiser through the electronic system; and (3) crypto miners in relation to the crypto assets will be subject to income tax.

For the crypto income of the crypto assets traders, they will be subject to final income tax with the tariff of:

6 According to our last discussion with Bappebti, we understand that the fit and proper person test mechanism is not yet implemented.

- 0.1 per cent of the transaction amount if the electronic system that is used for the transaction is registered with the Bappebti; or
- 0.2 per cent of the transaction amount if the electronic system that is used for the transaction is not registered with the Bappebti.

Supervising authority

Following the issuance of Law No 4 of 2023,[7] the supervising authority for crypto asset trading in Indonesia has been changed from Bappebti to the OJK. The transition period is expected to be finished by January 2025 – in which the authority to supervise the crypto asset trading in Indonesia would be under the OJK. During the transition period, it is expected that many new regulations will be issued to govern the crypto assets in Indonesia.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

After the issuance of PBI 22, payment system providers in Indonesia are classified into:

- Payment services providers (*penyedia jasa pembayaran* or PJP). These are banks or non-bank institutions that offer services of facilitating payment transactions to users such as account information services, payment initiation and/or acquiring services, account issuance services, and/or remittance services. A PJP company must obtain a licence from Bank Indonesia; digital wallets and e-money service providers will be categorised as PJP under PBI 22.
- Payment system infrastructure providers, or (*penyelenggara infrastruktur sistem pembayaran* or PIP). These are parties that provide infrastructure for transferring funds and carrying out clearing and/or final settlement. A PIP company must obtain a so-called appointment from Bank Indonesia.

PBI 22 also introduces foreign direct investment restrictions. PJP business is open to 85 per cent foreign shareholding, provided that at least 51 per cent of shares with voting rights, management control and veto rights are held by Indonesian shareholders. PIP business is only open to 20 per cent foreign shareholding, provided that at least 80 per cent of shares with voting rights, management control and veto rights are held by Indonesian shareholders. The calculation of the shareholding participation will be traced up to the ultimate beneficiary of the shareholders.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

As a result of constant innovation in the fintech sector, some fintech business models are not yet covered by the existing regulations. To deal with this problem, the government regulates this matter as follows.

7 Undang-undang No 4 Tahun 2023 tentang Pengembangan Dan Penguatan Sektor Keuangan.

For fintech related to the payments systems: Bank Indonesia Regulation No 23/6/PBI/2021 on Payment Services Provider[8]

Under this regulation, Bank Indonesia may determine that a particular product, activity, service, or business model may be 'sandboxed' for testing purposes. The purpose of this is to (1) encourage technological innovation and (2) monitor/detect opportunities and risks of technological innovation, the development of the digital economic and financial ecosystem, and the implementation of the payment system.

For fintech related to lending and all other aspects of fintech: OJK Regulation No 13/POJK.02/2018 of 2018 on Digital Financial Innovation in the Financial Services Sector[9]

This regulation establishes a digital financial innovation (DFI) regime that consists of three separate aspects: recordation, regulatory sandbox and registration.

Initially, the prospective DFI providers should be recorded with the OJK as the DFI providers. Once the provider has been recorded, the OJK will review whether it is qualified to participate in the regulatory sandbox process. After completing the sandbox process, the OJK will issue a recommendation status. If the provider receives a recommendation for registration, it must apply for registration to the OJK within six months of the issuance of the recommendation.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

Bank Indonesia has issued the Regulation of Members of the Board of Governors No 23/15/PADG/2021 on the Implementation of National Standard Open Application Programming Payment Interface.[10] This regulation sets out protocols and instructions that facilitate open interconnection between applications in payment transaction processing.

8 Peraturan Bank Indonesia No 23/6/PBI/2021 tentang Penyedia Jasa Pembayaran.

9 Peraturan Otoritas Jasa Keuangan No 13/POJK.02/2018 Tahun 2018 tentang Inovasi Keuangan Digital di Sektor Jasa Keuangan.

10 Peraturan Anggota Dewan Gubernur No 23/15/PADG/2021 tentang Implementasi Standar Nasional *Open Application Programming Interface* Pembayaran.

Japan

Yuri Suzuki[1]
Atsumi & Sakai, Tokyo
yuri.suzuki@aplaw.jp

Naoki Kanehisa[2]
Atsumi & Sakai, London
naoki.kanehisa@aplaw.jp

Kenichi Tanizaki[3]
Atsumi & Sakai, Tokyo
kenichi.tanizaki@aplaw.jp

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

In Japan, there are no specific fintech or financial innovation laws that have been enacted. However, there are numerous laws that are relevant to fintech companies, and a series of recent amendments thereof have enhanced the development of fintech and financial innovation. Below are summaries of the most relevant laws.

The Payment Services Act – regulation of funds transfer services

For a non-bank business operator to operate a remittance service, it must be registered as a funds transfer service under the Payment Services Act (PSA). Remittance services are generally considered as 'exchange transactions' (*Kawase Torihiki*) and only banks are allowed to provide such transactions. However, entities other than banks are also allowed to operate a remittance service by registering as a funds transfer service.

There are three types of funds transfer services. For Type 1 funds transfer services, there is no maximum amount of remittance per transaction. On the other hand, Type 2 funds transfer services and Type 3 funds transfer services have limits of JPY 1m and JPY 50,000 per remittance, respectively. It is easier to obtain registration as a funds transfer service provider than to obtain a banking licence.

The Payment Services Act – regulation of prepaid payment instruments (own business/third-party business)

Prepaid settlement services are regulated by the PSA and are categorised as either prepaid payment instruments for one's own business or as prepaid payment instruments for third-party business.

1 Yuri heads Atsumi & Sakai's fintech law practice. She has significant experience advising financial institutions, leading fintech companies and startups on banking and finance, fintech matters, new services and technologies.

2 Naoki heads Atsumi & Sakai's London office. He has advised domestic and foreign fintech companies, global payment service providers and international financial institutions on financial regulatory issues.

3 Kenichi is deputy manager of Atsumi & Sakai's fintech team. He has significant experience advising major banks, financial institutions and fintech companies on a wide range of banking and finance matters.

In this context, prepaid payment instruments for one's own business refers to prepaid settlement services that can only be used for products and services provided by the issuer of the prepaid settlement instrument. Prepaid payment instruments for third-party business refers to prepaid settlement services that can be used with merchants other than the issuer.

Prepaid settlement services include IC cards, server-based prepaid cards, server-based electronic money and virtual currencies used in online games. As there are some settlement services to which the PSA does not apply, it is necessary to confirm on a case-by-case basis whether the PSA applies to any given settlement service.

The issuer of a prepaid payment instrument for one's own business is required to submit a notification to the competent authority, if the unused balance of all the prepaid payment instruments is over JPY 10m as of the record date (the record date being 31 March and 30 September each year). Such notification is due within two weeks from the day after the record date. The issuer of a prepaid payment instrument for a third-party business is required to register before issuing such instruments. Only a registered issuer is allowed to issue a prepaid payment instrument for a third-party business.

Pursuant to a 2022 amendment to the PSA, regulations have been tightened for prepaid payment instruments for third-party businesses that can be electronically assigned or transferred (limited to payments in large amounts as provided for in the Cabinet Office Order referred to in Question 3).

The Banking Act – regulation of electronic payment services

Electronic payment services include:

- electronic remittance services, where remittance instructions are received online and the instructions relayed to the customers' bank on behalf of customers; and
- account information retrieval services, which are used by customers to obtain account information from the bank and provide it to customers online.

Electronic remittance services include real-time bank transfer services offered by cloud accounting services. Account information retrieval services include personal finance management (PFM) and cloud accounting services. Conducting either of the above services for business purposes requires registration as an electronic payment service under the Banking Act.

Regulation of crypto assets

Please see Question 2 for further details.

The Payment Services Act – regulation of stablecoins

Stablecoin regulations were introduced by the PSA amendment of 3 June 2022; please see Question 2 for further details.

Financial Action Task Force – Fourth Mutual Evaluation of Japan

The Fourth Mutual Evaluation of Japan by the Financial Action Task Force (FATF) concluded that further enhancement and optimisation of transaction filtering and monitoring was required in Japan. In response, under the 2022 amendment of the PSA, the business of providing transaction filtering and monitoring services has been defined as an 'exchange transaction analysis business'.

Therefore, any person who wishes to engage in the business of exchange transaction analysis is now required to obtain permission from the competent authority. Due to this amendment, several entities (including the Japanese Bankers Association) are now considering forming a coalition for AML/CFT measures.

Japanese Banks' Payment Clearing Network

The Japanese Banks' Payment Clearing Network is now considering providing funds transfer service providers with access to the data telecommunications system of all banks (the Zengin system), a money transfer system currently available to depository financial institutions only.

Provision of access to the Zengin system to funds transfer service providers would enable them to directly remit money to financial institutions and other funds transfer service providers, which is expected to lead to a reduction in time and costs required for remittances. Furthermore, this could increase competition in the development of new remittance services using smartphone apps.

2. Regulations on crypto assets: a summary of the legal framework relating to crypto assets and how they are regulated.

In Japan, applicable laws and regulations on crypto assets vary depending on the type of digital asset as well as the related products and services. The major digital assets and applicable laws are as follows:

Crypto assets

Crypto assets such as Bitcoin are regulated by law. Any of the following activities conducted in the course of trade constitutes 'crypto asset exchange services', and any person who conducts crypto asset exchange services falls within the scope of PSA regulation and must be registered with the regulator for:

1. purchase and sale of crypto assets and exchange for other crypto assets;
2. intermediation, brokerage or agency of (1);
3. management of user funds for the purposes of (1) or (2); or
4. management of crypto assets for another person.

Crypto asset derivative transactions

Under the 2019 amendments to the Financial Instruments Exchange Act (FIEA), crypto asset margin trading is deemed to be 'over-the-counter transactions of derivatives' and conducting such transactions on a regular basis requires regulation as a 'financial instruments business'. Therefore, any person who conducts financial instruments business falls within the scope of FIEA regulation and must be registered with the regulator.

Security tokens

The 2019 amendments to the FIEA clarify that certain types of security tokens are categorised as 'securities', and as such the activities of purchasing, selling and underwriting of such security tokens are regulated as 'financial instruments business'. Therefore, any person who conducts financial instruments business falls within the scope of FIEA regulation and must be registered with the regulator.

Stablecoins

The 2022 amendments to the PSA, the Banking Act and other laws introduced a new regulatory framework for stablecoins. Under this framework, stablecoins are categorised as follows:

1. stablecoins that are issued at a price linked to the value of fiat currency (eg 1 coin = 1 JPY or 1 coin = 1 US$) enabling redemption at the issued price; and
2. stablecoins other than (1) above (eg stablecoins that attempt to achieve price stability through means of algorithmic mechanisms).

While the category of stablecoins described in (2) are regulated as 'crypto assets' under the pre-existing provisions of the PSA, as discussed above, the stablecoin usage described in (1) is more akin to that of electronic money regulated as money transmissions and means of payment. The 2022 amendments were intended to regulate the stablecoins described in (1), and a new licensing regime was introduced for intermediaries who handle such stablecoins.

Another key point to remember is that, in order to protect users' redemption rights, issuers of such stablecoins are limited to banks regulated under the Banking Act, funds transfer service providers regulated under the PSA, and trust companies regulated under the Trust Business Act, with such financial institutions already being regulated under their respective bankruptcy protection regimes.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

Payment service providers, and the provision of digital wallets by them, are regulated under the PSA. As described in Question 1, there are two types of payment service providers (funds transfer service providers and issuers of prepaid payment instruments (e-money)), which both usually provide digital wallets for their customers. Customers buying prepaid payment instruments hold their e-money in their wallets.

In addition to the restrictions mentioned in Question 1, the PSA requires funds transfer service providers to establish measures to ensure that they do not hold customer funds that are not being used for exchange transactions. In relation to this restriction:

- Type 1 funds transfer service providers are only allowed to hold funds that are received with specific remittance instructions from customers;
- Type 2 funds transfer service providers are required to check with a customer which holds more than JPY 1m in its account, to determine if (and ensure that) the funds in the account will be used for remittance purposes only (Type 2 funds transfer service providers are also required to establish measures to return funds to a customer or avoid holding any customer funds which they discover are not being used for remittance purposes); and
- Type 3 funds transfer service providers are not allowed to accept more than JPY 50,000 for each customer account.

Issuers of e-money who are not registered as funds transfer service providers are not permitted to allow customers to withdraw e-money as cash, unless the issuers have decided to stop providing their services or such customer is closing their account with the issuer.

Issuers of prepaid payment instruments that allow customers to charge high amounts for such prepaid payment instruments and transfer them to other customers are subject to anti-money laundering and know your client (AML/KYC) regulations pursuant to the provisions of the newly amended PSA and the Act on Prevention of Transfer of Criminal Proceeds, which came into force in June 2023. The new regulations require issuers of prepaid payment instruments for third-party businesses to comply with AML/KYC regulations, and to submit additional information and a business implementation plan when they make their registration application, specifically in situations where the issuer issues prepaid payment instruments that can be charged with high amounts and electronically transferred to other customers as follows:

- more than JPY 100,000 for one charge/transfer transaction; or
- more than an aggregate of JPY 300,000 for transactions by a customer that are conducted within a month.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

There are a number of special programmes promoting innovation and supporting the fintech ecosystem in Japan.

The Government of Japan Regulatory Sandbox

The regulatory sandbox framework facilitates realisation of innovative technologies and business models in Japan. The framework covers regulations on financial services. Under this framework, companies can apply to conduct 'demonstrations' and test the possibilities of using innovative technologies for future businesses. This is particularly useful for the purpose of testing or demonstrating certain types of business that currently cannot actually be conducted in Japan due to existing Japanese regulations.

Ministry of Economy, Trade and Industry (METI)

Alongside the government's regulatory sandbox framework, METI enhances Japan's industrial competitiveness through two systems under the Industrial Competitiveness Enhancement Act.

Under the System to Remove Gray Zones, where there is uncertainty over whether existing laws and regulations will be applied to certain products and services due to their innovative nature, METI, together with the other competent ministry, can provide clarity and confirmation regarding the applicability of existing regulations to the concerned company.

In addition, METI's System of Special Arrangements for Corporate Field Tests allows preferential regulatory flexibility to individual enterprises and aims at the satisfaction of safety standards and other requirements.

Financial Services Agency (FSA)

FSA's FinTech Support Desk is a one-stop point of contact for enquiries and exchange of information on fintech. It accepts a wide range of enquiries on various finance-related matters, including from fintech startups with innovative ideas and visions.

FSA's FinTech PoC (proof of concept) Hub aims to tackle challenges and obstacles to financial innovation by assisting fintech companies and financial institutions through alleviating and addressing reluctance and concerns related to the testing of innovative products and technologies. The Hub offers support by forming special working teams for various projects in cooperation with other relevant authorities as necessary.

Tokyo Metropolitan Government (TMG)'s 'Global Financial City: Tokyo' Vision 2.0

In order to establish and maintain Tokyo's position as a leading global financial city, TMG offers various programmes to increase the number of participants in the Tokyo market, including the fintech industry. TMG's programmes include:

- a project to attract overseas financial companies, including fintech companies;
- a green finance subsidy programme for Tokyo market entry:
- a project for temporary office allocation for foreign financial companies and human resources;

- an overseas financial corporation business establishment subsidy programme;
- a subsidy to support the base of operations of overseas financial corporations; and
- a financial award system, including an accelerator programme for fintech companies.

5. Open banking: a summary of regulations relating to open banking and direct or indirect regulations that affect open banking.

An amendment to the Banking Act, which came into force on 1 June 2018, introduced the concept of 'electronic payment services', which includes:

- services to provide funds transfer instructions via the internet at the request of depositors (Write API); and
- services to obtain account information from banks and provide such information to depositors via the internet (Read API) at the request of depositors.

Banks are also obliged to make efforts to share their established APIs. Introduction of open APIs by banks will enable fintech companies to provide various fintech services by accessing banking systems. Open API is one of the core technologies of open innovation and is believed to further facilitate and promote open banking.

In addition, under the Act on the Provision of Financial Services, which came into force on 1 November 2021, any person registered as a financial services intermediary business may intermediate transactions between:

- banks and customers;
- insurance companies and customers;
- securities companies and customers; and
- money lending companies and customers.

The financial services intermediary business is considered to promote the creation of sales channels and platforms for one-stop financial services.

Furthermore, although there are no currently scheduled amendments to other relevant provisions of law, cases of so-called 'embedded finance' transactions are increasing. Embedded finance is a type of financial service where non-financial institutions (such as retailers and real estate companies) in effect provide (in an agency capacity) the financial functions of banks to customers, an arrangement that has the potential to transform the roles of existing banks. The functions of the banks themselves, in this case, are referred to as Banking as a Service (BaaS), in the sense that the banking services are to be provided by the banks to the non-bank service providers, who supply the services to the bank customers. Additionally, there are cases where a fintech company called an 'enabler' operates between a bank and a non-bank service provider, and their emergence is one of the factors promoting the unbundling of banking services.

Malaysia

Chong Mei Mei*
Raja, Darryl & Loh, Kuala Lumpur
chongmeimei@rdl.com.my

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

There is currently no specific regulatory framework governing fintech players in Malaysia. Therefore, depending on the nature of the business, fintech players may be subject to existing Malaysian laws and regulations that are applicable to conventional financial institutions, financial service providers and capital market intermediaries, or may fall within the emerging regulatory framework promulgated by Malaysian regulators.

The two main regulators in Malaysia are the Central Bank of Malaysia or Bank Negara Malaysia (BNM) and the Securities Commission Malaysia (SC), both of which have been empowered and entrusted with significant regulatory and supervisory roles and responsibilities under the relevant legislations. Some of the relevant and key laws and regulations applicable to fintech players (depending on the nature of their business) in Malaysia are as follows.

Financial Services Act 2013 (FSA)

The FSA provides that the entities that carry out regulated businesses or activities, such as banking business, investment banking business, the operation of payment systems, the issuance of electronic money (e-money), merchant acquiring services, and insurance and *takaful*[1] business, shall apply for and obtain the requisite licences, approvals and/or registrations from BNM.

With regard to banking business, in particular digital banking business, BNM released a policy document on the licensing framework for digital banks (DB Policy Documents) on 31 December 2020, requiring digital banks that carry on digital banking business (defined thereunder as banking business conducted wholly or almost wholly through digital or electronic means) to comply with the requirements under the FSA. Following the issuance of the DB Policy Documents, BNM announced five successful applicants for digital bank licences in Malaysia – as of 12 July 2024, three out of the five digital banks have commenced operations.

Given the rise of alternative payment methods in Malaysia and the growing significance of merchant acquirers in the payment landscape, BNM has issued a policy document on merchant acquiring services (MAS Policy Documents) on 15 September 2021, introducing additional obligations and regulatory requirements to be complied with by merchant acquirers providing merchant acquiring services that meet the criteria under the MAS Policy Documents, as more specifically set out in Question 3.

---

* Mei Mei handles a wide spectrum of corporate and commercial work including banking and finance and fintech. Her clients include financial institutions, startups, e-commerce companies, payment service providers and cryptocurrency exchanges.

1 Takaful is an alternative insurance system designed to be compliant with the principles of Islamic finance. Under the Malaysian Islamic Financial Services Act 2013, takaful means an arrangement based on mutual assistance where participants agree to contribute to a common fund providing mutual financial benefits to participants or their beneficiaries on occurrence of pre-agreed events.

In relation to the issuance of e-money, the primary guidelines applicable to issuers of e-money in Malaysia are the updated electronic money guidelines (E-Money Guidelines) issued on 30 December 2022, which outline the broad principles and minimum standards to be observed by e-money issuers in relation to the operation of their e-money schemes.

With regard to the insurance and takaful business, in particular digital insurance business and digital takaful business, BNM has recently issued a policy document on the licensing and regulatory framework for digital insurers and takaful operators (DITOs) on 9 July 2024, setting out requirements that account for differences in the business and operating models of DITOs (compared to traditional insurers and takaful operators), the eligibility criteria for the licensing of DITO applicants, the application procedures and submission requirements and the overall regulatory requirements for licensed DITOs (including a foundational phase of three to seven years), which aims to support the development of digital insurance and takaful in Malaysia.

Islamic Financial Services Act 2013 (IFSA)

While the FSA provides for, amongst others, the regulation and supervision of financial institutions, payment systems operators and other relevant entities, the IFSA provides for similar regulation and supervision in regard to Islamic financial institutions, payment systems operators and other relevant entities in compliance with Sharia principles.

Money Services Business Act 2011 (MSBA)

It is provided under MSBA that any person who carries on money services business (which includes remittance business, money-changing business and wholesale currency business) must apply for the corresponding class of licence from BNM. The class, category or description of the money services business (MSB) licence required depends on the types of services to be offered by the applicant. Under the MSBA, appointment of a MSB agent by a MSB licensee must first be approved by BNM.

In light of the current market development in the remittance space, the MSBA has in 2024 been amended. The amendments include, amongst other things, a wider definition of 'remittance business' to cover different types of remittance transactions and the modus operandi used to undertake remittance transactions. Notably, certain activities that facilitate the transfer of funds will now be regarded as remittance businesses and will require a MSB licence from BNM.

Capital Markets and Services Act 2009 (CMSA)

Pursuant to CMSA, any person who operates a stock market, derivative market or recognised market (which term includes a peer-to-peer financing (P2P) platform, equity crowdfunding platform, property crowdfunding platform, digital assets exchange and e-service platform), or engages in regulated activities – such as fund management (which includes fund management in relation to portfolio management services, automated discretionary portfolio management, etc) and the provision of investment advices – is required to apply for and obtain the requisite licence or registration from the SC.

To operate a P2P financing platform, equity crowdfunding platform or a digital asset exchange (DAX), a person must be registered as a recognised market operator (RMO). SC issued the revised Guidelines on Recognised Markets (Recognised Market Guidelines) on 6 February 2024, which set out the requirements for the registration as an RMO and ongoing requirements that apply to RMOs. A recognised market essentially covers an alternative trading venue, marketplace or facility that brings together purchasers and sellers of capital market products. The level of regulation of a recognised market is less stringent as compared to approved markets (ie, approved stock markets of a stock exchange or derivatives markets of a derivatives exchange pursuant to Section 8 of CMSA).

With regard to robo-advisers – more specifically referred to as digital investment management (DIM) in Malaysia, whose scope of regulated activity is in 'automated discretionary portfolio management' – the DIM provider's services must involve automation of core components of portfolio management services. As part of its digital agenda for the capital market, SC has introduced the Digital Investment Management framework (under its existing licensing handbook and fund management guidelines), which sets out licensing and conduct requirements for offering such services to investors.

Regulations, policy documents and guidelines issued by BNM and SC pertaining to the FSA, IFSA, MSBA or CMSA

Some other key policy documents relevant to fintech players are as follows:

- policy document on risk management in technology (RMiT);
- policy document on operational risk integrated online network (ORION); and
- policy document on electronic know your customer (e-KYC).

Proposed Consumer Credit Act

In response to the growth in number of unregulated players in the consumer credit space, including companies that offer buy now pay later products/services, non-bank factoring and leasing companies, etc, the Public Consultation Paper on Consumer Credit Act (Part 2) has been published by the Consumer Credit Oversight Board Task Force (Task Force) with the support of the Ministry of Finance Malaysia (MOF), BNM and SC. This provides a comprehensive framework for regulating credit business (such as moneylending, pawnbroking, hire purchase, credit sale, buy now pay later schemes, factoring, leasing, etc) and credit service business (such as debt collection services, debt counselling, online crowdlending services, etc). The Consultation Paper requests feedback on the proposed regulatory framework and authorisation approach envisaged through the enactment of a proposed Consumer Credit Act.

As the deadline for submission of feedback on the Consultation Paper closed on 15 May 2023, the Task Force, together with MOF, BNM, SC and other regulators will be working towards finalising the consolidated credit industry regulatory framework, with the enactment of the Consumer Credit Act anticipated to take place in 2024.

The above is not exhaustive and only sets out some of the relevant key legislations that may apply to the business of a fintech player in Malaysia.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

Following the issuance of the Capital Markets and Services (Prescription of Securities) (Digital Currency and Digital Token) Order 2019, digital assets (ie, digital currency such as cryptocurrencies and digital tokens) are prescribed as 'securities' for purposes of Malaysian securities laws.

DAX

Pursuant to the Recognised Market Guidelines, a DAX operator is an RMO who operates an electronic platform that facilitates the trading of a digital asset and is required to be registered with the SC to facilitate the trading of a digital asset. SC will consider the following circumstances in determining whether a person may be deemed as operating, providing or maintaining a stock market or a derivatives market in Malaysia, and therefore may be considered an RMO:

- the stock market or derivatives market is operated, provided or maintained in Malaysia. This includes circumstances where the component parts of the stock market or derivatives market when taken together are physically located in Malaysia even if any of its component parts, in isolation, are located outside Malaysia; or
- the stock market or derivatives market is located outside Malaysia and actively targets Malaysian investors (ie, the operator or the operator's representative directly or indirectly promotes that market in Malaysia).

Initial exchange offering (IEO)

In line with digital currencies and digital tokens being prescribed as securities, SC has released the Guidelines on Digital Assets, which set out the requirements related to fundraising activities through a digital token offering, operationalisation of IEO platform and provision of digital asset custody. A person who seeks to operate an electronic platform which hosts IEO must be registered with the SC under the Guidelines on Digital Assets.

Digital assets custodian (DAC)

A DAC is a person who provides any of the services of safekeeping, storing, holding or maintaining custody of digital assets on the account of another person. A DAC is deemed to be providing capital market services and is required to be registered under section 76A of the CMSA.

A registered RMO or registered trustee who seeks to provide any of the aforesaid services must notify the SC of its intention prior to it providing the specified services. The SC may carry out an assessment on the registered RMO or registered trustee. The registered RMO or trustee shall be deemed to be registered as a DAC under the Digital Assets Guidelines, provided the SC is satisfied that the registered RMO or trustee is able to comply with the specified requirements under the Digital Assets Guidelines.

The above is not exhaustive and only sets out some of the key provisions regarding the legal framework of crypto assets in Malaysia.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

Payment system operators

Pursuant to FSA, a person who carries out the operation of a payment system (ie, a system or arrangement for the transfer, clearing or settlement of funds or securities) which enables the transfer of funds from one banking account to another, which includes any debit transfer, credit transfer or standing instructions but does not include the operation of a remittance system approved under Section 40 of MSBA, or provides payment instrument network operation which enables payments to be made through the use of a payment instrument, must be approved by BNM under the FSA. There are similar provisions under the IFSA.

Cross-border remittance service

Pursuant to MSBA, a person who carries out remittance business (defined in the MSBA as a business of transferring funds or facilitating the transfer of funds (regardless of the form, means or whether there is any movement of funds), on behalf of an originator inside or outside of Malaysia to a beneficiary inside or outside Malaysia, and the originator and the beneficiary may be the same person, but excludes such other businesses, activities, systems or arrangements as BNM may prescribe, is required to be licensed by BNM. Recent amendments to the MSBA have clarified that the term 'facilitating the transfer of funds' includes: offering services to transfer funds, accepting or receiving funds, transporting funds, arranging for transfer of funds, issuing receipt for transfer of funds, utilising a system to transfer funds, allowing an account to be used for transfer or receipt of funds, or engaging in any form of settlement activity, including net settlement, set-off and debt assignment, arising from transfer of funds.

BNM issued the Policy Document on Governance, Risk Management, and Operations for Money Services Business on 30 June 2022, which outlines the minimum standards that a MSB licensee must observe in implementing sound governance, appropriate risk management and robust internal control systems for their business. For instance, a MSB licensee is required to, inter alia, ensure that the exchange rates quoted by a MSB for all MSB transactions with its customers shall be based on the prevailing market rates when the transactions are executed, and the exchange rate used for the final transaction shall not be less favourable than the exchange rate disclosed to the customers.

Merchant acquiring services

Under the MAS Policy Documents, a merchant acquirer is required to be registered pursuant to Section 17 of the FSA to provide merchant acquiring services where it fulfils the following criteria, namely:

- enters into a contract with the merchants, resulting in a transfer of funds to the merchants by conducting or being responsible for fund settlement, or issuing fund settlement instructions;
- facilitates the merchant's acceptance of payment instruments; and

- is a direct participant (ie, a principal member) of payment instrument networks to provide merchant acquiring services.

Merchant acquirers are classified into large acquirers or small acquirers under the MAS Policy Documents, depending on their actual or projected amount of average monthly transaction value. While the requirements under the MAS Policy Documents generally apply to all acquirers, there are specific requirements that apply only to large acquirers.

While outsourcing arrangements are permissible pursuant to the MAS Policy Documents, merchant acquirers remain responsible and accountable for the services outsourced to any service provider (eg, payment facilitators, merchant recruitment agents, payment gateway service providers, IT service providers) under the outsourced arrangement.

Digital wallets

E-money is prescribed under the Financial Services (Designated Payment Instruments) Order 2013 as a designated payment instrument (whether tangible or intangible) that stores funds electronically in exchange of funds paid to the issuer and can be used as a means of making payments to any person other than the issuer. Pursuant to the E-Money Guidelines, e-money users may also send or receive funds to or from another user's e-money or bank account through peer-to-peer fund transfer service if the e-money issuer (EMI) is allowed to offer such service.

There are three categorisations of EMIs (standard EMI, limited purpose EMI and eligible EMI), which are determined based on the purpose of the e-money and market share.

The E-Money Guidelines set out the requirements that must be observed by EMIs such as:

- governance arrangements;
- operational and risk management requirements; and
- information technology requirements.

An EMI that acquires merchants for the purpose of accepting payment instruments including its own e-money shall be registered as a merchant acquirer under the FSA and shall also refer to the requirements in the MAS Policy Documents.

The above is not exhaustive and only sets out some of the key provisions regarding regulation of payment service providers and/or digital wallets in Malaysia.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

In Malaysia, BNM first introduced the Financial Technology Regulatory Sandbox Framework on 18 October 2016 to provide a regulatory environment that is conducive for the deployment of financial technology and to facilitate meaningful innovation in the Malaysian financial sector.

Through the regulatory sandbox, regulatory flexibilities may be granted to applicants to allow experimentation of fintech solutions in a live environment, subject to appropriate safeguards and regulatory requirements.

As part of its strategies to advance digitalisation of the financial sector, BNM issued an enhanced Financial Technology Regulatory Sandbox Framework (Framework) on 29 February 2024, which introduced two key enhancements to the Framework, namely simplifying the Sandbox's eligibility assessment to ensure that assessments are proportional with the development cycle of new innovations and introducing a risk-proportionate and accelerated track, referred to as the Green Lane, to facilitate faster testing of innovative solutions by granting regulatory flexibilities to financial institutions with strong risk management, governance and compliance capabilities.

Further, in September 2015, SC launched the Alliance of FinTech Community (aFINity) to act as a catalyst for fintech development in the Malaysian capital market. aFINity serves as a platform for ongoing interaction between the SC as a capital market regulator and the innovators, financial institutions, government agencies, investors and other fintech stakeholders. Through aFINity, SC also collaborates with international regulators to promote innovation, including by signing innovation co-operation agreements (fintech bridges) and frameworks.

Both SC and BNM regularly organise fintech conferences to bring together policymakers, innovators, investors and financial service providers for networking, collaboration and discussions. These events also serve to raise awareness in respect of issues relating to financial sectors, to promote the digitalisation of the Malaysian economy and advance policy initiatives.

The SC has also launched FIKRA ACE, a three year initiative aimed at enhancing the Islamic capital market ecosystem by facilitating development of Islamic fintech. The FIKRA Accelerator, as a component of FIKRA ACE, is a platform for fintech startups to develop innovative solutions, from ideation to minimum-viable product that may contribute to the advancement of Islamic finance through a structured six to eight weeks accelerator programme consisting of workshops, mentorship, networking activities and funding facilitation. Following the success of the first cohort of the FIKRA Accelerator in 2023, the SC is now inviting applicants for its 2024 cohort, which is expected to begin in August 2024 and is open to local and international applicants with less than three years market presence.

Furthermore, BNM has also collaborated with a number of partners as part of its continuous efforts to support fintech players. For instance, BNM has partnered with the Malaysia Digital Economy Corporation (MDEC), an agency under the Ministry of Communication and Multimedia Malaysia aimed at accelerating the digital economy growth of Malaysia, to launch several initiatives. This included the launch of the Fintech Booster Program in 2020 to assist Malaysian-based fintech players in better understanding of the legal, compliance and regulation requirements for their development of innovative products and services.

In terms of special support via funding, various initiatives have been implemented. For example, the Digital Innovation Fund (DIGID) was set up by SC to co-fund innovative projects that demonstrate the use of technology to allow new and competitive propositions in the Malaysian capital markets. Applicants for DIGID must be a capital market player regulated by SC with revenue of up to RM100 million for mid-tier companies, or have a headcount of up to 75 staff or revenue of up to RM20 million

for small and medium enterprises. Meanwhile, Malaysia Debt Ventures Berhad (MDV) was established by the government of Malaysia in 2002 with the objective of providing flexible and innovative financing facilities to develop the ICT sector in Malaysia and assisting startups. Various tax exemptions have also been introduced to boost the take up of certain fintech solutions (eg, certain tax exemptions for investors in equity crowdfunding platforms and stamp duty exemptions on instruments on P2P platforms that fulfil certain criteria).

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

BNM recognises the benefits of open application programming interface (Open API) standardisation initiatives to the industry and has developed strategies for the adoption of Open API within the financial services sector.

In the first quarter of 2018, BNM formed the Open API Implementation Groups at industry level for the banking/Islamic banking and insurance/takaful industries, with representation of a few fintech companies. The Open API Implementation Groups, in consultation with BNM, will continue to identify and develop standardised Open APIs for high-impact use cases. The aim of the Open API Implementation Groups was to pursue standardisation of Open APIs which would enhance third party developers' access to open data made available by banks/Islamic banking and insurance/takaful operators.

In January 2019, BNM published the policy documents on Publishing Open Date using Open API (API Guidelines) that are applicable to licensed financial institutions (ie, banks, Islamic banks, insurers and takaful operators) intending to publish Open Data APIs. The API Guidelines set out the recommendation of BNM in developing and publishing Open APIs. While not obliged, the financial institutions are encouraged to adhere to and adopt these specifications to ensure industry-wide publication of standardised Open Data API.

Further, the Interoperable Credit Transfer Framework (ICTF) was issued by BNM to foster a competitive and innovative payment landscape in Malaysia by enabling interoperability of credit transfer services and promoting collaborative competition through access to shared payment infrastructure. Part of the ICTF encourages an operator of a shared payment infrastructure to publish APIs and establish an innovation sandbox facility for use by any third party for the purpose of experimenting and testing of a new product, service or solution.

Meanwhile, BNM's Open API official portal offers access to relevant datasets information available on the BNM website for third-party developers and the public to use to build their own applications.

New Zealand

Zac Kedgley-Foot*
Bell Gully, Wellington
zac.kedgley-foot@bellgully.com

Campbell Pentney†
Bell Gully, Auckland
campbell.pentney@bellgully.com

Richard Massey‡
Bell Gully, Auckland
richard.massey@bellgully.com

Hamish Robinson§
Bell Gully, Wellington
hamish.robinson@bellgully.com

Ainsleigh Hall**
Bell Gully, Auckland
ainsleigh.hall@bellgully.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

In New Zealand, the regulatory regime that applies to financial services generally does not distinguish between fintech and other financial services: the same regulatory concepts apply across the board. In addition to registration and licensing requirements for certain financial service providers, the regulatory regime includes securities, consumer credit and responsible lending laws, market conduct, privacy and data protection, anti-money laundering rules, and other prudential regulations for banks, non-bank deposit takers and insurers.

Financial services and products regulation

The Financial Markets Conduct Act 2013 (FMC Act) is the principal legislation in New Zealand that regulates the provision of financial services and products (defined at the end of this section). It contains various regimes that apply to offers of financial products, and the provision of financial services, in New Zealand. The most relevant regimes for fintech are as follows.

---

* Zac is a partner and specialist banking and finance lawyer, who is experienced in advising on a broad range of banking, debt capital markets and derivatives transactions and financial services regulation.

† Campbell is a special counsel who specialises in indirect taxes such as GST and custom duties as well as emerging technologies, including blockchain and cryptocurrency.

‡ Richard is a partner who delivers strategic advice across a range of sectors, with a focus on consumer law, e-commerce, and emerging legal and regulatory requirements.

§ Hamish is a lawyer who specialises in banking and finance law. He advises on banking, debt capital markets and the regulation of financial products and services in New Zealand, including in respect of emerging technologies.

** Ainsleigh is a lawyer who specialises in banking and finance law and financial services regulation. She advises on domestic and international banking and capital markets transactions and the regulation of financial products, services and markets in New Zealand.

Fair dealing in relation to financial products and financial services

The 'fair dealing' provisions set out in Part 2 of the FMC Act prescribe standards for dealing in financial products and the supply (or possible supply) of financial services, and impose civil liability on anyone who engages in misleading or deceptive conduct in relation to financial products and financial services, which would include a person making misleading or deceptive statements in any offering or marketing material.

Sections 19 to 23 of the FMC Act provide for fair dealing in relation to financial products and financial services (including financial advice, client money or property services and discretionary investment management services (see below)) by prohibiting misleading or deceptive conduct, and false, misleading or unsubstantiated representations.

The fair dealing provisions in the FMC Act apply to conduct outside New Zealand by a person carrying on business in New Zealand to the extent that conduct relates to the supply of a financial service that occurs in New Zealand.

Regulated offers of financial products

Regulated offers of financial products to persons in New Zealand must comply with certain disclosure, registration and other requirements set out in the FMC Act. A regulated offer means an offer of financial products to one or more investors where at least one of those investors requires disclosure under the FMC Act (ie, at least one investor is not a wholesale investor, and the offer does not fall within an exemption that applies to the offer as a whole due to its nature or the nature of the issuer).

The principal disclosure obligations that apply to regulated offers of financial products are to:

- prepare a product disclosure statement (PDS) for the offer;
- lodge the PDS with the Registrar of Financial Service Providers; and
- supply to the Registrar of Financial Service Providers all the information that the register entry (if any) is required to contain.

The PDS and the register entry must include all material information about the offer of a financial product and be up-to-date, accurate and understandable. The FMC Act also contains restrictions on advertising a regulated offer (including an intended offer) of financial products.

In addition to the disclosure requirements, a person making a regulated offer of debt securities or managed investment product must comply with various governance and registration requirements (including a requirement to have a trust deed/governing document that complies with the FMC Act and to appoint a licensed supervisor).

Licensing of market services and financial product markets

The FMC Act imposes specific registration, licensing, disclosure and conduct obligations on providers of the certain financial services, which include the following.

Financial advice

In order to give regulated financial advice (ie, financial advice that is given in the ordinary course of a business and does not fall within a number of specific exceptions) to clients, a person must obtain a financial advice provider (FAP) licence or operate under another FAP's licence. FAP licences are subject to specific conditions. In addition, the financial advice regime imposes certain conduct and disclosure obligations on FAPs, which include duties relating to prioritising clients' interests, exercising care, diligence and skill, complying with the applicable code of conduct and not recommending the acquisition of financial products that contravene the financial advice regime.

The financial advice regime in New Zealand extends to robo-advice.

Financial product markets

The FMC Act requires that, subject to certain exemptions, a person must not operate a financial product market in New Zealand unless the person has a licence to do so. A financial product market is a facility where financial products are bought or sold, or where offers or invitations to buy or sell financial products are made. A financial product market is taken to be operated in New Zealand in a number of circumstances, including if it is promoted to investors in New Zealand by or on behalf of the operator.

Obtaining a financial product market licence is time-consuming and expensive, as the licence can only be issued by the responsible minister on advice of the regulator. Among other conditions and obligations, a licensed financial product market must be operated under market rules that are approved under, and comply with, the FMC Act.

P2P lending or crowdfunding intermediaries

There is no requirement for a peer-to-peer (P2P) lending or crowdfunding service to be licensed; however, providers may choose to apply for a licence because there are less onerous disclosure requirements for borrowers that offer debt securities through a licensed P2P lending service or companies who want to offer shares through a licensed crowd funding service (in particular, not being required to supply a PDS).

In order to obtain a licence, the applicant must demonstrate that it meets certain eligibility criteria set out in the FMC Act and the corresponding regulations, including that it has fair, orderly, and transparent systems and procedures for providing the service, it has an adequate fair dealing policy and it has adequate systems and procedures for ensuring that each issuer does not raise more than NZ$2m in any 12-month period under the service. A licensed P2P lending or crowdfunding service must comply with certain disclosure and conduct obligations (eg, supply a disclosure statement (different to a PDS), provide prescribed transaction information to the investor and enter into a client agreement with the investor before the investor applies for or acquires any financial products under the service), with the standard conditions (eg, in relation to outsourcing and governance arrangements) and any specific conditions imposed by the regulator when issuing the licence.

Derivatives issuers

Under the FMC Act, a person acting as a derivatives issuer (ie, a person that is in the business of entering into derivatives) in respect of a regulated offer of derivatives (see the paragraph titled 'Regulated offers of financial products' above) that is made by the derivatives issuer must be licensed. Licensed derivatives issuers have a variety of compliance obligations, including complying with various client fund and client agreement rules, record keeping requirements and reporting obligations. In addition, a licensed derivatives issuer must ensure compliance with the conditions attached to its derivatives issuer licence, which include restrictions on outsourcing arrangements, financial resource requirements and minimum standards on governance arrangements.

Discretionary investment management service

Licensing obligations apply to persons who are in the business of providing a 'discretionary investment management service' (DIMS) to retail clients. This includes arrangements where the provider decides which financial products to acquire, or dispose of, on behalf of an investor and in doing so, is acting under an authority to manage some or all of the investor's holdings of financial products (ie, a separately managed account).

Licensed DIMS providers must comply with certain conduct and DIMS-specific disclosure obligations, including to ensure that a disclosure statement is provided to each investor before an investment authority is granted, enter into a written client agreement for the DIMS, ensure clients' money and property is held by an independent custodian, and comply with certain record keeping and reporting obligations.

In the case of some of the above market services, a licence will not be required to offer that service to wholesale investors only. For example, to provide financial advice to wholesale clients only, a licence is not required but certain duties will still apply. These include the duty to give priority to your client's interests when there is a conflict, and the duty to exercise care, diligence and skill when giving advice.

Client money or property services

A provider of a client money or property service is subject to disclosure and conduct obligations under the FMC Act and the corresponding regulations (ie, regulated), unless a limited set of exclusions applies, such as in relation to a provider that is the operator of a designated settlement system or a derivatives issuer. A client money or property service is the receipt of client money or client property by a person and the holding, payment, or transfer of that client money or client property and includes a custodial service.

A regulated client money or property service provider is, among other requirements, subject to the following disclosure, conduct and handling obligations:

- to hold or ensure that client money or client property is held on trust for the client; and
- to ensure that the client money and client property are held separate from money or property held by or for the provider on its own account.

A provider who provides a custodial service that is a regulated client money or property service and that relates to a financial product (subject to a number of exemptions) (ie, a custodian) has additional obligations imposed by regulations. Under these regulations, custodians have reporting, reconciliations, assurance engagement and general conduct obligations among others.

If a provider of regulated client money or property services only deals with certain categories of wholesale clients, it will not be subject to the disclosure and handling obligations that apply to providers under the FMC Act and the corresponding regulations, but will be required to comply with certain high-level conduct obligations in the FMC Act.

Relevant definitions

The following definitions are relevant to the above summary of regulatory regimes under the FMC Act.

Financial services

The definition of financial services is broad, and several of the services that are captured under the definition will be relevant for fintech, including:

- providing market services (see the paragraph titled 'Licensing of market services and financial product markets' above);
- providing a regulated client money or property service (including a custodial service);
- keeping, investing, administering, or managing money, securities or investment portfolios on behalf of other persons;
- being a creditor under a credit contract;
- acting as an offeror of financial products offered in certain circumstances;
- operating a money or value transfer service;
- issuing or managing the means of payment (including electronic money);
- changing foreign currency; and
- trading financial products or foreign exchange on behalf of other persons.

Financial products

Financial products under the FMC Act are of four types (with each type, in turn, having its own definition): debt securities, equity securities, managed investment products, and derivatives. In addition, the regulator has a 'call-in' power under the FMC Act. The regulator may declare that a security (the definition of which is wider than the definition of financial product and which could, for example, include a fintech product that would not otherwise be a financial product) is a financial product of a particular kind. Before making such a declaration, the regulator is required to consult with those who would be substantially affected, and a declaration cannot be retrospective.

Registration of financial service providers

The Financial Service Providers (Registration and Dispute Resolution) Act 2008 (FSP Act) applies to persons who are in the business of providing a financial service (see the definition titled 'Financial services' above) in New Zealand. The FSP Act requires financial service providers to register on an online register for each financial service they provide. In addition, if a person provides a financial service to a client that is not a wholesale client under the FSP Act, they may also be required to become a member of an approved dispute resolution scheme.

However, a financial service provider will not be required to comply with the FSP Act if it meets certain requirements, including that it does not have a place of business in New Zealand and does not provide the relevant financial service to clients that are not wholesale clients under the FSP Act in New Zealand.

Privacy and data protection

The Privacy Act 2020 (Privacy Act) is New Zealand's primary privacy and data protection legislation. The Privacy Act does not distinguish between fintech businesses or other agencies, but rather applies to any business in New Zealand, and overseas business carrying on business in New Zealand, in relation to the collection, storage, use and disclosure of personal information relating to an identifiable individual.

The Act sets out 13 'information privacy principles'. These include, for example, that an agency should take reasonable steps to inform the individual of various specified matters (including that personal information is being collected and the purposes for which the information will be used) before the information is collected or as soon as practicable thereafter. In practice, this requirement is usually met by covering these items in a privacy policy. The principles also restrict disclosure of personal information and include specific restrictions for cross-border disclosure (although that is permissible in limited circumstances including where the disclosing agency believes on reasonable grounds that the recipient is: 'subject to privacy laws that, overall, provide comparable safeguards' to those under the Privacy Act or is required to protect the information in a way that, overall, provides comparable safeguards to those under the Privacy Act, such as under a data processing agreement).

The Privacy Act repealed and replaced its predecessor (the Privacy Act 1993) on 1 December 2020. The new Privacy Act is intended to reflect changes in technology and the ways in which personal information is collected, stored and shared. One of the key changes was the introduction of mandatory reporting of 'notifiable privacy breaches' to the Officer of the Privacy Commissioner and affected individuals. For that purpose, a 'privacy breach' is defined broadly and can comprise:

- unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of personal information; or
- an action that prevents an agency from accessing personal information on either a temporary or permanent basis.

A privacy breach is 'notifiable' if it is reasonable to believe it has caused serious harm to an affected individual or is likely to do so. Whether harm is 'serious harm' depends on the circumstances of the

privacy breach and requires an assessment on a breach-by-breach basis, taking into account specific factors set out in the Privacy Act.

Consumer credit and responsible lending laws

The Credit Contracts and Consumer Finance Act 2003 (CCCFA) contains New Zealand's credit contracts legislation.

It imposes a range of obligations on lenders in respect of consumer credit contracts (ie, loans provided to individuals for personal, domestic or household purposes). Those obligations include requirements to comply with responsible lending conduct obligations and specific disclosure requirements. Certain provisions of the CCCFA, which address oppressive credit contracts and repossession rights, also apply to all credit contracts (ie, both business and consumer loans).

In December 2019, the CCCFA was amended to address a number of perceived issues in the credit market, with a particular focus on addressing harm to vulnerable consumers. The amendments included expanded requirements to carry out 'responsible lending', including:

- more prescriptive requirements regarding how and when affordability and suitability tests must be conducted; and
- introduction of a new certification, and fit and proper person requirement for lenders, their directors and senior managers.

The amendments were implemented in stages, with the final amendments taking effect from December 2021. Following criticism of the extensive reach of the new obligations, a series of targeted amendments were implemented to partially reduce the compliance burden on lenders. Further changes are expected under the new coalition government (including likely amendments to the suitability and affordability regulations) although the details of the reforms are yet to be confirmed. In addition, the government has confirmed changes to the treatment of 'buy now, pay later' (BNPL). BNPL products have not previously been treated as 'consumer credit contracts' for the purposes of the CCCFA (because they do not charge interest or credit fees, or take security). Under new regulations (which take effect from 2 September 2024) BNPL products will be subject to certain targeted aspects of the CCCFA. As a result, BNPL providers will need to comply with various CCCFA obligations, including:

- ensuring that default fees are 'reasonable' (ie, that they are calculated based on the actual cost of defaults);
- assisting borrowers to make informed decisions and treating them reasonably and ethically; and
- providing relief to borrowers who face 'unforeseen hardship'.

Some of the CCCFA obligations have been modified under the regulations to suit the BNPL context. In particular, BNPL providers will not have to carry out any affordability assessments (provided they comply with certain credit reporting and disclosure requirements).

Anti-money laundering and countering financing of terrorism

The Anti-Money Laundering and Countering Financing of Terrorism Act 2009 (AML/CFT Act) imposes obligations on reporting entities. A reporting entity includes a financial institution. The term financial institution is broadly defined in the AML/CFT Act and captures several of the services covered by the definition of financial services (see the paragraph titled 'Financial services' above).

The AML/CFT Act is silent on whether it applies to reporting entities constituted (or otherwise located) outside New Zealand. However, the AML/CFT supervisors have issued a guidance note (Guidance Note) on the territorial scope. The Guidance Note states that the definition of reporting entities in the AML/CFT Act implies a place of business in New Zealand from where the activity is directed and, therefore, an overseas person carrying on business in New Zealand and engaged in one or more of the activities listed in the AML/CFT Act in New Zealand will be a reporting entity under the AML/CFT Act, whereas an overseas person that is not carrying on business in New Zealand is unlikely to be a reporting entity under the AML/CFT Act.

Among other requirements, a reporting entity must:

- establish, implement, and maintain a compliance programme that complies with the requirements in the AML/CFT Act, is based on a risk assessment and includes internal procedures, policies and controls to detect money laundering and the financing of terrorism; and
- manage and mitigate the risk of money laundering and financing of terrorism.

In 2021, the Ministry of Justice and the regulators initiated a statutory review of the AML/CFT Act and on 30 June 2022 released its report with 215 recommendations. The outcome of the review and report is expected to be a 'once in a generation' reform of the existing regime, changing and modernising the AML/CFT Act and associated regulations. The first set of amending regulations (it is expected that additional amendments to the regime will be introduced in the future) has already been implemented.

These regulations will enter into force on a staggered basis with the first part of the regulations having entered into force on 31 July 2023. By way of example, 'a person who, in the ordinary course of business, provides safekeeping or administration of virtual assets on behalf of any person' is now declared to be a financial institution (and, therefore, a reporting entity), meaning that the AML/CFT will apply to it (subject to the AML/CFT Act's territorial scope as set out in the Guidance Note).

Overseas companies

The Companies Act 1993 requires an overseas company that commences to carry on business in New Zealand to register under Part 18 of the Companies Act within 10 days of doing so. An overseas company is a body corporate that is incorporated outside New Zealand.

The application of the carrying on business rules to an overseas company that does not have an office or other physical presence in New Zealand is uncertain. However, relatively minimal activity can constitute carrying on business. It is an aggregate assessment that takes into account all of the relevant overseas company's activities in New Zealand.

Fair trading legislation

The Fair-Trading Act 1986 (FTA) regulates conduct by persons in trade in New Zealand. Subject to a limited 'in-trade exemption', it is not possible to contract out of the FTA.

The FTA sets out a series of 'unfair conduct' prohibitions. The most important prohibition provides that 'no person shall, in trade, engage in conduct that is misleading or deceptive or is likely to mislead or deceive'. In addition, under the FTA, the making of unsubstantiated representations or false or misleading representations in connection with the supply, or possible supply, of goods or services is also prohibited. These prohibitions are similar to the fair dealing prohibitions in relation to financial products and financial services outlined in the paragraph titled 'Fair dealing in relation to financial products and financial services' above.

The FTA also contains a prohibition on including or enforcing any term in a standard form consumer contract or standard form small trade contract that the court has declared to be an 'unfair contract term'. The FTA sets out a so-called 'grey list' of terms that may be unfair in such a contract.

In 2022, a new prohibition on unconscionable conduct was introduced. Unconscionable conduct is not defined in the FTA; therefore, it is left to the courts to determine what type of conduct will be unconscionable. This prohibition applies whether (1) there is a system or pattern of unconscionable conduct, (2) a particular individual is identified as disadvantaged, or likely to be disadvantaged, by the conduct, or (3) a contract is entered into. In addition, it cannot be contracted out of.

Unsolicited electronic messages

The Unsolicited Electronic Messages Act 2007 (UEMA) regulates the sending of commercial electronic messages with a 'New Zealand link'. Under the UEMA, a person must not send, or cause to be sent, a commercial electronic message (such as an email, text or instant message) with a New Zealand link without consent from the recipient.

The UEMA requires that all commercial electronic messages with a New Zealand link must include accurate sender information and a functional unsubscribe function (ie, a clear and operational 'opt-out' feature).

Prudential regulation

New Zealand has prudential regulatory regimes that apply to banks, non-bank deposit takers (NBDTs) and insurance companies. The New Zealand Reserve Bank has regulatory, licensing and supervisory oversight of finance companies, insurers, building societies and credit unions, and it operates New Zealand's wholesale payment and settlement systems.

NBDTs are entities that offer debt securities to the New Zealand public and are in the business of borrowing and lending money, or providing financial services, or both. This includes finance companies, credit unions, building societies and can include entities offering certain types of fintech services (see, for example, the paragraph titled 'Platforms that provide fiat currency wallet or lending/deposit services' in Question 2) but excludes registered banks.

A major reform of New Zealand's regulatory regime in relation to banks and NBDTs is currently underway with the Deposit Takers Act 2023 (DTA) having received Royal Assent on 6 July 2023. The DTA will come into force on a staggered basis, with the initial focus being on the implementation of the 'depositor compensation scheme' contemplated by the DTA. It is expected that the DTA will fully come into force in 2028, establishing the new regime in respect of deposit takers, after a multi-year work programme to develop policy, standards and regulations to support the commencement of the new regime.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

Aside from taxation and certain AML/CFT regulations (see the paragraph titled 'Anti-money laundering and countering financing of terrorism' under Question 1), there are no specific regulatory regimes that apply to crypto assets (eg, Bitcoin or USDC) and crypto services (eg, cryptocurrency trading and crypto lending/deposit programmes) in New Zealand. However, the provision of crypto assets and crypto services in New Zealand may be regulated under regulatory regimes of general application.

Regulatory regimes applicable to crypto assets

A determination of the regulatory regimes that apply to crypto assets and providers of crypto services requires analysis of the particular crypto assets and crypto services being provided. Below is a high-level indication of the regulatory regimes that may apply to providers of crypto assets and/or crypto services (with a focus on cryptocurrency exchange providers).

Registration requirement for crypto asset platforms

A crypto asset or crypto service provider is required to be registered on the Financial Service Providers Register for any financial services (see the definition titled 'Financial services' under Question 1) that it provides. This may include, in relation to a cryptocurrency exchange provider, the following financial service categories:

- operating a money or value transfer service;
- keeping, investing, administering, or managing money, securities, or investment portfolios on behalf of other persons;
- operating a financial product market; and/or
- providing a regulated client money or property service.

The provider may also be required to join an approved dispute resolution scheme and comply with certain ongoing obligations (see the paragraph titled 'Registration of financial service providers' under Question 1).

Fair dealing in relation to financial products and financial services

A crypto assets or crypto service provider may also be subject to the fair dealing regulatory regime outlined in the paragraph titled 'Fair dealing in relation to financial products and financial services' under Question 1, which prescribes standards for dealing in financial products and the supply (or possible supply) of financial services.

If the fair dealing regulatory regime does not apply, the provider may nevertheless be required to comply with the FTA regulatory regime (outlined in the paragraph titled 'Fair Trading Legislation' under Question 1).

Platforms that facilitate trading crypto assets that are financial products

A crypto assets or crypto service provider may also be subject to the requirement to be licensed to operate a financial product market (see the paragraph titled 'Financial product markets' under Question 1) if one or more of the crypto assets traded on the platform is a financial product under the FMC Act.

The correct FMC Act classification of a particular crypto asset (ie, whether it will constitute a financial product) requires an analysis of the specific features of that crypto asset. By way of example, while we consider that prominent cryptocurrencies such as Bitcoin and Ether do not constitute a financial product under the FMC Act, certain stablecoins (for example, USDC) will likely constitute a financial product.

Platforms that provide fiat currency wallet or lending/deposit services

If the provider offers a fiat currency wallet account or a lending/deposit service (whereby the client provides fiat currency to the platform in exchange for, for example, interest) to clients in New Zealand that essentially operates as a deposit account (and so the funds in that account may not necessarily be used immediately to convert into cryptocurrency), and those funds are at any point not held in a separate trust account maintained with a registered bank, then this could be considered a debt security (and, therefore, a financial product) and attract a considerable regulatory burden (see the paragraph titled 'Regulated offers of financial products' under Question 1).

The provision of a fiat currency wallet account or a lending/deposit service may also trigger the application of the regulated client money or property service regulatory regime if the provider of the crypto service holds, pays, or transfers client money or client property in connection with crypto assets that are financial products (see the paragraph titled 'Client money or property services' under Question 1).

If a fiat currency wallet account or a lending/deposit service is a debt security, this could result in the provider being subject to the complex NBDT regulatory regime (see the paragraph titled 'Prudential regulation' under Question 1).

A lending and deposit service in relation to crypto assets (whereby the client provides crypto assets to the provider in exchange for, for example, interest paid in the form of crypto assets) may also constitute a financial product, requiring the provider to comply with the onerous disclosure and

governance rules in the FMC Act (see the paragraph titled 'Regulated offers of financial products' under Question 1).

Registration as an overseas company

The requirement to be registered as an overseas company in New Zealand (including a number of continuing obligations) under the Companies Act 1993 would apply to providers offering crypto assets or services that are carrying on business in New Zealand (see the paragraph titled 'Overseas companies' under Question 1). Registration as an overseas company would also invoke the application of New Zealand's anti-money laundering regime (see the paragraph titled 'Anti-money laundering and countering financing of terrorism' under Question 1).

Taxation of crypto assets

Until recently there was no specific New Zealand tax legislation dedicated to crypto assets. Therefore, the general tax provisions prevailed: as crypto assets are treated as property under New Zealand law, the usual tax rules for property sales applied. While New Zealand does not have a capital gains tax, income tax is payable on any profits derived from the disposal of property that was acquired for the purpose of resale. The Inland Revenue Department's general view is that crypto assets such as Bitcoin will generally be presumed to be acquired for resale, meaning that they are treated the same as gold bullion. It is possible that some other crypto assets may be treated as acquired for some other purpose (such as staking income) and therefore the proceeds of sale would not be taxed.

Recently, the New Zealand tax laws were updated to provide for two changes specific to crypto assets:

- the New Zealand GST legislation was updated to confirm that crypto assets are not subject to GST when sold. However, this does not extend to non-fungible tokens (NFTs) which are still potentially subject to GST;
- the income tax legislation was amended so that crypto assets are generally exempt from the financial arrangement rules. These rules are intended to apply to financial instruments such as certain bonds so interest income payable on redemption is instead taxed gradually over the period of the investment.

Inland Revenue has also provided its interpretation of the tax treatment of forks and airdrops, along with employee remuneration paid in crypto assets. Further developments to clarify the tax treatment of more advanced crypto asset transactions, such as decentralised lending, has been expected for some time but there has been very little development on this front. We are not aware of any upcoming changes that would impact the taxation treatment of crypto assets at this stage.

Regulatory developments

There are currently no laws specifically aimed at regulating providers of crypto assets or related products and services. However:

- legislators are considering taxation aspects of crypto assets;
- some major reforms of the AML/CFT Act have already been implemented and further reforms are expected to follow (see the paragraph titled 'Anti-money laundering and countering financing of terrorism' under Question 1);
- the Reserve Bank of New Zealand is consulting on the future of money, with potential plans for a New Zealand issued central bank digital currency; and
- following a Parliamentary inquiry established in July 2021 to consider 'the current and future nature, impact and risks of cryptocurrencies', a select committee of the New Zealand Parliament has released a report with 22 recommendations for the New Zealand Government, including recommendations to bring certain digital assets within the ambit of the regulated client money or property service and the regulated financial advice regimes (see the paragraphs titled 'Client money or property services' and 'Financial advice' under Question 1). However, the report did not recommend a bespoke regulatory regime to be adopted in New Zealand for digital assets.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

As per the position in relation to crypto assets and crypto services, there are no specific regulatory regimes that apply to fintech payment service providers (eg, electronic money) and/or digital wallets. We summarise the potentially applicable regimes below.

- Part 18 of the Companies Act 1993, which requires the registration of overseas companies carrying on business in New Zealand (see the paragraph titled 'Overseas companies' under Question 1) and the AML/CFT Act, if the provider is carrying on business in New Zealand/required to register as an overseas company (see the paragraph titled 'Anti-money laundering and countering financing of terrorism' under Question 1).
- The FSP Act, which requires persons in the business of providing a financial service (see the definition titled 'Financial services' under Question 1) to register under that Act and, in certain circumstances, to join an approved dispute resolution scheme (see the paragraph titled 'Registration of financial service providers' under Question 1).
- The provisions of the FMC Act and the corresponding regulations that apply to regulated offers of financial products in New Zealand. Similarly to the position outlined above in relation to fiat currency wallets offered in connection with crypto assets, onerous disclosure and governance obligations arise where the payment or digital wallet services offered by a provider constitute a regulated offer of debt securities (see the paragraphs titled 'Regulated offers of financial products' under Question 1 and 'Platforms that provide fiat currency wallet or lending/deposit services' under Question 2).
- Certain laws of more general application that would apply – dealing with issues such as unsolicited emails, privacy, and fair dealing (see, for example, the paragraphs titled 'Privacy and data protection', 'Fair trading legislation' and 'Unsolicited electronic messages' under Question 1).

In May 2022, the Retail Payment System Act was passed into law. It introduced a new regulatory regime that governs New Zealand's retail payments system and entities involved in the retail payments system (such as banks, merchants, non-bank merchant acquirers and card schemes).

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

There are no government-led innovation hubs or accelerators specific to fintech. In addition, the relevant regulators in New Zealand have taken the view that New Zealand's legislation is sufficiently flexible, along with the principled approach of regulators, that no specific sandbox is needed.

However, there are a number of initiatives that can provide support to fintech businesses. For example:

- there is an R&D tax incentive that is delivered jointly by Callaghan Innovation and the Inland Revenue Department which offers a 15 per cent tax credit on eligible research and development (R&D) expenditure; and
- Callaghan Innovation is a government innovation agency that also provides a range of innovation and R&D services, including assisting with technology and product development, experts and R&D funding.

There are also various private sector initiatives promoting fintech. For example, the New Zealand Financial Innovation and Technology Association (FinTechNZ) is an industry working group that is funded by members from the following sectors: financial services providers, technology innovators, investor groups, government regulators and financial educators. The purpose of FinTechNZ is to contribute to the prosperity of New Zealand through technology innovation.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

In June 2023, the Government issued a draft of the Customer and Product Data Bill, which establishes a 'consumer data right' (CDR) in New Zealand. The draft Bill sets out significant new rights for consumers and small businesses to control access to their data. The proposed CDR regime will initially focus on the banking sector, and is likely to facilitate the growth in third-party fintechs offering services to banking customers, including budgeting tools, comparison services and customised financial insights. It will be extended to other sectors in due course, which the government has confirmed 'may include the energy, finance, insurance, and health sectors'.

The CDR is intended to create a statutory right for consumers and small businesses to require entities holding their data such as banks ('data holders') to share that information with accredited third-party services such as product comparison websites ('accredited requestors').

Significantly, the draft Bill proposes 'action initiation' – allowing authorised third parties to make decisions on behalf of customers. For example, fintechs could be authorised to initiate customer payments or change a customer's online profile, with the customer's prior consent.

The draft Bill applies to data about 'customers', which includes any person (whether an individual or a business) that acquires goods or services from a data holder. The draft Bill does not exhaustively define what customer data is subject to the CDR regime, although it provides that customer data will include personal information within the meaning of the Privacy Act. The discussion paper accompanying the draft Bill explains that 'derived data' is intended to be subject to the CDR regime, which may prove a contentious issue. (In Australia, a similar proposal was criticised by the Australian Banking Association on the basis that it may compromise data holders' proprietary insights, ie, data enriched by the institution using their own internal models or other intellectual property). Submissions on the draft Bill closed in July 2023.

Singapore

Adrian Ang*
Allen & Gledhill, Singapore
adrian.ang@allenandgledhill.com

Benjamin Samynathan†
Allen & Gledhill, Singapore
benjamin.samynathan@allenandgledhill.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

Fintech-related legal work in Singapore covers a wide range of topics and will typically include financial and regulatory compliance (ie, whether a fintech product or service involves the conduct of a regulated activity that must be provided under a licence: if so, the nature of the required licence or whether an exemption or exclusion from licensing requirements is applicable), technology contracts, data protection and intellectual property issues and financing (ie, regulatory due diligence in relation to investments in fintech companies). We would highlight that any fintech businesses planning to provide services to persons in Singapore or from Singapore to persons elsewhere should consider if they are engaging in any regulated activities, and if so, whether a licence is required or whether an exemption or exclusion from licensing requirements is applicable.

Key regulatory authorities

The Monetary Authority of Singapore (the MAS) is Singapore's central bank and integrated regulator and supervisor of financial institutions in Singapore. The MAS regulates financial institutions in the banking sector (eg, deposit-taking institutions, full banks, wholesale banks, merchant banks and finance companies), capital markets sector (eg, capital markets entities such as fund managers, real estate investment trust managers, corporate finance advisers, trustees, dealers, credit rating agencies and financial advisers), insurance sector (eg, insurance companies and insurance brokers such as licensed insurers, authorised reinsurers and registered insurance brokers) and the payments sector (eg, payment service providers and payment systems, including clearing and settlement systems).

The Registry of Moneylenders oversees the registration and regulation of moneylenders in Singapore, and the Enterprise Singapore Board is the regulatory body responsible for administering the Commodity Trading Act 1992, which regulates activities involving spot commodity trading.

---

* Adrian is a Partner in the Financial Services Department and is Co-Head of both the company's Fintech Practice as well as its ESG & Public Policy Practice.

† Benjamin is an Associate in the Financial Regulatory and Compliance Practice at Allen & Gledhill.

Primary legislation

Securities and Futures Act (SFA)

The SFA regulates organised markets, trade repositories, clearing facilities, capital markets services intermediaries such as broker-dealers, corporate finance advisers, fund managers (including those handling crypto funds) and custodians.

Financial Advisers Act (FAA)

The FAA regulates the provision of financial advice on investment products and arranging of life insurance policies by intermediaries. This would include businesses that give advice on investment products.

Insurance Act (IA)

The IA regulates the conduct of life insurance businesses, general insurance businesses, general insurance agents and insurance brokers.

Payment Services Act (PS Act)

The PS Act entered into effect on 28 January 2020, and regulates the provision of payment systems adopting an activity-based approach. There are seven types of payment services or activities that are regulated under the PS Act:

- e-money issuance;
- account issuance;
- domestic money transfer services;
- cross-border money transfer services;
- merchant acquisition services;
- money changing services; and
- digital payment token (DPT) services.

We set out further activities that will be regulated by the PS Act in the near future in Question 2.

Financial Services and Markets Act (FSMA)

The FSMA regulates DPT services provided by a Singapore-based person to persons outside of Singapore. Specifically, under Part 9 of the FSMA, which deals with digital token service providers, and which has not been brought into force as of the date of this publication, a Singapore-incorporated entity that undertakes DPT activities outside Singapore will need to be licensed.

Subsidiary legislation

Apart from primary legislation, the MAS also establishes rules for financial institutions which are implemented through subsidiary legislations, which are known as regulations. These have the force of law and must be complied with. One example of such subsidiary legislation is the Payment Services Regulations 2019 (PS Regulations), which is issued under the PS Act. The PS Regulations apply to all entities regulated under the PS Act, and set out licensing and other ongoing requirements. Exemptions from certain requirements of the Act can also be found in the PS Regulations.

The MAS also issues Directions, Notices and Guidelines. Directions and Notices have the force of law and must be complied with. Guidelines (which set out MAS's expectations and have been formulated to encourage best practices among financial institutions) should be complied with.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

Legal status

The term 'crypto asset' is not defined in Singapore. Hence, the specific structure and characteristics of the 'crypto asset' must be examined individually to determine how the 'crypto asset' would be characterised under Singapore law. It is the legal characterisation of the crypto asset that determines the legislation that would apply to it. For example, if a crypto asset confers or represents a legal or beneficial ownership interest in a corporation, it is likely to be characterised as 'securities', which is a type of 'capital markets product' that is regulated under the SFA. In contrast, crypto assets such as Bitcoin, Ethereum and Ripple would amount to a DPT (as defined below), and activities conducted in relation to them would be regulated under the PS Act (which regulates DPT services).

DPTs

A DPT is defined as 'any digital representation of value (other than an excluded digital representation of value) that —

(a) is expressed as a unit;

(b) is not denominated in any currency, and is not pegged by its issuer to any currency;

(c) is, or is intended to be, a medium of exchange accepted by the public, or a section of the public, as payment for goods or services or for the discharge of a debt;

(d) can be transferred, stored or traded electronically; and

(e) satisfies such other characteristics as the [MAS] may prescribe.'

Examples of DPTs include Bitcoin and Ethereum.

As set out above, the MAS regulates the provision of DPT services under the PS Act. The term 'digital payment token services' currently includes the following two activities:

1. 'facilitating the exchange of' DPTs (ie, operating a platform allowing persons to buy or sell DPTs on a centralised basis); and

2. 'dealing in' DPTs (ie, buying or selling DPTs as a service).

The Singapore Parliament passed the Payment Services (Amendment) Act on 4 January 2021 (PS(A)A). However, the PS(A)A has not yet been brought into force. Under the PS(A)A, the scope of DPT services will be expanded such that a service provider will require a licence under the PS Act if:

1. it has control over DPT and provides the service of safeguarding that DPT;

2. it has control over DPT and provides the service of carrying out customer instructions relating to that DPT;

3. it has control over one or more DPTs associated with a DPT instrument and provides the service of safeguarding that DPT instrument;

4. it has control over a DPT instrument and provides the service of carrying out customer instructions relating to one or more DPTs associated with that DPT instrument;

5. it provides the service of arranging (whether as principal or agent) for the transmission of DPTs from one DPT account (whether in Singapore or elsewhere) to another DPT account (whether in Singapore or elsewhere) (DPT transmission); or

6. it provides any service of inducing or attempting to induce any person to enter into or offer to enter into any agreement for or with a view to buying or selling any DPT in exchange for any money or any other DPT (whether of the same or a different type) (DPT brokerage).

On 3 July 2023, the MAS published a Consultation Paper on Proposed Amendments to the Payment Services Regulations (PSR Consultation Paper). The PSR Consultation Paper set out draft amendments to the PS Regulations that would introduce a new regulation 16C into the PS Regulations, which sets out certain requirements in relation to handling, custody and segregation of customer assets that would apply to licensed DPT service providers. These requirements are aimed at mitigating the risk of loss or misuse of customers' assets and facilitating the recovery of customers' assets in the event of a DPT service provider's insolvency. The MAS also stated in the PSR Consultation Paper that DPT service providers should prepare to comply with the policy positions by October 2023, as MAS's policy positions in relation to segregation and custody requirements have been finalised and published.

On 3 July 2023, the MAS also published a Consultation Paper on Proposed Measures on Market Integrity in Digital Payment Token Services (Unfair Trading Practices Consultation Paper). In the Unfair Trading Practices Consultation Paper, MAS seeks comments on (1) the general requirements for DPT service providers and DPT platform operators, (2) the further requirements for DPT service providers relating to the fair, orderly, and timely handling and execution of customers' orders and prevention and detection of unfair trading practices, (3) the proposed provisions relating to prohibited conduct, insider trading and prohibitions against unfair trading practices, and (4) the implementation of the regulatory measures. This includes proposed legislative provisions and the types of wrongful conduct that constitute offences.

Stablecoins

In Singapore, the term 'stablecoin' is not a term of art, unlike a DPT'(as defined above) or e-money (which is defined under the PS Act to be 'denominated in any currency, or pegged by its issuer to any currency).

Stablecoins do not fit squarely in the category of DPTs or e-money. On the one hand, they appear to be (or their issuers purport to have them) pegged or denominated in one or more fiat currencies. On the other hand, they are commonly issued on distributed ledger technology, much in the same way as other types of DPTs - the values of which do fluctuate according to market mechanisms (and are thus not pegged or denominated in fiat currency).

On 26 August 2022, the MAS published a Consultation Paper on Proposed Regulatory Approach for Stablecoin-Related Activities, which set out MAS's proposals to support the development of stablecoins as a credible medium of exchange in the digital asset ecosystem (the Stablecoin Consultation Paper). The consultation closed on 21 December 2022; on 15 August 2023, MAS published its Response to Public Consultation on Proposed Regulatory Approach for Stablecoin-Related Activities (the Stablecoin Consultation Response).

Set out below is a summary of some aspects of the proposed stablecoin framework arising out of the Stablecoin Consultation Response.

Regulation of SCS Issuers

Under the proposed framework, an entity is required to hold a major payment institution licence (MPIL) under the PS Act for undertaking a 'stablecoin issuance service' where:

1. the single currency stablecoin (SCS) is issued in Singapore;
2. the SCS is pegged to the Singapore dollar or any currency of the Group of Ten; and
3. the value of SCS in circulation exceeds S$5m.

MAS has indicated that the term 'stablecoin issuance service' will cover activities necessarily undertaken by a stablecoin issuer, such as custody of that issued SCS and management of reserve assets backing that issued SCS (para 2.7 of the Stablecoin Consultation Response).

The key proposed issuer requirements relate to value stability, audit and segregation of reserves and timely redemption at par value, disclosures in the form of a white paper containing prescribed information (including redemption rights), and prudential standards, details of which may be found in the Stablecoin Consultation Response and the infographic released therewith. Among these requirements, we highlight the following key observations:

- MAS has stated that, under the proposed framework, it will not allow multi-jurisdictional issuance at the onset and will require SCS issuers to issue solely out of Singapore, given (1) the difficulty in establishing regulatory equivalence and cooperation with other jurisdictions at this nascent state of global stablecoin regulation; and (2) practical difficulties with tracing SCS's issuance origin and its implications on monitoring and establishing the adequacy and availability of foreign reserve assets;

- MAS confirmed that it would implement 'labelling' requirements in relation to MAS-regulated SCS versus non-MAS regulated SCS, in order to help customers make informed decisions on the risks involved in using unregulated stablecoins; and
- another key aspect of MAS's response is the emphasis placed on SCS issuers not exposing themselves to risks beyond the primary activity of 'stablecoin issuance services' (and ancillary custody or transmission activities), including (1) investing in/lending to other companies (including holding a stake in other companies); (2) lending or staking activities in relation to SCS and/or other DPTs; (3) DPT trading activity.

Regulation of SCS intermediaries

Separately from the regulatory regime as it relates to SCS issuers, the Stablecoin Consultation Response also sets out MAS's final proposals in relation to SCS intermediaries: that is, entities which do not act as the issuer of a given SCS.

Such entities, should they conduct a regulated DPT service in relation to SCS, would require a licence under the PS Act whether now or in the future (depending on the precise DPT service triggered) as discussed in Part 1 of this article, unless excluded or exempt from the PS Act.

In this regard, MAS's proposals highlight that such SCS intermediaries would be subject to requirements relating to: (1) timely transfer of SCS (ie, within three business days from payer to payee); and (2) segregation of customers' SCS in line with MAS's recent proposals applicable to customer assets (including DPTs).

AML/CFT measures

The MAS issues Notices, Guidelines and other Guidance that set out requirements relating to anti-money laundering (AML) and countering the financing of terrorism (CFT). For example, Notice PSN02 on the Prevention of Money Laundering and Countering the Financing of Terrorism – Digital Payment Token Service and the Guidelines thereto set out requirements for DPT Service Providers on AML and CFT.

These notices and guidelines generally follow the guidance provided by the Financial Action Task Force (FATF).

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

As stated above, the PS Act regulates seven types of payment services or activities: e-money issuance, account issuance, domestic money transfer services, cross-border money transfer services, merchant acquisition services, money changing services and the provision of DPT services. Depending on the type of products or services that a payment provider offers, such payment provider may need to be licensed under the PS Act for the provision of a number of these payment services.

E-wallet services in Singapore are usually regulated under the PS Act; an entity that wishes to carry on a business of providing an e-wallet service would typically be required to have a licence. For example,

an e-wallet being an account that stores e-money is likely to be a 'payment account' as defined under the PS Act, and a provider of such an e-wallet would be engaging in the regulated activity of providing an 'account issuance service'.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

Singapore Fintech Association

One of the three main fintech associations in Singapore is the Singapore Fintech Association. It is a cross-industry non-profit initiative, intended to be a platform designed to facilitate collaboration between all market participants and stakeholders in the fintech ecosystem. The association provides information on laws, regulations, and incentives, and the opportunity to meet and network with other fintech stakeholders.

MAS Fintech Regulatory Sandbox

This is a special regulatory regime created for fintech entities that offer innovative products or services. If a fintech product or service has been allowed to be offered in the Regulatory Sandbox, MAS will provide regulatory support by relaxing specific legal and regulatory requirements. However, upon successful completion of and on exiting the Sandbox, the fintech entity will have to comply fully with the relevant legal and regulatory requirements, including obtaining a full licence.

MAS Sandbox Express/Plus

Apart from the Regulatory Sandbox, MAS has also introduced the Sandbox Express. The Sandbox Express provides companies with a faster option to test certain innovative financial products and services in the market. Eligible applicants can begin market testing in the pre-defined environment of Sandbox Express within 21 days of applying to MAS. Currently, the Sandbox Express is available specifically for:

- carrying on business as an insurance broker; and
- establishing or operating an organised market.

There are also various funds and initiatives to facilitate access to capital for fintech entities, such as:

- MAS's Sandbox Plus, which provides assistance for firms looking to introduce innovative products and services that are regulated by MAS. To be eligible for the financial grant under Sandbox Plus, the proposed technology must not yet be applied in financial services in Singapore, and the Sandbox application must be approved by MAS. Funding support will cover 50 per cent of qualifying expenses, capped at $400,000. The grant will be disbursed over three payments upon meeting certain conditions, during and after the sandbox period. Qualifying

expenses include manpower expenses, professional services, hardware/software infrastructure and licences, equipment and IP rights, and capability transfer-related training costs.

- The Financial Sector Technology and Innovation (FSTI) scheme provides grants for innovation support for early-stage development of innovative projects, including setting up innovation labs, institution level projects and technology infrastructure. The FSTI scheme is valid until March 2026.
- Startup SG Accelerator, Startup SG Equity, Startup SG Founder, Startup SG Infrastructure, Startup SG Tech, Startup SG Loan, Startup SG Network and Startup SG Talent (all operated by Enterprise Singapore Board) provide governmental co-investment, mentorship support and startup capital grants.
- The MAS National Artificial Intelligence (AI) Programme in Finance was launched to build deep AI capabilities within Singapore's financial sector to strengthen customer service, risk management and business competitiveness. Under this programme, MAS will provide funding, contribute government data, and convene the necessary expert stakeholders to drive AI adoption in the financial sector. In May 2023, the MAS launched the Financial Sector Artificial Intelligence and Data Analytics (AIDA) Talent Development Programme under the National AI Programme in Finance, which aims to increase the supply of AIDA talent to build deep AI capabilities in the financial sector.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

MAS maintains the Financial Industry API Register which aims to serve as the initial landing site for open APIs available in the Singapore financial industry. It is updated on an ongoing basis as Singapore's financial institutions make available their open APIs.

The open APIs are classified into the following main functional categories:

- product APIs (to provide information on financial product details and exchange rates);
- sales and marketing APIs (to handle product sign-ups, sales/cross-sales and leads generation);
- servicing APIs (to manage customer profile/account details and customer queries/feedback); and
- transaction APIs (to support customer instructions for payments, funds transfers, settlements, clearing, trade confirmations and trading).

Each functional category is further classified as either (1) transactional (contains sensitive client data, user/partner authentication required) or (2) informational (contains non-sensitive data, no/minimal authentication required).

South Korea

Doil Son*
Yulchon, Seoul
dison@yulchon.com

Sun Hee Kim†
Yulchon, Seoul
kimsh@yulchon.com‡

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

The most relevant laws and regulations on fintech business are:

- the Electronic Financial Transactions Act, which regulates electronic financial transactions in general;
- the Banking Act, the Specialised Credit Finance Business Act, and the Financial Investment Services and Capital Markets Act, which regulate specific finance sectors;
- the so-called 'Three Data Acts', consisting of the Personal Information Protection Act, the Credit Information Use and Protection Act, and the Act on Promotion of Information and Communications Network Utilisation and Information Protection – these regulate the collection and use of personal information;
- the laws related to anti-money laundering (AML);
- the Virtual Asset User Protection Act; and
- the Special Act on Support for Financial Innovation, governing fintech innovation.

Electronic Financial Transactions Act (EFTA)

Under EFTA, there are seven types of electronic financial business licences:

- electronic funds transfer business;
- electronic currency business;
- electronic prepayment business;
- electronic debit payment business;
- electronic payment settlement agency business;

---

* Doil Son is the Head of the IP & Technology Practice of Yulchon. He also serves as Co-Chair of the Technology Law Committee of the IBA.
† Sun Hee Kim is a partner in the Data & Technology Team at Yulchon. She also serves as Membership Officer of the Asia Pacific Regional Forum of the IBA.
‡ The authors thank Da Yeon Ahn, Sang Hyun Park, Ki Won Lee, Ji Hye Han and Jae-Eun Claire Chong for their contributions to this article.

- payment deposit business; and
- electronic notification settlement business.

According to the Finance Consumer Service Center, operated by the Financial Services Commission (FSC) and the Financial Supervisory Service (FSS), the registration status of the electronic financial businesses as of 13 November 2023 is shown in Table 1:

Type of business licence	Number of registered companies
Electronic funds transfer business	0
Electronic currency business	0
Electronic prepayment business	82
Electronic debit payment business	24
Electronic payment settlement agency business	148
Payment deposit business	41
Electronic notification settlement business	16
Total	311 registrations (by 186 companies)

Table 1: Registration status of the electronic financial businesses as of 13 November 2023

Amendments to EFTA have been discussed since 2020, as the current EFTA fails to encompass integrated and comprehensive financial services such as fintech. A proposed amendment bill to EFTA at the National Assembly intends to simplify the existing seven types of electronic financial business licences into three by recategorising/consolidating the types by function, and adding 'payment instruction service business' and 'comprehensive payment settlement business' licences (see Figure 1).

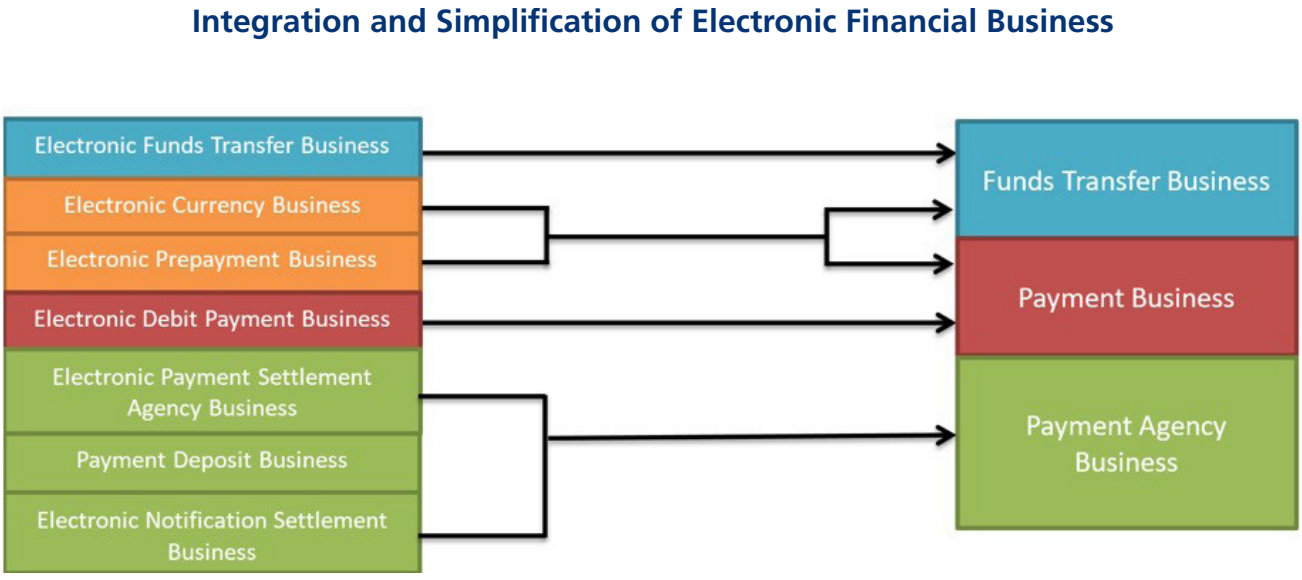

Figure 1: Integration and simplification of electronic financial business

While the above amendment bill to the EFTA is still pending at the National Assembly, another amendment bill to the EFTA has passed the National Assembly and will be effective from 15 September 2024 (the '2024 Amendment'). The 2024 Amendment focuses on the regulation of electronic prepayment means.

The 2024 Amendment expands the scope of regulated electronic prepayment means. Currently, to qualify as an electronic prepayment means under the EFTA, it must be used to purchase goods or services from two or more business categories. However, the 2024 Amendment removes this business category requirement, thereby broadening the range of electronic prepayment means. This means that those used to purchase goods or services from a single business category will be subject to the regulations under the EFTA after 15 September 2024. For more details of the issuance and management of electronic prepayment means, see Question 3.

In addition, the 2024 Amendment introduces various regulations aimed at safeguarding the integrity of electronic prepayment means, such as the separate management of prepaid recharges. Once the 2024 Amendment comes into force, it is also expected that relevant regulations and guidelines specifying the details delegated under the EFTA will be amended.

The current EFTA contains provisions regarding the security of electronic financial transactions, and the details of such safety measures are stipulated in the Electronic Financial Supervisory Regulations. The following are some noteworthy regulations and guidelines.

Regulations on the use of cloud services in the financial sector

For financial companies to use cloud services, they must (1) undergo a complex evaluation process, including a business importance assessment and safety assessment of the cloud service provider (CSP), etc; (2) enter into a service contract with the CSP approved by their internal information protection committee; and (3) file a prior report on the use of cloud services with the FSS.

To ease the burden on financial business entities, the FSC has prepared a plan to clarify the scope of work that can use the cloud, simplify any overlapping or similar administrative procedures, and change the prior reporting requirement to *ex post facto* reporting.

Regulations on network separation

Financial companies must operate the business network that manages and operates important customer information separately from the general internet network.

Following several announcements regarding the relaxation of regulations pertaining to network separation, on 28 June 2023, the FSC and the Financial Security Institute (FSI) introduced a regulatory sandbox to allow financial institutions to utilise software as a service (SaaS) solutions provided by CSPs within their internal networks.

To be more specific, the financial institutions designated within the aforementioned regulatory sandbox are permitted to employ SaaS solutions on their internal networks for non-critical tasks that involve the processing of customers' personal information, credit information, and/or transactional data. These financial institutions may utilise SaaS for purposes such as collaboration tools, ERP, and

other various internal services. However, it is important to note that the use of SaaS in this context should not extend to security management, IT development, and/or customer-related services.

To be qualified for exemption from the network separation requirement, CSPs offering SaaS to financial institutions must undergo safety assessments conducted by the FSI.

Regulations on specific finance sectors, the Three Data Acts, and AML-related laws

The laws regulating conventional financial businesses, such as the Banking Act, the Specialised Credit Finance Business Act, and the Financial Investment Services and Capital Markets Act, may apply to fintech companies if they perform financial business regulated by these laws.

In addition, the Three Data Acts (ie, the Personal Information Protection Act, the Credit Information Use and Protection Act, and the Act on Promotion of Information and Communications Network Utilisation and Information Protection) should also be considered when processing personal information or personal credit information. The Credit Information Use and Protection Act currently allows the operation of the MyData Service, which enables individuals to browse and manage their personal financial information gathered from various sources (ie, banks and other financial companies). This service was introduced to enhance the data sovereignty of financial consumers.

The Act on Reporting and Using Specified Financial Transaction Information, along with applicable AML laws and regulations for financial companies, may also be applied to fintech business. Please see Question 2 for details.

Virtual Asset User Protection Act

See Question 2.

Special Act on Support for Financial Innovation

See Question 4.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

The Amendment to the Act on Reporting and Using Specified Financial Transaction Information, effective as of 25 March 2021, first defined the term 'virtual assets' and imposed reporting obligations on virtual asset service providers (VASPs). Accordingly, VASPs must fulfil requirements related to information security management systems, real-name confirmation of deposit and withdrawal accounts, qualification of its representatives and executives, and reporting to the Korea Financial Intelligence Unit (KoFIU). Moreover, VASPs must comply with the following AML obligations:

- Suspicious transaction report (STR): A financial institution should report to the Commissioner of the KoFIU if it has reasonable grounds to suspect that the assets received in relation to any

financial transactions are illegal or the counterparty to the financial transaction is engaged in money laundering or financing of terrorism.

- Currency transaction report (CTR): A financial institution must report details of transactions to the KoFIU when a customer makes or withdraws more than KRW 10m in cash a day.
- Customer due diligence (CDD): When engaging in financial transactions with customers, a financial institution shall take necessary measures to verify the customers' identity, actual ownership, the purpose of transactions, etc.
- Provision of wire transfer information (so-called 'travel rule'): Where a remitter routes more than KRW 1m (for domestic remittances) or US$1,000 (for overseas remittances) by wire transfer, the sending financial institution shall provide the name and account number of the sender and the recipient to the receiving financial institution. In the case of overseas remittances, the address, resident registration number, or passport number of the sender must be provided as well. Furthermore, for domestic remittances, the sending financial institution is obligated to provide the address, resident registration number, or passport number of the sender to the Commissioner of the KoFIU or the receiving financial institution within three business days upon request.[1]

Regarding taxation, the Income Tax Act will apply to virtual assets. The recent amendment to the Income Tax Act, which took effect on 1 January 2023, classifies the income generated from transferring or loaning virtual assets as 'other income', and imposes tax at a rate of 20 per cent.

In July 2023, the Virtual Asset User Protection Act (VAUPA), a special law concerning crypto assets, was enacted. The VAUPA, scheduled to take effect on 19 July 2024, aims to safeguard users' assets and regulate unfair trade practices. Specifically, the VAUPA encompasses requirements related to deposit protection, safekeeping of virtual assets, insurance subscription, and maintenance of transaction records.

Additionally, the VAUPA prohibits one's engagement in unfair trade practices, which include the use of non-public information, market manipulation, fraudulent trade activities, trading or transactions involving virtual assets issued by VASPs or related parties, and arbitrary blocking of virtual asset deposits and withdrawals.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

Payment service providers or digital wallets can be subject to the following business licences under the current EFTA. Please note that this may be changed once the National Assembly passes the amendment to the EFTA.

1 When the travel rule applies to a VASP (ie, when it transfers virtual assets worth KRW 1m or more to another VASP), the sending VASP shall provide the name and virtual asset address of the sender and the recipient to the receiving VASP (in case requested by the Commissioner of the KoFIU or the receiving VASP, also the resident registration number or passport number of the sender, within three business days upon request).

Electronic Payment Settlement Agency Service

This is the so-called payment gateway (PG) service. An 'electronic payment settlement agency service' means any service to transmit or receive payment settlement information in purchasing goods or using services by electronic means or to execute as an agent or mediate the settlement of prices thereof (Article 2, Subparagraph 19, EFTA).

Any person who intends to provide electronic payment settlement agency services shall be registered with the FSC (Article 28(2), Subparagraph 4, EFTA). However, an exception applies to any person who performs the electronic payment settlement agency services prescribed by the Presidential Decree, such as delivering information only for the electronic processing of electronic payment transactions without direct involvement in the transfer of funds (Article 28(3), Subparagraph 2, EFTA).[2]

Issuance and management of electronic prepayment means

An 'electronic prepayment means' refers to any certificate (or the information thereon), excluding electronic currency, issued with transferable monetary values stored by electronic means and satisfies all of the following requirements: (1) it should be used to pay for the purchased goods or services from a third person other than the issuer (including affiliates of the issuer prescribed by Presidential Decree), and (2) it shall be able to purchase goods or services which belong to at least two different business categories (Article 2, Subparagraph 14, EFTA).[3]

Exemptions for the registration obligation for the electronic prepayment means under the EFTA include:

- when the total balance of the issued amount does not exceed KRW 3 billion (the term 'total balance' refers to the average of 'outstanding unused balance' at the end of each quarter). However, it is worth noting that the 2024 Amendment narrows this exemption by specifying that both the 'total balance' and the 'annual issuance amount' should be above a certain level (to be specified in the Presidential Decree);
- when an electronic prepayment means is used by ten or fewer merchants. However, the 2024 Amendment further restricts this exemption by granting an exemption only when used by a single merchant; and
- when the price of electronic prepayment means has not been prepaid directly by a user (eg, issued in the form of mileage) and is covered by refund guarantee insurance to discharge the liability for the charged monetary values (as prescribed by Presidential Decree).

Although there are no specific laws on this point, foreign payment service providers and digital wallets may not, in practice, be subject to licensing requirements if they satisfy the following conditions for 'reverse solicitation':

2 If a PG provides services to a specific offshore cybermall operated by its affiliate, it can be registered as a 'limited PG'. The concept of limited PG was introduced in 2013 to ease some of the requirements for PGs servicing only the online malls operated by overseas affiliates.

3 As explained above in Section 1, the 2024 Amendment focusing on electronic prepayment means has recently been approved by the National Assembly. With the 2024 Amendment scheduled to take effect on 15 September 2024, this requirement (2) (ie, the at least two different business categories requirement) will be removed from the EFTA.

- there should be no active solicitation or advertisement directed towards Korean customers;
- there should be no intent to 'target' Korean buyers (ie, no marketing to Korean buyers through email, phone or postal mail);
- the website and platform should not provide any Korean translations to ensure that services are not specifically tailored for Korean users; and
- there should be no employees physically located in Korea.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

The Korean Government has been operating the Financial Regulatory Sandbox scheme since April 2019 under the Special Act on Support for Financial Innovation to provide a systematic basis for testing fintech companies' new and innovative ideas.

Under the Special Act on Support for Financial Innovation, the term 'innovative financial services' refers to the services provided in the financial industry or related businesses that are recognised for their differentiated content, method, form, etc from the existing financial services (Article 2, Subparagraph 4, Special Act on Support for Financial Innovation).

Once designated as an innovative financial service, a fintech company will be given regulatory exemptions for up to four years to pilot test their ideas, innovations, and new services. The Financial Regulatory Sandbox has the following schemes:

- Innovative financial services: once designated as an innovative financial service, a fintech company can operate innovative financial services within the designated scope without obtaining a separate financial business licence, and will be given special treatment as to the regulations related to financial laws, such as licensing, registration, reporting, governance, soundness, and business conduct.
- Designated agent: in principle, financial institutions cannot entrust their essential financial business to a third party (Proviso of Article 3(1) of the Regulations on Entrustment of Financial Institutions, etc). However, through the designated agent scheme, fintech companies can be designated by financial institutions and entrusted to directly operate banking, insurance, and securities businesses.
- Commissioned test: under the commissioned test scheme, a fintech company (which is unauthorised to provide financial services) can commission a financial institution with the right to use its new fintech service for testing. Under this scheme, unlicensed companies and small companies can secure test opportunities.
- Quick check on regulations: the quick check on regulations scheme refers to a system where financial services providers can receive prompt confirmations on the applicable laws and regulations related to their services.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

No law explicitly regulates open banking. However, open banking has been introduced and operated as follows:

- August 2016: Introduction of the Joint Banking Open platform, a predecessor of the open banking service;
- 25 February 2019: The 'financial settlement infrastructure innovation plan' was announced to establish an innovative infrastructure in the financial sector (ie, an open joint payment system) through close cooperation with the banking sector. Detailed action plans were prepared as part of this initiative;
- 30 October 2019: A pilot implementation of the open banking service was initiated; and
- 18 December 2019: The full implementation of the open banking service was realised.

Currently, the open banking service operates under private agreements among participating institutions, such as financial institutions and electronic financial companies.

Although not definitive, it is presumed that the amendment to the EFTA may include provisions to establish the legal framework for designating electronic payment transaction clearing systems (open banking) by the FSC, and empower the FSC to authorise the Financial Telecommunications and Clearings Institute (KFTC) as an electronic payment transaction clearing institution to engage in electronic payment transaction clearing business.

Taiwan

Robin Chang[1]
Lee and Li, Taipei
robinchang@leeandli.com

Eddie Hsiung[2]
Lee and Li, Taipei
eddiehsiung@leeandli.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

In Taiwan, carrying out financial activities generally requires a licence from Taiwan's financial regulator, the Financial Supervisory Commission (FSC). However, there is currently no special licence specifically for fintech companies. In other words, if any business to be carried out by fintech companies would involve financial activities regulated by the FSC, the fintech companies must meet certain requirements under relevant financial laws and regulations, depending on the types of financial activities they wish to conduct.

However, certain fintech-related regulations, mechanisms or developments have been introduced in Taiwan recently.

E-payment

See Question 3.

Open Banking

See Question 5.

Digital-only banks

The FSC promulgated relevant regulations governing the establishment of digital-only banks in 2018. Digital-only banks refers to banks who mainly utilise the internet or other forms of electronic communication channels to provide financial products and services to its customers, without

1 Robin Chang is a partner at Lee and Li and the head of the firm's banking practice group. His practice focuses on fintech services and regulatory issues, banking, IPOs, capital markets, mergers and acquisitions, project financing, financial consumer protection law, personal data protection law, securitisation and antitrust law. Mr Chang advises major international commercial banks and investment banks on their operations in Taiwan. He successfully assisted the listing of some foreign companies in Taiwan. He is also involved in many M&A transactions of financial institutions in the Taiwan market.

2 Eddie Hsiung is a partner at Lee and Li, Attorneys-at-Law. He is licensed to practise law in Taiwan and New York, and is also a CPA in Washington State. His practice focuses on securities, M&A, banking, finance, asset and fund management, cross-border investments, general corporate and commercial, fintech, startups, etc. He regularly advises leading banks, securities companies, payment and credit cards and other financial services companies on transactional, licensing and regulatory and compliance matters, as well as internal investigation. He is familiar with legal issues regarding the application of new technologies such as fintech (e-payment, digital financial services) and blockchain (cryptocurrencies, platform operators) and AI, and is often invited to participate in public hearings, seminars and panel discussions in these areas.

physical branches. In 2019, three applications were filed with the FSC for setting up digital-only banks, and these applications were approved by the FSC in the same year. At the time of writing, all such digital-only banks have received banking licences from the FSC and have started their business operations.

Digital-only insurance companies

Following digital-only banks, in December 2021, the FSC proposed a new policy on establishment of digital-only insurance companies. For this purpose, by the end of June 2022, the FSC promulgated amendments to relevant regulations to set forth the requirements for the establishment of digital-only insurance companies as well as detailed regulations governing their insurance solicitation, underwriting and claims settlement. According to the FSC's press releases, the FSC started to accept applications for establishment of digital-only insurance companies in August 2022, while the two applications filed with the FSC were not approved by the FSC. According to relevant news reports, the FSC will explore the feasibility of re-opening for the applications of digital-only insurance companies, and the plan in this regard will be announced by the end of 2024.

Robo-advisers

The Operating Rules for Securities Investment Consulting Enterprises Using Automated Tools to Provide Consulting Service (Robo-Adviser) (Robo-Adviser Rules) have been issued by the Securities Investment Trust and Consulting Association (SITCA), Taiwan's self-regulatory organisation for the asset management industry.

The Robo-Adviser Rules were first announced in 2017, with the latest amendment in 2022. According to the Robo-Adviser Rules, FSC-licensed securities investment consulting enterprises (SITEs) may provide online securities investment consulting services by using automated tools and algorithms (ie, robo-adviser services), and must comply with certain rules, such as:

- a periodical review of the algorithm;
- a special committee established to supervise the adequacy of the robo-adviser services; and
- customers should be informed of precautions before using robo-adviser services.

In June 2024, the FSC issued a proposed amendment to the regulations governing SITEs, under which any change to the algorithms adopted by the SITEs shall be reviewed and approved by the SITCA. At the time of writing, it is still uncertain as to when such amendment will be officially announced.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

Except for certain rules and regulations governing 'security tokens' and anti-money laundering (AML) (as explained below), no Taiwanese laws or regulations have been specifically promulgated or amended to formally regulate crypto assets.

In December 2013, both the Central Bank of the Republic of China (Taiwan) (Central Bank) and the FSC first expressed the government's position towards Bitcoin by issuing a joint press release, under which the two authorities held that Bitcoin should not be considered a currency, but a highly speculative digital virtual commodity. In another FSC press release in 2014, the FSC ordered that local banks must not accept Bitcoin or provide any services related to Bitcoin, such as exchange Bitcoin for fiat currency.

The FSC issued a further press release on 4 March 2022, which indicates that crypto assets (except for 'security tokens' as explained below), including Bitcoin, are not currencies under the current regulatory regime in Taiwan; instead, a crypto asset is deemed to be a digital virtual commodity.

Security token offerings (STOs)

The FSC issued a ruling in July 2019 to officially define 'security tokens' (ie, cryptocurrencies of 'securities' nature) as a type of security. Thereafter, the FSC, together with the Taipei Exchange (TPEx), one of the securities exchanges in Taiwan, enacted a set of rules and regulations on security token offerings (STO Regulations), and authorised the TPEx to supervise STOs. Below is a summary of certain key rules under the STO regulations.

- STOs carried out under the STO Regulations shall be in an amount of TWD 30m (around US$1m) or less.
- The issuer must be a company limited by shares incorporated under the laws of Taiwan, and no listed company can be an issuer.
- The issuer can only issue profit-sharing or debt tokens without shareholders' rights, meaning that 'shares' with regular shareholders' rights of issuers cannot be issued as security tokens while bonds can be issued as debt tokens.
- Currently, only 'professional investors' are eligible to participate in STOs. When the professional investor is a natural person, the maximum subscription amount is TWD 300,000 per STO.
- Issuers must conduct STOs on a single platform.
- The platform operator should obtain a securities dealer licence (with a minimum paid-in capital of TWD 100m).
- The platform operator should enter into an agreement with the Taiwan Depository and Clearing Corporation (TDCC) and deliver trading information, such as balance changes and balance statements, to the TDCC on a daily basis, for record-keeping purposes.
- Subscription and trading of security tokens should be conducted on a real-name basis.

Anti-money laundering

Taiwan's latest amendment to the Taiwanese AML law, the Money Laundering Control Act (MLCA), has brought relevant cryptocurrency-related service providers into the AML regulatory regime.

Under the amended MLCA, the FSC published the Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for Enterprises of Virtual Currency Platforms and Trading Business (Crypto AML Regulations) in 2021. According to these regulations, the designated operators of crypto assets and exchanges (VASPs) are required to establish, among others, internal control and audit mechanisms, reporting procedures for suspicious transactions, know your client (KYC) procedures, and making a filing with the FSC declaring their compliance with the Crypto AML Regulations (AML Compliance Statement). The MLCA also underwent an amendment in July 2024. Under such amendment, VASPs shall complete their anti-money laundering registration (AML Registration) with the FSC before they may provide services, and any offshore VASPs shall set up a company or branch office in accordance with the Taiwan Company Act and complete the aforementioned AML registration before providing relevant services within Taiwan. Anyone who violates the above provisions may be sentenced to imprisonment for not more than two years, detention, or in lieu thereof or in addition thereto a criminal fine of not more than NT$5m. Furthermore, in addition to punishing the perpetrator, if a juristic person is the actor, such juristic person shall also be subject to a criminal fine. In short, any VASP providing services in Taiwan without completing the AML registration with the FSC beforehand would be subject to criminal liability under the newly amended MLCA.

At the end of September 2023, Taiwan's FSC also issued a set of guiding principles governing VASPs (VASP Guidelines) under the MLCA framework. Many of the provisions/obligations under the VASP Guidelines are non-AML related, such as:

- the disclosure of any virtual assets listed/launched on the VASP's platform;
- the VASP's obligations to review the listing/launching application;
- separation of the VASP's assets and clients' assets;
- inclusion of rules for trading of virtual assets in the VASP's internal control system; and
- prohibition of foreign VASPs (ie, those foreign VASPs who have not made the Compliance Statement with the FSC) from carrying out advertising activities within Taiwan or targeting at Taiwan clients.

While purely from a legal viewpoint these VASP Guidelines will not be considered binding, there is an expectation that the FSC will gradually require compliance with these rules. Also, local VASPs have officially completed the establishment of a self-regulatory organisation (SRO) for VASPs and it is also generally expected that the self-regulatory rules, once promulgated, will substantially incorporate the content of the VASP Guidelines.

Lastly, the FSC is considering the possibility of introducing a specific law for cryptocurrencies, with a feasibility study report expected to be announced before the end of 2024 and the draft law before mid-2025. It is recommended that industry players closely monitor potential regulatory changes in Taiwan.

Non-fungible tokens (NFTs)

To date, no Taiwanese laws or regulations have been specifically promulgated or amended to address the rise and development of NFTs in Taiwan. From a local law perspective, the classification of any NFT should be determined case by case. Although some argue that NFTs should be considered as, for example, 'art creation' so the sale of these should not be deemed as the offering of cryptocurrency, we cannot completely rule out the applicability of Taiwan securities and financial regulations, especially if there are multiple NFTs that are linked to, or represent, the same asset and the NFTs have an investment characteristic.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

In 2015, the Act Governing Electronic Payment Institutions (E-Payment Act) was enacted to govern and regulate the activities of electronic payment institutions (EPIs), acting in the capacity of an intermediary between payers and recipients. A recent amendment to the E-Payment Act took effect in July 2021. Under the amended E-Payment Act, the scope of business of an EPI includes (1) core businesses and (2) ancillary and derivative businesses.

The core businesses are:

1. collecting and making payments for real transactions as an agent (which, as we understand, is similar to the concept of 'escrow agent' in some other jurisdictions);
2. accepting deposits of funds as stored value funds;
3. small amount domestic and cross-border remittance services; and
4. foreign exchange services relating to the above (1) through (3) businesses.

An EPI should obtain a licence from the FSC unless it engages only in (1) above, and the total balance of funds collected, paid and kept by it as an agent does not exceed the specific amount set by the FSC.

The ancillary and derivative businesses are all new under the amended E-Payment Act, which include:

- assisting the contracted merchants with integration and transmission of acquiring and payment information;
- sharing terminal equipment at the contracted merchants;
- assisting the information exchange between the users and between the users and the contracted merchants;
- providing an electronic uniform invoice system and its value-added services;
- taking custody of paid price of vouchers/tickets of goods/services, and assisting in the issuance, sales, validation and related services for vouchers/tickets;

- providing services for integration of bonus points and offsetting/settling payments for real transactions with bonus points;
- providing value storing blocks in electronic stored-value cards or application programs for use by others; and
- providing any planning, instalment, maintenance or consultancy services for the information system and facilities in relation to the above seven ancillary and derivative businesses of EPIs.

The amended E-Payment Act also allows qualified 'non-EPIs' to apply to the FSC for acting as a 'small amount cross-border remittance service provider', exclusively for foreign workers in Taiwan in accordance with the enforcement rules and regulations promulgated by the FSC.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

To promote fintech services and companies, Taiwan enacted a law in 2018 for the fintech regulatory sandbox, the FinTech Development and Innovation and Experiment Act (Sandbox Act), to enable fintech businesses to test their technologies in a controlled regulatory environment. Please see below certain applications that have been approved by the FSC to enter into the sandbox under the Sandbox Act:

- to facilitate digital banking businesses, ie, online credit (credit card, credit facility), by means of a mobile phone ID verification system;
- outbound remittance by foreign workers through local convenience stores;
- to use blockchain technology for the transmission of fund transfer information between banks;
- to enable customers to purchase travel insurance on the website of a travel agency by means of application programming interfaces (API) connections;
- to provide the 'fund exchange' service by means of blockchain technology;
- to narrow the fund transmission gap by means of a T+0 contract mechanism;
- to provide a group buying platform for investing in bonds issued using blockchain technology; and
- to allow investors to buy US ETFs using dollar-cost averaging strategy based on the advice provided by robo-advisers.

According to the FSC's official website, press releases and relevant news articles, some of the experiments which are included in the regulatory sandbox now exist in practice, while some may be implemented legally in the real world soon. In practice, experimental sandbox applicants under the Sandbox Act may apply for the new licence or approval for their business once the existing laws and regulations involved in the experiments have been amended by the FSC and/or the Congress.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

Traditionally, financial institutions are required by the FSC to provide relevant customer and product data to the Joint Credit Information Center (JCIC) for the purpose of the banks' credit check for credit extension. But in recent years, in response to the advocate for open banking, the FSC has also requested the Bankers' Association to set out relevant self-regulatory rules to implement the concept of open banking.

In Taiwan, the FSC does not require 'mandatory disclosure', but instead encourages banks to voluntarily open up their APIs for programmatic access by third-party financial service providers (TSPs) in accordance with relevant information security standards.

The FSC has adopted a three-phase approach for open banking. Phase I was launched in late 2019, allowing 'public products information' to be searchable by TSPs. Phase II involves access to 'customer data', and according to relevant FSC press releases and news reports, certain TSPs and banks have been allowed by the FSC to collaborate with each other in Phase II. Phase III will involve processing of 'transaction data'; the timeline to launch Phase III is still under discussion but according to relevant news reports, Phase III will be launched in early 2024 at the earliest.

Central America

Costa Rica

Diego Gallegos
Arias, San José
diego.gallegos@ariaslaw.com

1. Fintech regulatory framework: please provide a description of the most relevant laws and regulations on fintech and financial innovation in your country. Please also refer to any new law or regulation foreseen in the near future or any bill on fintech and financial innovation in your jurisdiction.

Current regulations

Costa Rica has no current fintech-specific legislation or regulation overseeing the sector. Therefore, companies operate within the restrictions and parameters of regular financial entities, securities-offering regulations and anti-money laundering (AML) legislation. In principle, fintech companies do not need a prior habilitating license to operate unless they perform a restricted activity, namely: (1) financial intermediation[1] and (2) the public offering of securities and or securities-related services, as Costa Rican private counterparties can enter into all contracts that are not prohibited by law based on the freedom of contract principle.[2]

From a practical standpoint, even when a habilitating licence is not required, depending on the line of business of the company, there are certain regulations to bear in mind, specifically: (1) access to the Central Bank's Electronic Payment Processing System and (2) registration before the Superintendency of Financial Entities (Superintendencia General de Entidades Financieras or SUGEF) for AML controls in the event the business operates local bank accounts.

Payment processing companies that want to have direct access to the Central Bank's Electronic Payment Processing System (Sistema Nacional de Pagos Electrónicos or SINPE) will need to abide by the regulation issued by the Costa Rican Central Bank granting direct access to the platform. Otherwise, they can utilise an entity that already has access to the system, as all supervised financial entities do.

Certain activities in Costa Rica do not require a habilitating licence but are subject to registration requirements under the Law on Narcotics, Psychotropic Substances, Drugs of Unauthorised Use, Related Activities, Money Laundering and Financing of Terrorism (Law Number 7786). Among the economic activities that require AML registration under Article 15 and 15bis of Law Number 7786 are:

1 Article 116, Organic Law of the Central Bank, Law number 7558 defines financial intermediation as: 'being in the business of receiving money deposits from the members of the public and investing it for the intermediary's account and specific risk in any form of credit or securities investments'.

2 Article 28, Constitution of the Republic of Costa Rica.

- systemic and substantial transfer of funds (exceeding US$400,000 per year);
- the administration of third-party funds;
- the granting of credit facilities; and
- providing remittance services.

Such registration will be required if the local entity receives or sends funds through a local bank account that originates in such activities.

Future regulation

There are several initiatives that seek to regulate the 'up-and-coming' fintech sector in Costa Rica. As is the case in many jurisdictions, regulators are adapting to new technology and a desire to foment investment in the fintech sector itself, but also responding to concerns from traditional financial institutions, and banking and securities regulators that want to maintain their authority over the local financial system.

One of the main regulatory initiatives is a bill of law filed to regulate crypto assets in Costa Rica, called the Law on the Crypto Market, which seeks to regulate how crypto assets and the trading of such assets is performed and recognised in Costa Rica. This includes the ability of companies to offer such services to register before SUGEF for AML control purposes and access the Central Bank's SINPE system.

Other initiatives for the sector have not been formally presented as a proposed law or regulation but have been discussed at Central Bank and SUGEF level – such as the need to have a legal definition of fintech companies, to be able to count them and understand the services they provide. Currently, estimations of the Central Bank are based on the companies that request access to SINPE; however there is no database or definition of which companies operate in the country and the services they perform. There has also been a push in recent months to restrict the ability of companies registered in SINPE to offer accounts to their general public customers, since this way of operating circumvents minimum legal reserve requirements and SUGEF AML supervision that locally licensed financial entities have to abide by.

2. Regulations on crypto assets: please provide a summary of the legal framework of crypto assets in your country and how crypto assets are regulated in your jurisdiction.

Crypto assets are not currently regulated in Costa Rica, although there is a bill of law seeking to do that (see Question 1). The Central Bank has considered that crypto assets are not a currency and therefore not subject to currency exchange restrictions or regulations. Similarly, the Securities Regulatory Agency (Superintendencia General de Valores or SUGEVAL) has not considered cryptocurrencies to be a security, and therefore not within its jurisdiction to limit an unauthorised public offering of securities.

Companies may provide crypto assets within the territory of Costa Rica, as the activity is not a restricted activity and will only be subject to possible AML controls in the event they are subject to registration requirements under Law Number 7786.

3. Payment service providers and digital wallets: please describe how payment service providers and/or digital wallets are regulated in your country. Please mention any foreseen law or regulation in this respect.

Payment service providers and digital wallets do not engage in a restricted activity in Costa Rica as long as they do not perform financial intermediation or an unauthorised public offering of securities.

If such providers issue local credit or debit cards, they must abide by the terms of the Regulation on Card Payment System (Reglamento del Sistema de Tarjetas de Pago). Also, depending on the activity carried out, it is likely that they will have to register before SUGEF for AML control purposes under law 7786.

4. Special support to fintechs: does your jurisdiction provide any special programme supporting the fintech ecosystem, in particular fintech start-ups (eg regulatory sandboxes, accelerator programmes). Are such programmes supported by the regulator in your country?

The National Council on Supervision of the Financial System (Consejo Nacional de Supervisión del Sistema Financiero or CONASSIF) with the support of the Inter American Development Bank (IDB) has implemented the Financial Information Centre (Centro de Innovación Financiera or CIF). The CIF is a joint initiative of the Central Bank and the entities in charge of regulating and supervising the Costa Rican financial, securities, insurance and pension systems whose stated purpose is to guide financial innovators in the process of developing and inserting their initiative within the framework of financial regulation. Interested parties may submit initiatives through a form to the CIF, which will then be analysed and advanced through the appropriate channels.

There are also private sector organisations that group fintech companies and promote sector regulations and education initiatives, such as the Costa Rican Blockchain Association and the Central American and Caribbean Fintech Association.

5. Open banking: please advise whether in your jurisdiction there are regulations on open banking. If the response is no, please provide any reference to regulations that may directly or indirectly affect open banking. Please include any foreseen laws and regulations on open banking.

Costa Rica, despite having a thriving fintech sector, remains undeveloped with respect to open banking initiatives and has no specific regulations for that activity. Concerns about safeguarding sensitive data hinder progress, and convincing financial institutions to share customer information, even with informed consent, is challenging.

Any initiative must navigate a strong resistance from financial entities and their clients to share their personal data to allow application programming interfaces (APIs) to properly function and coordinate the structure to implement a system to share such data. Currently, even the sharing of individualised data by financial institutions to the Central Bank is contested as a possibly illegal action, and has been a subject to ongoing disputes among the Central Bank, SUGEF and certain banks which have refused to provide such information.

El Salvador

Zygmunt Brett
BLP Legal, San Salvador
zbrett@blplegal.com

1. Fintech regulatory framework: please provide a description of the most relevant laws and regulations on fintech and financial innovation in your country. Please also refer to any new law or regulation foreseen in the near future or any bill on fintech and financial innovation in your jurisdiction.

To some extent, El Salvador has become a favourable environment for fintech companies, given the government's support and promotion of the development and growth of this industry, especially bitcoin and crypto assets. Besides some laws concerning the use and implementation of Bitcoin and digital assets, there are no specific regulations nor a specific law for fintech in El Salvador. Nevertheless, there is a legal framework that provides some technological financial alternatives. The most relevant are:

- *Bitcoin and Crypto Act*: see Question 2.
- *Financial Inclusion Facilitation Act (FIFL)*: This Act aims to promote financial inclusion by creating the concept of electronic money, which is commonly used through phone apps, in which users have the technological tools to carry out e-money transactions.

  FIFL's main goal is to promote electronic money as an alternative access to financial services for those who historically have not been able to be part of the formal banking system, making available to the public a user-friendly alternative payment method by means of technological innovation.

  The electronic money industry is a heavily regulated activity and FIFL sets the regulations for: (1) requirements for the constitution, authorisation, operation, capital and guarantees for electronic money provider companies; (2) requirements that banks, cooperative banks and savings and loan companies must meet to provide electronic money; (3) generation and use of electronic money, as well as establishing the entities that can provide it; and (4) create underlying principles for the formulation of public policies to promote financial inclusion.

  Electronic money provider companies, who are responsible for making available electronic money to the public and related services thereof, must first obtain a licence from the financial regulator before their incorporation and beginning of operations. These companies may manage and operate mobile payment systems. These companies must have adequate personnel, equipment and technological means to provide electronic money and related services, administrative control systems, security applications, business plans, manuals, procedures, policies, internal controls, and business continuity plans that guarantee the proper functioning of the services.

  Electronic money provider companies may request the Central Bank to authorise them to be administrators of mobile payment systems, provided that they comply with the requirements that the Central Reserve Bank provides. Mobile payment administrators may be authorised to operate

technological systems or platforms that allow payments or money transfers, mainly electronic money, between products from different financial institutions and regardless of the mobile telephone operator that the client has.

2. Regulations on crypto assets: please provide a summary of the legal framework of crypto assets in your country and how crypto assets are regulated in your jurisdiction.

El Salvador is developing a complete legal framework for the use, promotion, implementation and trading of crypto assets. Below, you will find a summary and description of the most relevant laws:

- *The Bitcoin Act*: The Bitcoin Act introduces and regulates Bitcoin as legal tender in El Salvador to facilitate the use of Bitcoin in the country. Some of the most relevant aspects of the Bitcoin Act are: (1) Bitcoin can be used as a payment alternative since it has legal recognition/support and the same/similar effects as a fiat money currency; (2) all prices may be expressed in Bitcoin; (3) taxes may be paid in Bitcoin; and (4) it obliges every economic agent to accept Bitcoin as a payment alternative when acquiring goods or services. It also establishes that the state shall promote the training and mechanisms necessary for the population to access Bitcoin transactions.

  The Bitcoin Act has been complemented and developed by statutory provisions/regulations enacted by the government, with the following being the most relevant:

  - The Bitcoin Act Statutory Provisions (*Reglamento de la Ley Bitcoin*), which sets the rules and framework for the provision of Bitcoin-related services. For the provision of custody, exchange and digital wallet services, providers must apply for registration before the Bitcoin Service Providers Registry managed by the Central Reserve Bank of El Salvador.

  - NRP-29 Technic Rules to Facilitate the Participation of Bank in the Bitcoin Ecosystem (*Normas Técnicas para Facilitar la Participación de las Entidades Financieras en el Ecosistema Bitcoin*), which establishes certain rules to facilitate banks' participation/involvement in the bitcoin ecosystem.

- *Issuance of Digital Assets Act (LIDA)*: LIDA creates a legal framework for operations involving digital assets used in public or private offerings carried out in El Salvador, as well as regulating the requirements and obligations of issuers, digital asset service providers, and other participants that operate in the market, aiming to promote the development of the digital asset market and protecting investors.

  In essence, the LIDA creates the framework for the offering, selling, issuance and regulation of digital assets. In El Salvador, digital assets are not considered securities per se and have different regulations and legal treatment as the El Salvador securities market has.

  The LIDA set some specific minimum rules to ensure the proper functionality of the digital asset market. For instance, the issuance of digital assets is divided between public offerings and private placements, each of which is subject to specific trading and offering rules and restrictions. Furthermore, the LIDA provides certain rules to ensure market integrity and prevent insider trading and market manipulation, among others. Per LIDA, the key market players are:

- *Digital Asset Service Providers*, defined as any person whose main line of business involves rendering one or more digital asset services. Digital asset service providers are the main facilitators and enablers of the market as they are responsible for providing all the structure and service for the issuance and trading of digital assets, including services such as: (1) the exchange of digital assets for fiat money or equivalent or for other digital assets; (2) placing of digital assets on digital platforms or wallets; (3) transfer of digital assets or the means of accessing or controlling them, between the acquirers, electronic wallets or digital asset accounts; (4) executing of orders to buy or sell derivative digital assets; and (5) issuance of certifications of digital assets and smart agreements. Prior to rendering any services, digital asset service providers must register before the National Digital Assets Commission, and must meet some requirements, such as providing the business and technological capabilities to render said services.
- *National Digital Assets Commission*, the main regulator of the market and whose purpose is to promote, protect and strengthen the digital assets market in El Salvador. The Commission has the prerogative to issue rules and statutory provisions to regulate the market and supervise all the participants therein.
- *Certifiers*, which are responsible for performing a financial, legal, technical and administrative analysis of the information supporting digital assets issuances.
- *Issuers*, which can comprise the state, individuals, companies, either private or public.
- *Investors*, any person or entity that acquires or invests in digital assets.
- *Bitcoin Fund Management Agency*, which is attached to the Ministry of Economy and receives resources from the General Budget of El Salvador. This agency: (1) manages and holds all funds from public offerings of digital assets carried out by the State of El Salvador or any of its autonomous institutions; (2) invests the funds from public offers made by the State or any of its autonomous institutions; (3) dictates internal regulations and establishes its organisational structure; (4) supervises and controls the entities where investments have been made; and (5) makes direct agreements/contracts that it considers necessary to carry out operations.
- *Registry of Digital Asset Service Providers*, administered by the National Commission for Digital Assets.

LIDA also grants tax benefits to issuers, digital asset service providers and investors. The benefits include a total exemption from income, VAT, and other existing or future taxes in El Salvador.

3. Payment service providers and digital wallets: please describe how payment service providers and/or digital wallets are regulated in your country. Please mention any foreseen law or regulation in this respect.

In El Salvador, the legal framework regulating payment services providers is as follows:

1. *FIFL*, mentioned and described in Question 1;

2. *The Bitcoin Regulation and LIDA*: One of the services contemplated by the Bitcoin Regulation and LIDA is the provision of digital wallets, which are defined by the LIDA as 'an electronic device or a mobile application that allows transactions through the exchange of digital asset units and scriptural money and is also known as an "electronic wallet"'. See Question 2; and

3. the Central Reserve Bank has issued regulations for the operation of automated clearing houses (ACH) payment systems. These regulations foresee an update on the payment systems and the development of ACHs in El Salvador. They also establish the requirements to become an ACH system operator and therefore carry out transferences among local banks in El Salvador.

Additionally, the most relevant aspects regarding digital wallets are:

- *LIDA*: As mentioned before, one of the services contemplated by the LIDA is the provision of digital wallet services, which is defined as an electronic device or a mobile application that allows transactions to be carried out by exchanging units of digital assets and scriptural money. For more information, see Question 2; and

- *FIFL*: This Act facilitates the implementation of mobile payment systems, which, to some extent, resemble digital wallets. For more information, please refer to Question 1.

4. Special support to fintechs: does your jurisdiction provide any special programme supporting fintech ecosystems, in particular fintech start-ups (eg regulatory sandboxes, accelerator programmes). Are such programmes supported by the regulator in your country?

There are no special programs supporting fintech ecosystems. However, as previously mentioned, the El Salvador government is aiming for growth in this area with laws like LIDA, which indirectly intends to support and promote fintech by creating a clear framework and granting tax exemptions.

5. Open banking: please advise whether in your jurisdiction there are regulations on open banking. If the response is no, please provide any reference to regulations that may directly or indirectly affect open banking. Please include any foreseen laws and regulations on open banking.

Currently in El Salvador, there are no regulations for open banking. Nevertheless, open banking may not be feasible given the existing banking regulation since in El Salvador passive banking activities require a licence and the collection of funds without a banking licence would be considered a crime.

The Banking Act establishes that any collection of funds from the public with or without advertising, on a regular basis and under any form, is prohibited to those who are not authorised according to the Banking Law and other rules that regulate this matter. The violation of these provisions will be punished according to the Criminal Code.

Guatemala

Claudia Pereira Rivera*
Mayora & Mayora, Guatemala City
cpereira@mayora-mayora.com

María Fernanda Morales Pellecer†
Mayora & Mayora, Guatemala City
mfmorales@mayora-mayora.com

Carlos Ortega Aycinena**
Mayora & Mayora, Guatemala City
cortega@mayora-mayora.com

1. Fintech regulatory framework: please provide a description of the most relevant laws and regulations on fintech and financial innovation in your country. Please also refer to any new law or regulation foreseen in the near future or any bill on fintech and financial innovation in your jurisdiction.

Currently, Guatemala has not issued laws and regulations concerning fintech and financial innovations. However, the lack of regulation has not limited Guatemala's ability to venture into the fintech world – indeed, to this date Guatemala is among the fastest growing Central American countries in fintech.

It is worth mentioning that, although fintechs have not yet been regulated in Guatemala, this does not exempt them from complying with existing laws applicable to any company incorporated in Guatemala, nor with laws related to anti-money laundering and counter-terrorism financing (AML/CFT). Additionally, they must comply with laws that limit activities strictly reserved for financial institutions such as receiving money deposits, and lending money to third parties with funds received as deposits.

---

* Claudia joined Mayora & Mayora in 1998 and became a partner in 2004. She currently heads the Banking, Finance and Commercial practice area and is Vice-Chair of the firm's Board of Directors. International agencies, publications and directories such as Chambers & Partners, The Legal 500 and Latin Lawyer, recognise her as a leading lawyer in banking, finance, corporate, commercial and M&A matters, highlighting her expertise in complex cases. She has advised renowned clients such as Marriott International, Chevron and Citibank, among others.
She was also part of the team from the firm responsible for the privatisation of the Guatemalan telecommunications industry. She is a member of the Board of Directors of the Pro Bono Association of Guatemala on behalf of the firm, a very important institutional initiative in the country. She participates annually in various international conferences and congresses organised by professional and academic institutions.

† María Fernanda has been part of the firm since 2008, as an expert in banking and financial law, and was promoted to partner in 2019. Prior to joining Mayora & Mayora, she was Director of Special Verification Intendency (IVE) of the Superintendency of Banks of Guatemala, as well as in-house legal adviser to several national and international banks. Her professional experience has provided her with a broad and intimate knowledge of financial and banking regulations.
She has been a university professor for more than twenty years in subjects such as commercial law, civil law and financial institutions, among others. Her postgraduate studies include courses on banking, money laundering, financing of terrorism and administrative law at institutions in Costa Rica, Mexico, Spain and the United States.

** Carlos joined Mayora & Mayora in 2012. He has extensive experience in commercial, civil, contract, banking and financial law. During his professional career, he has provided services to different clients, especially in banking, financial and commercial advice, as well as in national and international mergers and acquisitions. He was assistant professor of Civil Contracts at Francisco Marroquín University. He holds a Master's Degree in American Law with a specialisation in International Business from Boston University and has completed other postgraduate studies at Harvard University.

2. Regulations on crypto assets: please provide a summary of the legal framework of crypto assets in your country and how crypto assets are regulated in your jurisdiction.

With respect to crypto assets, Guatemala has not regulated them. However, Guatemalan laws currently in effect do not prohibit the commercialisation of crypto assets. Consequently, in Guatemala the commercialisation of crypto assets is permitted, and can be used as a paying mechanism if the parties freely agree to it. Such transactions will be made wilfully by the parties and will not be covered by any specific financial law or government insurance coverage.

In 2021, when El Salvador opted to use crypto assets as a paying mechanism, the Guatemalan banking authority (Superintendency of Banks) issued a press release in which they clarified that, because cryptocurrency is not an official foreign currency in any country, its use would not be secured by the Guatemalan government, and it cannot be forced as a payment mechanism.

3. Payment service providers and digital wallets: please describe how payment service providers and/or digital wallets are regulated in your country. Please mention any foreseen law or regulation in this respect.

With respect to payment service providers and digital wallets, Guatemala has not yet regulated their use. However, fintechs can venture into creating payment services and digital wallets if they do not fall within the scope of activity of a banking and financial institution (ie, receiving monetary deposits). Any payment service that falls within the scope of a banking and/or financial institution would require a banking licence. The foregoing does not prohibit nor limit a fintech's ability to create payment services and/or digital wallets for banking institutions, nor as a standalone service subject to the legal prohibition to receive money deposits without having the licence to operate as a bank or financial institution.

4. Special support to fintechs: does your jurisdiction provide any special programme supporting fintech ecosystems, in particular fintech startups (eg regulatory sandboxes, accelerator programmes). Are such programmes supported by the regulator in your country?

The Guatemalan government has not created special programmes to support fintechs. There is, however, a fintech association that promotes and advises individuals and/or companies that seek to venture into fintech. This association is of a private nature.

There was a sandbox project for fintech regulation sponsored by the Superintendency of Banks; however it has not been active recently.

5. Open banking: please advise whether in your jurisdiction there are regulations on open banking. If the response is no, please provide any reference to regulations that may directly or indirectly affect open banking. Please include any foreseen laws and regulations on open banking.

There are no laws that promote or limit open banking. Consequently, financial institutions can contract with fintechs that provide open banking services. Due to the confidentiality of banking transactions, any exchange of banking information between a banking institution and a fintech would require the express authorisation of the individual that seeks to use open banking through its banking institution, and the express authorisation of the banking institution.

Final remark

In Guatemala, as we have mentioned above, there are no specific laws and regulations related with fintechs, crypto assets, digital wallets and open banking. Nevertheless, the National Strategy for Financial Inclusion for the years 2019–2023 (*Estrategia Nacional de Inclusión Financiera* or ENIF), which is elaborated by Guatemalan monetary authorities, includes plans to enact laws and regulation regarding these financial services.

Honduras

José Ramón Paz Morales*
Consortium Legal, Tegucigalpa
josepaz@consortiumlegal.com

Karla Andino†
Consortium Legal, Tegucigalpa
kandino@consortiumlegal.com

José Manuel Hernández**
Consortium Legal, Tegucigalpa
josehernandez@consortiumlegal.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

The fintech industry has grown significantly in Honduras since 2018 when a Fintech Congress, organised by the Inter-American Development Bank, took place.

Subsequently, the National Congress of Honduras held assemblies in which bills were discussed to regulate the services offered by these new entities. This resulted in the publication of Legislative Decree No 83-2021, by which it was ordered to the Central Bank of Honduras to regulate the organisation, operation and functioning of national and foreign legal entities that provide payment and transfer services, as well as to regulate these services.

Honduras has regulations regarding electronic wallets, as well as the Law of Electronic Commerce which regulates activities related to electronic transactions. However, it was not until 2021, after Decree No 83-2021 was issued, that the Central Bank of Honduras and the National Banking and Insurance Commission were empowered at a legislative level to regulate the services offered by fintechs. As a result, the Central Bank of Honduras issued the following regulations:

1. Regulation for Payment and Transfer Services Using Electronic Money; and

2. Regulation for Services Offered by Electronic Payment Service Providers.

The most recent regulatory development in the country is that, in February 2024, the National Banking and Insurance Commission issued a resolution in which it prohibits the institutions supervised by the National Commission to maintain, invest, intermediate or operate with cryptocurrencies, crypto assets, virtual currencies, tokens or any other similar virtual assets, which have not been issued or authorised by the Central Bank of Honduras as the country's

* José Ramón Paz Morales is a partner at Consortium Legal, and has 15 years of experience in banking law, financial law, stock market law, insurance and reinsurance law, corporate law, contract law and horizontal property law.

† Karla Andino is a senior associate at Consortium Legal and has 15 years of experience in the financial sector. She specialises in banking and corporate and has advised fintech companies that provide various financial technology services including payments processing services and gateways, technological software for financial institutions, electronic wallets, retail payment systems and credit card processors.

** José Manuel Hernández is an associate at Consortium Legal, and has extensive experience in advising fintech companies and vast knowledge in banking and corporate law processes. He has advised several financial institutions and has participated in mergers, acquisitions and corporate reorganisations in the financial sector.

monetary authority, as well as not allowing their financial users to utilise their platforms to perform operations with the aforementioned instruments.

It is worth mentioning that these new regulations complement the existing regulations that regulate financial services performed in a traditional or analogous way, such as the Securities Market Law, Financial System Law and others. Over time, these have fulfilled the role of dictating the basis of the procedures to be performed and the definitions that the regulator issues on the services to be offered. Therefore, to understand the regulatory regime that may be applicable to fintechs, assessing the different laws, regulations and resolutions issued by the regulators together is recommended.

The new fintech regulation is considered innovative due to the challenges that the regulator faces in entering and regulating the organisation, operation and functioning of national and foreign legal entities that provide fintech services through technological platforms, but specifically regarding electronic payments. Notwithstanding this, such regulation is likely to evolve as new technologies become more present in the Honduran market. Currently the purpose of the regulators is merely data collection, registration and analysis of services provided by electronic payment service companies. This could mean that in the future the regulation could be broadened to other financial technologies as well as the adoption of a more defined role in the supervision of these as it is currently exercised by the regulations applicable to financial institutions.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

There have been no specific regulations issued regarding crypto assets or cryptocurrencies as of June 2024. Regulators have been waiting to see how the adoption and uses of cryptocurrencies turn out, though this matter is expected to be tackled by provisions that will emerge from the Board of Financial Action Task Force´s (FATF) recommendations and statements from 2019.

It is worth mentioning that the Central Bank of Honduras issued a statement in February 2018 warning users that cryptocurrencies are not endorsed by it and that it does not regulate cryptocurrencies, nor does it ensure or guarantee their trading. Thus, any transaction performed using cryptocurrencies are under the responsibility and risk of each user.

The most recent regulatory communication regarding crypto assets in the country is that of February 2024, in which the National Banking and Insurance Commission issued a resolution in which it prohibits the institutions supervised by this regulatory entity (financial and insurance institutions, among others) to maintain, invest, intermediate or operate with cryptocurrencies, crypto assets, virtual currencies, tokens or any other similar virtual assets which have not been issued or authorised by the Central Bank of Honduras as the country's monetary authority, as well as not allowing their financial users to utilise their platforms to perform operations with the aforementioned instruments.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

As previously mentioned, two recent regulations were issued related to these products and services: the Regulation for Payment and Transfer Services through Electronic Money; and the Regulation of the Services Offered by the Electronic Payment Service Providers.

The Regulation for Payment and Transfer Services through Electronic Money provides a regulatory framework for entities that will provide this product and service as they come under the regulatory scope of supervised and regulated entities. This supervision function is performed jointly by the National Banking and Insurance Commission, due to the withholding of electronic money and the conversion of physical money to digital money, and by the Central Bank. The supervision includes among others, aspects related to the prevention of money laundering and financing of terrorism.

On the other hand, the Regulation of Services Offered by Electronic Payment Service Providers lists, among others, some of the following staple electronic payment services:

- payment gateways;
- merchant services;
- payment services for remittances;
- collection services;
- payment transactions with government entities;
- e-commerce payments;
- payments for purchases in commerce; and
- others that may be authorised by the Central Bank by administrative ruling.

This regulation requires electronic payment services providers to comply, among other things, with a registration in the special registry of fintech companies the Central Bank has created to this effect. However, as of June 2024, the regulation does not carry out supervision and control over the fintech companies registered in the EPSPE Registry.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

In Honduras there is no legislation or regulation to his effect, and as of June 2024 there are no regulatory sandboxes in Honduras.

However, the Honduran Fintech Association (AFINH) gathers Honduran and international fintech companies with the main purpose of uniting the industry and having a stronger presence before the regulator in terms of proposals that benefit the development of the industry in the country.

Additionally, at the initiative of the regulators, a Financial Innovation Roundtable (MIF) has been created, which is a public-private collaboration forum promoted and managed by the Central Bank of Honduras (BCH) and the National Banking and Insurance Commission (CNBS). It promotes innovation and healthy competition in the provision of financial products and services through the use of technology and digitisation, with the aim of contributing to financial inclusion through the adoption and use of financial technology.

The function of the Financial Innovation Roundtable is to prepare and present to the representatives of the public sector technical proposals prepared by the working groups and presented at the plenary meeting of the MIF, with the sole purpose of fulfilling the general and specific objectives of the Roundtable.

To facilitate the formulation of proposals for improvement in operational, regulatory and technical matters, the MIF currently has two working groups:

- Payments and Transfers; and
- Transversal Technologies and Alternative Financing.

These working groups are integrated by members of the public and private sector, who work together to address current problems for the development of the fintech industry in the country and propose these problems to the regulators in order to obtain possible innovative solutions to expand the development of fintech.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

Currently in Honduras, there are no specific regulations for open banking, however there are no prohibitions against it either. Currently the Financial System Law and the Commercial Code would be the base to start considering the potential limitations of open banking in Honduras. As of June 2024, we do not foresee any laws or regulations to this effect.

Mexico

Miguel Gallardo-Guerra*
Bello, Gallardo, Bonequi y García, Mexico City
mgallardo@bgbg.mx

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

Over the past few years, we have seen the evolution of financial systems, mainly how transactions and their functions have changed or targeted specific sectors.

As a result, financial systems have adopted increasingly automated or digital transactions, securities and systems to facilitate financial relationships between their subjects – whether users, clients, financial intermediaries or government regulators.

Mexico has issued laws, provisions and guidelines to regulate fintech entities, including (most importantly), the Law to Regulate Financial Technology Institutions (the Fintech Law) published in the *Official Federal Gazette* in March 2018. In January 2021, the applicable provision to regulate the electronic payment fund institutions referred to in article 48, second paragraph; 54 first paragraph, and 56, first and second paragraphs of the Fintech Law was published by the Ministry of Finance and Public Credit. Finally, in March 2021, the third version of the Guidelines for the application of authorisation for the organisation and operation of electronic payment funds was published by the National Banking and Securities Commission (the 'Commission').

These institutions are legal entities authorised by the Commission to carry out activities. The Fintech Law describes two types of financial technology institutions:

- collective financing institutions (crowdfunding), which carry out activities intended to connect the general public to provide financing through debt, capital, co-ownership or royalty financing transactions, carried out through computer applications, interfaces, web pages, or through any other means of electronic or digital communication; and
- electronic payment fund institutions providing services on a regular and professional basis, consisting of issuing, administration, redemption, and transmission of electronic payment funds (wallets).

Currently, the Commission has authorised and registered 76 financial technology institutions, including collective financing institutions and electronic payment fund institutions, duly conducting activities in Mexico.

---

* Miguel is a senior partner and managing director at the Mexican law firm bgbg. He is Head of the banking, finance, fintech, and compliance practice areas, and has been certified by the National Banking and Securities Commission as a compliance officer and anti-money laundering expert, as well as by the National Insurance and Bonding Commission as an insurance contract expert.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

Arising from the global evolution in technology, payment methods have also evolved. Today we have a new challenge, the so-called 'virtual assets' as defined by Chapter Three of the Fintech Law:

> 'The representation of value registered electronically and used among the public as a means of payment for all legal acts is deemed as a virtual asset and the transfer of which can only be carried out through electronic means. In no case shall the legal tender in national territory, currencies, or any other asset denominated in legal tender or currency be understood as a virtual asset.'

Under Mexican law, a virtual asset has several characteristics, including that: it is security; it is electronic; it is a payment means used by people; it can only be carried out by electronic means; and national currency, currencies, or other assets in the legal tender may never be taken as a virtual asset.

The Bank of Mexico has issued its opinion regarding virtual assets, in addition to issuing regulations limiting them in various ways. The Bank of Mexico established that virtual assets have several problems as a substitute for the Mexican currency, derived from the fact that they do not feature money characteristics as we know them: deposit in value, means of exchange or unit of account. In Mexico, the Bank of Mexico is an autonomous constitutional entity responsible for issuing currency, generating economic policies to protect the purchasing power of our currency, working to ensure that Mexicans have a healthy financial system and ensuring that payment systems function properly.

In March 2019, the Bank of Mexico published the Ruling 4/2019 regarding virtual assets in the *Official Federal Gazette*. Such ruling provides that in connection with virtual assets, there is a problem of information asymmetry produced by two causes:

- the complexity of the mathematical and cryptographic processes that support virtual assets and the difficulty for users in knowing such processes; and
- the complexity of the factors that determine the price of virtual assets, the unawareness of the elements that determine supply and demand, and the lack of any reference with which an estimate of their price can be obtained.

Another position of the Bank of Mexico is that virtual assets represent a significant risk in terms of preventing operations with illicit resources and terrorism financing due to the ease of transferring virtual assets to different destinations, as well as the absence of controls and protection measures at a global level.

Accordingly, the Bank of Mexico established that distance must be kept between virtual assets and the financial system; however, the Bank of Mexico also established that it also seeks to promote and take advantage of the use of technologies that could have a benefit, as long as they are used in the context of the internal operation of financial technology institutions and banking institutions. This does not imply an increase in operational and financial risks, so we must understand that it is intended to protect the final consumer.

That is why, in the second paragraph of Provision Three of Ruling 4/2019, it is clearly stated that the institutions authorised to operate virtual assets must prevent the transfer, directly or indirectly, of the risk of such transactions to the institution's customers.

As a result of the policy of the Bank of Mexico and the limited regulation issued by Mexican authorities to promote the sector to date, virtual assets have not been substantially adopted by financial institutions. However, taking into account that such Ruling 4/2019 does not apply to commercial entities, the crypto assets sector has evolved mainly in the commercial arena, where different sectors have implemented crypto assets as an option to conduct commercial transactions, mainly adopting the most popular crypto assets, such as Bitcoin.

The Tax Administration Service and virtual assets

In addition, the Tax Administration Service (Servicio de Administración Tributaria or SAT) has established virtual assets in accordance with Article 17, section XVI of the Federal Law on the Prevention and Identification of Transactions with Illegally-Obtained Funds (LFPIORPI), applicable to commercial transactions between companies or persons, other than financial institutions, as a vulnerable activity:

> 'The usual and professional offering of exchange of virtual assets by subjects other than financial institutions that are carried out through electronic platforms, who manage and operate by facilitating or conducting operations to buy or sell such assets owned by their customers, or providing means to keep, store, or transfer virtual assets other than those recognised by the Bank of Mexico in terms of the Fintech Law.'

As of February 2020, it is mandatory to carry out the registration procedure related to virtual assets as a vulnerable activity for the LFPIORPI with the SAT through the system of the Anti-Money Laundering website. Therefore, notices must be submitted by the 17th day of the following month in which the act or transaction was made to the Financial Intelligence Unit through the SAT, where the amount of the transaction performed by each customer is equal to or greater than 645 units of measurement and update (UMA), provided that such UMA has currently an exchange rate of MXN108.57 per UMA – even if that threshold is reached by the aggregation of transactions. However, if no transaction has been carried out during the corresponding month, a report shall be submitted stating that no acts or transactions were carried out in the corresponding month that are the subject of the notice.

Furthermore, the SAT states that information and documentation that supports the vulnerable activity must be kept, protected and prevented from destruction or concealment, as well as the document that identifies its customers or users, for a period of five years from the date of the performance of the activity.

Therefore, those who carry out the vulnerable activity with virtual assets must have a document with their guidelines for identifying customers or users, as well as the internal criteria, measures and procedures to comply with the provisions of the LFPIORPI, its regulations, general rules, and other requirements derived from this law.

Given the abovementioned, this regulates the prevention of money laundering and terrorism financing, which is one of the concerns of our central bank.

Ruling 4/2019 on General Provisions applicable to Credit Institutions and Financial Technology Institutions in Transactions with Virtual Assets

In accordance with the first provision of Ruling 4/2019, the purpose is to:

- determine virtual assets;
- establish the limitations of the transactions that institutions may carry out with virtual assets;
- establish the time limits, terms, and conditions to be met by the institutions in cases where the virtual assets with which they perform transactions become other types of virtual assets or change their characteristics;
- determine the information related to virtual asset transactions that the institutions must submit to the Bank of Mexico to obtain authorisation to perform transactions with virtual assets; and
- establish the characteristics of the authorisations.

The Bank of Mexico states that only fintech entities and banking institutions shall be able to perform transactions with virtual assets internally. Internal transactions are those activities carried out to carry out passive, active and service transactions that they execute with their customers or that they carry out on their proprietary account, including activities carried out by the institutions to support the international transfers of funds they carry out.

While the Fintech Law gives us a definition regarding virtual assets, the Ruling is more concise and sets forth the characteristics of the virtual assets that can be used to perform transactions:

- to be identifiable units of information, electronically registered, that do not represent the ownership or rights of an underlying asset or that represent said ownership or rights for a value less than these;
- to have emission controls defined by protocol; and
- to have protocols that prevent replications of information units or their fractions.

However, the final paragraph of the fourth provision of this Ruling provides that the institutions may carry out internal transactions using virtual assets with characteristics other than those set out above, for which they must be subject to the provisions applicable to them regarding the use of automated data processing technologies and systems.

The Ruling is clear on how to perform transactions with virtual assets: it is only through authorisation granted by the Bank of Mexico for the term that it determines. Therefore, the institution must submit a request via email to the Management of Authorisations and Queries of the Bank of Mexico.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

In Mexico, companies that provide these services are those in charge of the issuance, management and redemption of balances registered electronically, known as electronic payment institutions or digital wallets. These balances can be used to make payments or electronic transfers through interfaces, internet pages, or any other means of electronic or digital communication.

Digital wallets must maintain one or more accounts of electronic payment funds for each client, as well as make the transfers of said funds among their clients through the respective instalments and charges in the corresponding accounts. Digital wallets may act as transmitters of money in accordance with the provisions of the General Law of Auxiliary Credit Organisations and Activities; may grant credit or loans in the form of an overdraft, subject to the conditions established in the Fintech Law; and may provide services related to payment instrument networks, issue securities on their account and transmit virtual assets on their account or on behalf of their clients.

It is important to mention that electronic payment institutions are prohibited from paying their clients interest or any other monetary benefit or profit for their accumulated balance. Likewise, an obligation is established so that the clients of these institutions designate beneficiaries, who will be given the corresponding funds in case of death.

The Law includes a catalogue of activities or services that will prohibit an electronic payment institution from being considered as such. Therefore, they must be incorporated under specific parameters and characteristics contemplated within the Fintech Law to operate in the market.

4. Crowdfunding institutions: a summary of regulations applying to crowdfunding service providers.

In Mexico, companies that provide these services are those aimed at putting people from the general public in contact with each other to grant financing, carried out regularly and professionally through computer applications, interfaces, internet pages, or any other electronic or digital communication media.

The clients of a crowdfunding institution may carry out between them and through such institution, either (1) debt crowdfunding so that investors may grant loans, credits, mutuals, or any other financing causing a direct or contingent liability to the applicants; (2) crowdfunding for investors to purchase or acquire securities representing the capital stock of legal entities acting as applicants, and (3) crowdfunding of co-ownership or royalties for investors and applicants to enter into joint ventures or any other type of agreement by which the investor acquires a proportional share or participation in a current or future asset or in the income, profits, royalties, or losses to be obtained from the performance of one or more activities or projects of an applicant.

The transactions mentioned in the paragraph above shall be denominated in local currency. Likewise, the crowdfunding institutions may carry out such transactions mentioned above in foreign currency or with virtual assets, in the cases and subject to the terms and conditions established by Bank de México through general provisions issued for such purpose.

The crowdfunding institutions will be prohibited from assuring returns or yields on the investment made or guaranteeing the result or success of the investments.

5. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

In Mexico, the Fintech Law provides regulations applicable to a regulatory sandbox, attempting to regulate technologies that have facilitated accessibility to financial services which break with traditional schemes and whose main component is innovation. The authorities are aware of this and want to leave open the possibility of new players in the market with technological solutions other than those described above.

All companies that want to enter the market without breaking the law must obtain temporary authorisation from financial authorities, which will be granted or denied in a discretionary manner, and which will have a duration consistent with the services that are intended to be provided and that may not be greater than two years.

Any entity filing for a sandbox registration shall provide the following documentation and information to the Commission:

- the draft bylaws, including an innovative model;
- the product to be offered or the service to be provided to the public, which must require testing in a controlled environment;
- the description of the risk analysis policies, including the procedures to be followed regarding technological infrastructure security and information security;
- the way in which the reserved activity is to be developed must represent a benefit to the client of the product or service in question with respect to what exists in the market;
- establishment of the target market or a maximum number of clients to whom the product or service would be offered;
- how the entity will be able to compensate the damages caused to their clients due to the provision of services granted during the development period;
- evidence the project is at a stage where the start of operations can be immediate, allowing it to be tested with a limited number of clients; and
- the exit procedure to be carried out in case financial authorities do not grant the definitive authorisation, registration, concession, or if the validity of the temporary authorisation or its extension expires, as appropriate.

The definitive authorisation to continue providing services regularly must be processed during the temporary period granted to the legal entity that seeks to operate in the market. At the discretion of the financial authority, the temporary authorisation may be extended for up to one more year

to obtain a definitive authorisation. It is essential that once these types of companies obtain their temporary authorisation, they must prepare and deliver reports to the financial authorities in the timeframe and terms indicated so as to inform:

- the number of transactions carried out during the period;
- the number of clients;
- any risk situations that have arisen during the period; and
- all other information required by financial authorities.

The regulatory sandbox has not been successful in the Mexican market, mainly because of the financial authorities' strict approach to this business model. At this moment, no regulatory sandbox has been approved by the Commission.

6. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

Under Mexican law, open banking is regulated under the Fintech Law, which provides under Article 76 that financial entities shall establish standardised computer application programming interfaces that enable connectivity and access to other interfaces, developed or managed by the same entities and third parties specialised in information technology, to share open financial data, aggregated data and transactional data.

Such regulations also provide that entities may only use the information for the purposes previously authorised by customers, provided that open banking will be subject to further rules to be issued by financial authorities, including the Bank of Mexico. The entities enabled to apply open banking must be authorised by the Bank of Mexico, provided that financial authorities shall approve any applicable commission.

Currently, there are some rulings issued by Mexican financial authorities in connection with open banking, focused mainly on public information related to ATM location data. The next set of regulations is expected to address the sharing of customers' transaction data.

Nicaragua

Gloria Alvarado
Alvarado Y Asociados, Managua
gmalvara@alvaradoyasociadoslegal.com

Alfredo Montano Acuña
Alvarado Y Asociados, Managua
amontano@alvaradoyasociadoslegal.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

In Nicaragua there are no specific regulations regarding fintech. However, several laws address related topics, namely:

- Law No 974, Law of the Nicaraguan Legal Digest of the Matter of Banking and Finance approved on 10 May 2018 and published in *Official Gazette* No 164 of 27 August 2018, is a compendium of laws and regulations on banking issues;
- Law No 732, Organic Law of the Central Bank of Nicaragua, approved on 14 July 2010 and published in *Official Gazette* No 148 and 149 of August 5 and 6, 2010 respectively, states that it is the responsibility of the Central Bank of Nicaragua to approve the rules for the operation and surveillance of the country's payment system;
- Law No 561, General Law of Banks, Non-Banking Financial Institutions and Financial Groups, approved on 27 October 2005 and published in *Official Gazette* No 232 of 30 November 2005;
- Law No 1072, approved on 12 May 2021 and published in *Official Gazette* No 89 of 17 May 2021, the law on reforms, and additions to Law No 977, the law against money laundering, financing of terrorism and financing of the proliferation of weapons of mass destruction, and additions to Law No 561, General Law of Banks, non-banking financial institutions and financial groups;
- Law No 842, Law for the Protection of the Rights of Consumers and Users, approved on 13 June 2013 and published in *Official Gazette* No 129 of 11 July 2013, and its regulations Decree No 36-2013, approved on 10 October 2013 and published in *Official Gazette* No 192 of 10 October 2013, contains provisions on electronic transactions of financial services; and
- Resolution CD-BCN-XXV-1-22, Regulation of Financial Technology Providers of Payment Services and Virtual Asset Service Providers, published in *Official Gazette* No 76, on 27 April 2022. Contains reforms approved by Resolution CD-BCN-LXIX-2-22 of 20 October 2022 and published in *Official Gazette* No 212 of 11 November 2022. Its purpose is to regulate the authorisation process of financial technology providers of payment services and establish other provisions applicable to authorised providers.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

There is no specific regulation on crypto assets. However, Resolution CD-BCN-XXV-1-22, Resolution CD-BCN-LXIX-2-22, and Resolution CD-BCN-XLIX-3-23 of July 26, 2023 (published in *Official Gazette* No 140 of 3 August 2023) incorporate new terminology, such as:

- virtual asset (the previous regulation only spoke of virtual currency);
- acquirer;
- strong client authentication (SCA);
- digital wallet (also called electronic wallet or e-wallet);
- virtual asset management account;
- fiat currency;
- contactless payments;
- online payment gateways;
- virtual asset service provider (VASP);
- electronic currency trading; and
- exchange services.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

Legal entities authorised and regulated by the Central Bank of Nicaragua (BCN), dedicated to providing payment services with (1) digital wallets, (2) mobile sales points, (3) electronic money, (4) purchase and sale services and electronic currency exchange, (5) fund transfer services, (6) online payment gateways, and (7) other innovative payment services catalogued by the BCN Board of Directors, and the procedures for obtaining the corresponding licence, are regulated in Resolution CD-BCN-XXV-1-22.

There is a Draft Law on Financial Technology Providers ('fintech') which has not yet been presented as a bill in the National Assembly, and is in a consultation period with the entities involved. The project aims to regulate the financial services provided by financial technology service providers, their incorporation, organisation and operation, and the corresponding regulatory authority.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

We found no government programmes that are supporting fintech. However, the Central American Bank for Economic Integration (CABEI) runs regional projects, such as the DINAMICA Initiative, CAMBio II, Dry Corridor and the Financial Sector Support Facility for Financing MSMEs. These seek to promote business and private sector development to generate jobs and income in order to contribute to economic development and poverty reduction in Central America and the Dominican Republic, by promoting the use of fintech in day-to-day business, among other issues.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

There is no specific regulation on open banking in Nicaragua. However, Article 115 of Law No 561 states that the Superintendency of Banks will establish a registration system, called a risk centre, which will have consolidated and classified information on bank debtors. The corresponding information will be available to financial institutions authorised by the Superintendency of Banks. Private risk centres will be subject to the approval and regulation of the Superintendency, and will be subject to reservation in accordance with the provisions of Article 113 of the Law. Banks will be able to provide information about their active operations to private credit bureaux, also with the restrictions on bank secrecy stablished in Article 113 of the same law.

Private risk centres are regulated in Resolution No CD-SIBOIF-577-1-MAR18-2009, approved on 18 March 2009 and published in *Official Gazette* No 79 on 30 April 2009.

Panama

Kharla Aizpurua Olmos
Morgan & Morgan, Panama
kharla.aizpurua@morimor.com

Roberto Vidal
Morgan & Morgan, Panama
roberto.vidal@morimor.com

Alejandro Vásquez
Morgan & Morgan, Panama
alejandro.vasquez@morimor.com

Miguel Arias
Morgan & Morgan, Panama
miguel.arias@morimor.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

There are currently no specific regulations for fintechs in Panama, nor does Panama have a fintech law. Therefore, fintech companies that enter the local market must do an in-depth analysis, based on regulations related to traditional banking and financial services, to understand grey areas in existing regulation which are or may be applicable to their business to mitigate any regulatory risk.

The most relevant laws which are relevant to the local fintech market are the following:

- Executive Decree 52 of 2008 – single text of the Banking Law (the 'Banking Law');
- Decree Law 1 of 1999 – on the Securities Market in the Republic of Panama and the Superintendence of the Securities Market (the 'Securities Law');
- Law 48 of 2003, which regulates money remittance houses (the 'Remittance Law');
- Law 23 of 27 April 2015, as amended ('Law 23') adopts measures to prevent money laundering, financing of terrorism and financing of weapons of mass destruction, and applies to:
    - regulated financial entities (*sujetos financieros regulados*) including, but not limited to, banks, trust companies, financial companies, leasing companies, factoring companies, issuers of credit cards, debit cards and prepaid cards, and entities dedicated to payment processing services or electronic money, among others. All of which, for the purposes of this law, are supervised by the Superintendence of Banks of Panama (SBP); and
    - regulated non-financial entities (*sujetos financieros no regulados*), which includes companies doing business in the Colón Free Trade Zone, foreign exchange companies, casinos, real estate companies or brokers, companies in construction, and lawyers and certified public accountants and notaries which perform certain specific activities including incorporating,

operating, and managing legal persons, managing bank accounts (savings or investments), and acting as a resident agent, among others. The regulated non-financial entities are supervised by the *Intendencia de Supervision y Regulación de Sujetos No Financieros.*

- Law 42 of 23 July 2001, as amended, and its regulation Executive Decree 213 of 26 October 2010, which regulates financial companies ('Law 42');
- Law 51 of 22 July 2008, as amended ('Law 51'), regulates e-commerce; and
- Law 81 of 2019 regulated by Executive Decree 285 of 2021 (the 'Data Protection Regulation') regulates the protection of personal data of natural persons, as well as its handling, storage and treatment.

There have been attempts to regulate as bills have been submitted for the consideration of our legislative branch, one of which was approved on 28 October 2022, but the President of Panama submitted objections on the grounds of unconstitutionality. The matter was sent to be decided by the Supreme Court of Justice, which ended up deciding that it was unconstitutional and therefore did not become a law.

We do foresee that the efforts to regulate these matters will continue and that new legislation will be enacted.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

Currently, there is no regulation applicable to digital or crypto assets, cryptocurrencies or virtual currencies in Panama. However, both the SBP and Superintendency of Securities Market (SSM) have issued public notices and opinions (respectively) stating that they do not monitor cryptocurrencies in general. Specifically, each entity established the following:

SSM

Through Opinion 07-2018, SSM indicated that it does not consider cryptocurrencies (specifically referring to Bitcoin) as currencies given that to date 'in the Republic of Panama, no inherent value has been given to Bitcoin or another type of cryptocurrency'. SSM also confirmed that the concept of 'securities' under the Securities Law does not encompass virtual currencies and/or currencies, so Bitcoin is not considered a security. Finally, SSM established that there is no forex regulation applicable to cryptocurrencies, since it only applies to currencies which are an exclusive and incidental activity of the broker dealer houses.

Through its Statement of 25 April 2018, it referred to cryptocurrencies as 'digital assets that are intended to make purchases, sales or other financial transactions, are created by companies or individuals and are stored electronically in a blockchain, a database that maintains a permanent record of these digital transactions'.

Therefore, the SSM does not consider that digital assets, cryptocurrencies or virtual currencies are subject to its supervision, so no licence is required to operate the activity object of this

memorandum: 'activity of exchange of virtual currencies or cryptocurrencies, using Bitcoin as currency and with a view to adding other cryptocurrencies'.

SBP

On 24 April 2018, the SBP issued a public notice where it warned the public in general about the use of 'Bitcoin or any other instrument of the same category' and that they do not have specific regulation, so they are not within the competence of the SBP.

At the date of said public notice the SBP also indicated that, no subject regulated by the SBP had requested authorisation to '[take] custody, invest, intermediate or operate with these instruments'. Additionally, it established that 'as usual, the Regulated will maintain due diligence measures to prevent the improper use of their services and platform, in accordance with the provisions of the Banking Law, Law 23 of 2015 and Agreement 10 of 2015 and other applicable regulations'.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

Panama does not have a Central Bank. The local regulator of the banking business is SBP and the administrative unit of the state-owned bank, Banco Nacional de Panama, which oversees and acts as clearing house for the local banking business.

There is no specific law applicable to payment service providers and digital wallets (other than Law 23 as detailed above). Nonetheless, given the existing regulation, such as the Banking Law or Law 23, there is existing regulation that should be analysed and considered in the regulatory analysis for any company looking to develop these businesses.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

In Panama, as of today there are no special programmes supporting the fintech ecosystem related to fintech startups, such as regulatory sandboxes and accelerator programmes.

Nonetheless, there are private initiatives and organisations that allow and provide programmes and spaces trying to help the development of this sector.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

Currently in Panama, there are no specific regulations for open banking. The banking business continues to be regulated and supervised by SBP.

Europe

Austria

Stephan Heckenthaler*
Binder Grösswang, Vienna
heckenthaler @bindergroesswang.at

Miriam Broucek
Binder Grösswang, Vienna
broucek@bindergroesswang.at

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

There is no special fintech or financial innovation legal framework established in Austria. There is also no legal definition of fintechs available.

However, the Austrian regulator, the Financial Market Authority (Finanzmarktaufsichtsbehörde or FMA) has publicly expressed its understanding of fintech companies. According to the FMA, companies that are active in the field of financial market technologies are commonly understood as fintechs. Fintechs typically focus upon information technology-based financial innovations, which are mostly – but not exclusively – developed by companies that do not hold regulatory licences, include interfaces to undertakings that hold regulatory licences, and may bring sustainable changes to the existing way of functioning of the financial sector.

Depending on the services offered and whether these services qualify as regulated financial services, fintechs active in Austria might – like all other companies – be subject to a licence requirement under the Austrian financial regulatory laws. The Austrian regulator has adopted a technology-neutral approach in this regard, which means that it is not the involved technology that is decisive, but the activity as such (substance over form).

The Austrian Banking Act (*Bankwesengesetz* or BWG) and the Austrian Securities Supervision Act (*Wertpapieraufsichtsgesetz 2018* or WAG 2018) provide for licensing requirements for regulated banking and investment services. The Austrian Payment Services Act (*Zahlungsdienstegesetz 2018* or ZaDiG 2018) provides for licensing requirements for regulated payment services. The management of investment funds or alternative investment funds is subject to a licensing requirement under the Austrian Investment Funds Act (*Investmentfondsgesetz* or InvFG) or the Alternative Investment Funds Manager Act (*Alternatives Investmentfonds Manager-Gesetz* or AIFMG). The provision of crypto asset services in Austria is currently subject to a registration requirement under the Austrian Financial Markets Anti-Money Laundering Act (*Finanzmarkt-Geldwäschegesetz* or FM-GwG).

If securities or investments are publicly offered and where there is no applicable exemption available, the requirement to publish a prospectus is required.

---

* Stephan Heckenthaler is a partner in Binder Grösswang's Banking & Finance Team. He serves as Co-Chair of the Banking Law Committee of the IBA. He focuses on financial services regulation.

Prior to starting any fintech business in Austria, we recommend conducting a thorough legal analysis to determine whether any regulated services might be carried out and whether a licence, registration or prospectus requirement would apply. FMA is generally strict, and any unauthorised provision of regulated services can result in high administrative fines.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

Austria has not established a specific regulatory framework regarding crypto assets. However, Austria has also implemented Directive 2018/843 (AMLD5) requiring crypto asset service providers to file for registration with the regulator and to follow the applicable rules on the prevention of money laundering and the combat of terrorist financing (AML). The respective provisions of AMLD5 have been transposed in the FM-GwG as defined above.

Article 2, no 21 of the FM-GwG uses the term 'virtual currencies' instead of 'crypto assets', and defines virtual currencies as a digital representation of value that is not issued or guaranteed by a central bank or a public authority. It is also not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange that can be transferred, stored, and traded electronically.

Article 2 No 22 of the FM-GwG further defines virtual asset service providers (VASPs) as providers (both natural persons and legal entities) that offer one or more of the following services:

- services to safeguard private cryptographic keys, to hold, store and transfer virtual currencies on behalf of a customer (custodian wallet providers);
- exchange of virtual currencies into fiat currencies and vice versa;
- exchange of one or more virtual currencies between one another;
- transfer of virtual currencies; and
- the provision of financial services for the issuance and selling of virtual currencies (eg in connection with an 'initial coin offering' or an 'initial token offering').

To provide these services in Austria, VASPs must apply for a registration under the FM-GwG from the FMA. It is noted that the FMA expressly refers to the principle of 'reverse solicitation' when it comes to the registration requirements for VASPs, and states that the obligation to register in Austria only applies if the initiative for concluding a contract originates from the foreign VASP and not from the customer. If a customer who is a resident in Austria intends to make use of crypto asset services provided by a foreign VASP at their own initiative, the registration requirement does not apply.

Like in other European countries, such as Germany, crypto asset service providers have gained increased regulatory attention. The FMA has developed a good understanding of the respective business models and is closely supervising registered VASPs' compliance with the AML-requirements under the FM-GwG.

The European Regulation on Markets in Crypto-Assets (MiCA), which will enter into force on 30 December 2024 in all European Union Member States, will significantly change the regulatory setup

concerning crypto-assets in Austria. We expect that several authorised crypto asset service providers will then passport their MiCA-licence to Austria and vice versa.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

Payment service providers are regulated in Austria based on the implementation of EU directives 2007/64/EC (PSD1) and 2015/2366 (PSD2) in the Austrian Payment Services Act (*Zahlungsdienstegesetz 2018* or ZaDiG 2018).

In line with PSD2, ZaDiG 2018 sets out an exhaustive list of regulated payment services, including:

- incoming and outgoing payment transactions;
- payment transactions involving the granting of credit;
- payment instrument transactions;
- money remittance transactions;
- account information services; and
- payment initiation services.

To provide regulated payment services, payment service providers are required to obtain a licence as a payment institution under ZaDiG 2018. Payment institutions are subject to a range of supervisory requirements such as requirements relating to own funds and risk management, suitability of directors and reporting. These requirements are based on those that apply to credit institutions. Austria has not made use of the option of Article 32 of the PSD2 to introduce a simplified form of payment institutions.

Providers that provide payment services based on payment instruments that can be used only in a limited way, such as the acquisition of goods or services only in the premises of the instrument issuer or within a limited network or for a limited range of goods or services, are exempted from the scope of the ZaDiG 2018 and do not need to obtain a licence. This 'limited network exclusion' stems from PSD2 and especially applies for store cards, fuel cards, membership cards, public transport cards, parking tickets, meal vouchers or vouchers for specific services.

It is noted that purely technical services are not subject to a licence requirement under the ZaDiG 2018. However, PSD2 has introduced the regulation of account information services and payment initiation services that until then have been considered purely technical services.

The regulatory framework relating to payment services has been under review, and amendments are on their way. The drafts of PSD3 and a new directly applicable Payment Services Regulation (PSR) have been published in June 2023 (see also Question 5).

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

The Austrian regulator FMA has established the FinTech Point of Contact, which may be contacted by fintechs to ask specific questions relating to licensing requirements, the obligation to publish a prospectus, compliance or anti-money laundering regulations. FMA made clear that this is not intended to substitute legal advice, but it will give guidance on specific questions.

The FMA has further established a special sandbox regime for fintechs in September 2020. A fintech may apply for admission to the sandbox to the FMA and, after admission, operate its business model in a test phase with a licence in the sandbox. If the test is successful, the fintech leaves the sandbox for regular supervision. It is also an objective of the sandbox to deepen the regulator's knowledge about innovations in the financial market.

The sandbox involves four stages: once the FMA has admitted a fintech to the sandbox, the second, pre-support stage, starts. In this stage, FMA experts agree with the fintech on test parameters, milestones, and timetable for the test. Potential restrictions and conditions attached to the licence are discussed. The pre-support stage is concluded with the grant of a licence or registration, and the entity is allowed to provide its regulated services within the scope of the test licence or registration. In the third stage, the actual test phase, the fintech provides its services and is supervised in doing so. In regular management meetings, the test parameters and milestones are discussed. In the last stage, the test phase is evaluated and the fintech exits the sandbox and is transferred to regular supervision.

As of 2023, eight fintechs have been admitted to the FMA sandbox. One has already obtained a licence for the provision of investment services and the marketing of digital securities. Five are currently in the process of obtaining a licence as a crowdfunding service provider under Regulation (EU) 2020/1503 on European Crowdfunding Service Providers. The other fintechs are in the process of obtaining a licence for investment services and banking services to provide regulated services connected to crypto assets.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

The term 'open banking' generally refers to services where financial data can be shared between different parties using application programming interfaces (APIs). In particular, data can be shared between payment service providers and third-party service providers. Open banking is therefore not a specific technology, but a new way of offering customers a wider choice of products and services.

The PSD2 is the main European legislative body that addresses open banking by requiring payment services providers to grant third party service providers access to their customers' payment accounts. They must provide access through a secure interface to customers' account information, and the ability to trigger payments via third-party service providers. Consequently, the ZaDiG 2018, implementing PSD2 in Austria, is the most important legal act in Austria when it comes to open banking.

Under ZaDiG 2018, two new payment services have been introduced: payment initiation services (*Zahlungsauslösedienste*), and account information services (*Kontoinformationsdienste*). To provide payment initiation services, a licence as a payment institution has to be obtained. As regards account information services, a mere registration with the FMA is sufficient.

The most important services offered to customers in this regard are:

- payment initiation services (PISPs): at the request of the customer, a transaction is initiated in relation to a payment account held with another payment service provider;
- account information services (AISPs): at the request of the customer, consolidated information about payment accounts with various payment service providers is made available to them by the account information service;
- payment instrument issuing service provider (PIISP): a third-party issuer inquires about the availability of an amount of money from the account-managing payment service provider.

The European Commission has recently published a package of legislative proposals concerning financial data access and payments, which will, among other things, replace PSD2. Since the introduction of PSD2 in 2015, the payment market has undergone significant changes globally and in Europe, including in Austria.

Essentially, the Commission proposes to amend and modernise PSD2 with a new Payment Services Directive (PSD3) and to introduce a directly applicable regulation on payment services – the Payment Service Regulation (PSR). It is one of the aims of the package to improve competitiveness of open banking services. However, in our view, the new regulatory proposal does not introduce radical innovations, but rather a fine-tuning of the existing regime.

Belgium

Audrey Zegers*
Altius, Brussels
audrey.zegers@altius.com

Elias Nys†
Altius, Brussels
elias.nys@altius.com

1. Fintech Regulatory Framework: Please provide a description of the most relevant laws and regulations on fintech and financial innovation in your country. Please also refer to any new law or regulation foreseen in the near future or any bill on fintech and financial innovation in your jurisdiction.

General

The fintech sector is gaining increasing importance in the Belgian market. Belgium's fintech industry covers a broad range of products and services, the most common ones being related to payments, lending, insurance, crypto assets and capital markets.

There is no legal definition of fintech under Belgian law. Fintech (financial technology) generally refers to startups or established firms that use technology to offer innovative processes, products or services in the financial sector. Today, there is also no single legal framework in place governing fintech entities in Belgium, and so no specific 'fintech licence'. Depending on their business model and on the nature of the services and products offered, fintechs and their activities may be subject to a diverse set of financial laws and regulations.

The Belgian legal framework is largely determined by legislative initiatives on European level that are either directly applicable or transposed and implemented into Belgian law. These essentially comprise:

- *Credit institutions*: the Act of 25 April 2014 on the legal status and supervision of credit institutions (Banking Act);
- *Consumer and mortgage credit providers*: Book VII of the Code of Economic Law;
- *Insurance companies*: the Act of 13 March 2016 on the legal status and supervision of insurance or reinsurance companies (the Solvency II Law) and the Act of 4 April 2014 on insurance;

* Specialising in corporate and financial as well as securities law, Audrey focuses on the regulatory aspects of banking and financial services, M&A and capital markets transactions involving financial institutions, as well as on loan finance. Audrey regularly assists Belgian and foreign corporate clients and financial institutions in both domestic and cross-border transactions and advises clients on regulatory matters including MiFID II, PSD II, AIFMD, EMIR, IDD, AML, as well as their Belgian equivalents and on consumer credit.

† Elias is an associate in the firm's banking and finance department. On a daily basis, Elias deals with a variety of financing transactions and various matters in the financial sector. He has diverse knowledge and experience in financial regulations such as AML, MiFID II, PSD II, UCITS and AIFMD. He regularly assists start-ups, fintech companies and well-established financial institutions with their compliance needs, approvals and authorisations, national and cross-border restructurings and discussions with supervisory authorities.

- *Payment institutions and electronic money institutions*: the Act of 11 March 2018 on the legal status and supervision of payment institutions and electronic money institutions, access to the business of payment service provider and to the activity of issuing electronic money, and access to payment systems (the Act of 11 March 2018) and Book VII of the Code of Economic Law;
- *Investment firms*: the Act of 25 October 2016 on the access to the investment services activity and the status and supervision of portfolio management and investment advisory companies, the Act of 25 April 2014 on the legal status and supervision of credit institutions and the Act of 2 August 2002 on the supervision of the financial sector and on financial services;
- *Financial intermediaries*: Book VII of the Code of Economic Law, the Act of 4 April 2014 on insurance and the Act of 22 March 2006 on intermediation in banking services and investment services and the distribution of financial Instruments; and
- *Crowdfunding service providers*: Regulation 2020/1503 on European crowdfunding service providers for business and the Act of 18 December 2016 on the recognition and definition of crowdfunding and containing various provisions on finance.

These are further complemented by executive (royal) decrees and soft law such as guidelines, circulars and communications issued by our Belgian regulators, the Financial Services and Markets Authority (FSMA) and the National Bank of Belgium (NBB).[1]

The regulatory financial services framework and the supervisory structure may be overwhelming for new fintech players. However, various initiatives have been taken by our regulators to make Belgium a fintech-friendly jurisdiction.

Public offers

Public offers of investment instruments in Belgium are regulated by the Act of 11 July 2018 on public offers of investment instruments and the admission of investment instruments to trading on a regulated market (the Prospectus Act). The Prospectus Act fully implements the Prospectus Regulation (2017/1129) in Belgium but also provides some further gold-plating. Prospectus and/or information note requirements may apply, not only to offerings of transferable securities, but also to offerings of other investment instruments. Investment instruments includes all types of instruments permitting to carry out a financial investment, regardless of the underlying assets. In practice, this is important, for example, for the offer and admission to trading of certain types of crypto, debt or real estate assets.

Lending

It is interesting to note that lending is not a regulated activity as such in Belgium. However, when developing lending as a professional activity, certain licensing and registration

1 Belgium has a 'Twin Peaks' supervisory architecture. Since April 2011, the supervision of the financial sector and financial markets is shared between FSMA and NBB.

requirements as well as mandatory legal provisions may apply depending on the type of clientele that are being targeted.

Following the European law model, fintech companies offering credit services to consumers must take into account Belgium's strictly regulated consumer credit framework. Registration as a consumer or mortgage credit provider or intermediary with the FSMA is required, depending on the intended activities. Strict information, conduct and publicity rules apply.

Furthermore, when providing lending activities to small and medium-sized companies on the Belgian market, fintech also must take into account mandatory legislation that aims to protect these companies. These mandatory requirements include code of conduct rules, specific information requirements, suitability tests, limitations on prepayment indemnities and nullity penalties on certain termination clauses.

Crowdfunding

Various types of crowdfunding platforms exist on the Belgian market:

- platforms through which the public can make a donation for a project or enterprise;
- reward-based platforms, which are platforms through which investors deposit money to receive a type of non-financial compensation;
- crowd-lending platforms, which are platforms through which investors invest in a project or enterprise through a loan (also referred to as loan-based crowdfunding); and
- equity-based crowdfunding platforms, which are platforms through which investors invest in a project or enterprise through a contribution in capital in consideration for a participation in the profits.

Since 2017, some of these crowdfunding platforms are regulated under Belgian law. Since the entry into force of the European harmonising framework in this context, the activities of Belgian crowd-lending and equity-based crowdfunding service providers are regulated by Regulation (EU) 2020/1503 of 7 October 2020 on European crowdfunding service providers for business (the Crowdfunding Regulation) as supplemented by the Belgian Act of 18 December 2016 on the recognition and definition of crowdfunding and containing various provisions on finance (the Crowdfunding Act). Belgian crowdfunding service providers must obtain an authorisation from the FSMA, meet certain organisational requirements, and comply with conduct and information rules (including the provision of key information sheets).

Offers of investment instruments to the public, without the involvement of a crowdfunding service provider, might be subject to other financial regulations. For example, if the offer exceeds certain thresholds, then prospectus or information note requirements might apply (see also the section above on public offers).

It is interesting to note that for peer-to-peer lending, the Belgian regulatory framework currently does not explicitly authorise crowdfunding by direct lending by consumers to consumers (as individuals are not allowed to make a public call to borrow money). Nevertheless, there are platforms

on the Belgian market that facilitate peer-to-peer lending, such as Mozzeno. Such platforms have a licence as a consumer credit provider and stand between the consumer-investor and the consumer-borrower. To allow the consumers to (indirectly) invest in peer-to-peer lending, such players issue debt notes in line with the applicable prospectus/information note requirements.

2. Regulations on crypto assets: please provide a summary of the legal framework of crypto assets in your country and how crypto assets are regulated in your jurisdiction.

Existing financial legislation applicable to crypto assets

Crypto assets come in all forms, sizes and shapes. Depending on their structure, underlying rights, the way they are issued, etc, it is possible that the assets themselves and services associated with them are regulated by existing financial legislative frameworks that were already in place and that are not directly targeted at the regulation of crypto assets. For example, crypto assets may be classified as a security within the meaning of the Prospectus Regulation or as an investment instrument within the meaning of the Belgian Prospectus Act. Depending on how the asset is classified, other legislation may also apply, such as the rules established by MiFID II if the crypto assets are financial instruments.

Financial legislation directed at crypto assets

Virtual currency providers

Since 2022, certain virtual currency service providers have been subject to a regulatory regime in Belgium.

This regime was introduced by:

- the Act of 1 February 2022, amending the Belgian AML Act of 18 September 2018, that introduces provisions on the status and supervision of service providers for the exchange between virtual and fiat currencies and custodian wallet providers (the VASP Act); and
- the Royal Decree of 8 February 2022 on the regulation and supervision of virtual asset services providers, (the VASP Royal Decree).

The regulatory regime applies to providers of services for the exchange between virtual currency and fiat currency and providers of custodian wallets (VASPs).

Belgian or European Economic Area VASPs with an establishment (which may take the form of a branch or other permanent establishment) or electronic infrastructure (such as an ATM) in Belgium must register with the FSMA. These VASPs will have to meet a series of conditions, including ones relating to their professional integrity and anti-money laundering obligations.

Third-country VASPs that seek to provide virtual assets exchange services or custodian wallet services must set up a legal entity in the EEA before they can register with the FSMA. For as long

as they are not registered with the FSMA, third-country VASPs are prohibited from offering their services in Belgium.

FSMA Regulation

The FSMA requested and was granted a new power by the government to regulate advertisements for virtual currencies. To this end, the FSMA issued a regulation on the marketing of virtual currencies that entered into force on 17 May 2023.

This regulation has three main aspects:

1. the basic principle that advertisements must be accurate and not misleading;
2. advertisements must contain mandatory information that points out the main risks; and
3. mass media campaigns must be notified to the FSMA in advance.

Regulation (EU) 2023/1114 of 31 May 2023 on markets in crypto assets (MiCAR)

MiCAR, which will be directly applicable in Belgium, introduces new uniformed rules on the supervision, consumer protection and environmental safeguards of crypto assets. MiCAR will essentially cover crypto assets that are not regulated by existing EU financial services legislation, such as MiFID. Key provisions for those issuing and trading crypto assets cover transparency, disclosure, licensing and the supervision of institutions and transactions. MiCAR's provisions will only gradually apply from mid-2024.

3. Payment service providers and digital wallets: please describe how payment service providers and/or digital wallets are regulated in your country. Please mention any foreseen law or regulation in this respect.

Payment services are a regulated activity in Europe and Belgium. In Belgium, the revised Payment Services Directive (PSD2) framework was implemented by the Act of 11 March 2018 on the legal status and supervision of payment institutions and electronic money institutions, access to the business of payment service providers and to the activity of issuing electronic money, and access to payment systems (the Act of 11 March 2018) and by the Code of Economic Law (CEL). Under the applicable legal framework, payment services can only be provided by certain licensed institutions, such as licensed payment institutions. In addition, certain rules govern the relationship between the payment service provider and its customers and users (especially for consumers) and the execution of payment transactions.

To summarise, PSD2 as implemented by the Act of 11 March 2018 lists the following as regulated payment services:

1. services enabling cash to be placed on a payment account;
2. services enabling cash withdrawals from a payment account;
3. the execution of payment transactions;

4. the execution of payment transactions where the funds are covered by a credit line;
5. the issuing of payment instruments and/or acquiring of payment transactions;
6. money remittance;
7. payment initiation services; and
8. account information services.

Some service providers in the market evade the regulatory regime by structuring their operations and services in a specific way and partnering with licensed service providers. Others make use of exemptions under the law, such as the limited network exemption, whereby no licence as a payment institution is required as the relevant payment instrument meets a specific limited need and allows payment transactions for the purchase of goods or services and can only be used (1) within a limited network of merchants or (2) for a very limited number of goods or services.

4. Special support to fintechs: does your jurisdiction provide any special program supporting the fintech ecosystem, in particular fintech startups (eg regulatory sandboxes, accelerator programs). Are such programs supported by the regulator in your country?

Although some market players and authors have lobbied for it, Belgium has not yet implemented a financial regulatory sandbox. To our knowledge, there are no plans to introduce such a sandbox in the near future. Nevertheless, Belgian regulators have identified fintech as an important theme in today's financial markets and as an important focus of their supervisory activities. They acknowledge that the financial regulatory framework plays a key role in accommodating both innovation and safety within the industry.

Initiatives have been taken to make Belgium a fintech-friendly jurisdiction. Since 2016, our regulators have been working together to inform market players active in Belgium about the regulation and supervision of innovative financial services and products. In that context, they have launched a joint fintech contact point, offering fintech companies the opportunity to contact them directly for the following purposes:

- an explanation of specific supervisory rules, policies and authorisation procedures;
- assistance in navigating the supervisory landscape; and
- information on potential supervisory issues, for example when developing an innovative financial concept.

The principle of proportionality is an important principle employed by our regulators in licensing procedures, and the supervision of fintechs and startups in general. Our regulators aim to consider the nature, size and complexity of a startup's activities and related risks when assessing compliance with legal requirements.

Furthermore, an important platform promoting and supporting the Belgian fintech sector is FinTech Belgium. Apart from promoting the Belgian fintech sector in Belgium and abroad, FinTech Belgium

seeks to establish an ongoing dialogue with financial regulators, in order to take into account the fintech specificities in the regulatory environment and to improve the appreciation by the regulators of the benefits that fintechs bring to consumers.

5. Open banking: please advise whether in your jurisdiction there are regulations on open banking. If the response is no, please provide any reference to regulations that may directly or indirectly affect open banking. Please include any foreseen laws and regulations on open banking.

There is no comprehensive regulation on open banking that is specific to Belgium.

The concept of open banking, where banks and payment service providers share payment account data with other service providers to allow new and different services based on the information shared, has been one of the focus points of the recent legislation on payments at the European level.

Although open banking existed before PSD2 in Belgium, it took place in a largely unregulated environment. PSD2 gave open banking a stable regulatory framework in Belgium, by introducing payment initiation and account information services to its scope and imposing an obligation on banks to facilitate access to payment data for new service providers via a secure interface.

According to a survey conducted by the European open banking platform, Tink, Belgium's bank executives are the most positive in Europe about open banking, with over 87 per cent seeing it as a positive development.[2] Open Banking has allowed Belgian banks to develop other income streams by providing extra services such as digital partnerships with telecoms companies (see Beats, a cooperation between Belfius and Proximus).

Nevertheless, there are still some hurdles and limits to open banking in Belgium. Although PSD2 has laid the foundations for open banking, fintechs still need to obtain a licence as a payment institution with the NBB to be able to benefit from the open banking framework. Despite great efforts on the NBB's part, the licensing procedure is still often seen as a brake on the development of new services as it remains a time-consuming and complex procedure for fintechs.

It is also an issue that some banks still refuse to share their customer data with third-party providers due to an alleged lack of security.

Another downside of the current open banking framework is that some banks are still using their own nom-standardised APIs, which sometimes are not compatible with fintechs' APIs. This means that fintechs often have had to build several bank-specific APIs, which is again costly and time-consuming.

In June 2023, the European Commission introduced a new package of draft legislative text focused on further developing the payment landscape and legislation at European level. This initiative makes a number of targeted amendments to the open banking framework to improve its functioning, while avoiding radical changes that might destabilise the market or generate significant further implementation costs. Hopefully this new package, once adopted and implemented in Belgium, will bring the necessary changes to improve the Belgian regulatory and market conditions.

2 *The open banking revolution* (Tink, 2021), see https://tink.com/survey-reports/open-banking-revolution.

Denmark

Morten Nybom Bethe
Gorrissen Fiederspiel, Copenhagen
mnb@gorrissenfederspiel.com

1. Fintech regulatory framework: please provide a description of the most relevant laws and regulations on fintech and financial innovation in your country. Please also refer to any new law or regulation foreseen in the near future or any bill on fintech and financial innovation in your jurisdiction.

The regulatory landscape for financial activities in Denmark is characterised by comprehensive regulations heavily influenced by European Union standards. However, when it comes to fintech and financial innovation, Denmark lacks specific regulations explicitly governing or prohibiting such activities. Instead, the permissibility of these activities hinges on whether they fall within established regulatory frameworks governing financial businesses and services.

The Danish Financial Supervisory Authority (the FSA) has clarified that most fintech models introduced in the Danish market are covered by the existing legal framework. The primary legislative pillars include the Danish Financial Business Act, which outlines general licensing requirements for financial activities, and the Danish Capital Markets Act, which oversees securities trading and incorporates various European Directives. Additionally, the Danish Payments Act holds significant importance as it implements the Revised Payment Services Directive (PSD2) and the E-Money Directive.

Certain financial activities may necessitate obtaining a licence to operate in Denmark. This applies, in particular, to activities related to:

- accepting deposits;
- performing payment services (as defined in the Annex to the Danish Payments Act implementing Annex I of the PSD2);
- issuing electronic money;
- offering foreign exchange services;
- engaging in investment services and/or providing investment advice; and
- conducting insurance activities.

Therefore, anyone considering launching a fintech business in Denmark must conduct a thorough analysis of the relevant regulatory framework. It is crucial to ascertain whether the planned activities fall under the purview of the Danish Financial Business Act, the Danish Capital Markets Act and the Danish Payments Act, and also consider compliance with the European Prospectus Regulation as previously mentioned.

2. Regulations on crypto assets: please provide a summary of the legal framework of crypto assets in your country and how crypto assets are regulated in your jurisdiction.

Presently, crypto assets in Denmark do not fall under any dedicated legislative framework. Moreover, to the best of our understanding, the Danish Capital Markets Act does not categorise crypto assets as financial instruments.

Nevertheless, as the characteristics of crypto assets continues to evolve, their classification has grown considerably intricate. The legal classification is becoming progressively challenging, rendering it difficult to decide regarding the legal categorisation of crypto assets as financial instruments.

If a crypto asset is categorised as a financial instrument, a wide range of financial regulations – such as the Prospectus Regulation, the Markets in Financial Instruments Directive 2014 (MiFID II), the Market Abuse Regulation (MAR), and the Short Selling Regulation – may apply to crypto asset service providers. This includes entities like the issuer, cryptocurrency exchanges, trading platforms, wallet providers, and more.

While we are not aware of any proposed modifications to the present Danish laws or regulations that would significantly alter the established framework as outlined above, the European Regulation on Markets in Crypto Assets (MiCA) is poised to have a substantial impact on Denmark's existing regulatory structure. MiCA aims to establish a consistent regulatory framework for crypto service providers, including crypto custodians. As is already the case in Denmark, these custodians will become subject to a European licence and will be subject to ongoing prudential and good conduct requirements. Notably, unlike the current national regulations, this licence has the potential to be recognised and utilised in other EU Member States through a passporting mechanism similar to that in the existing financial services regime.

3. Payment service providers and digital wallets: please describe how payment service providers and/or digital wallets are regulated in your country. Please mention any foreseen law or regulation in this respect.

Payment service providers are subject to the Danish Payments Act, which is the primary legal framework governing payment services in Denmark. As mentioned in the answer given to Question 1, it implements the provisions of PSD2 and provides detailed rules and requirements for payment service providers, including licensing requirements, conduct of business rules and consumer protection measures. Similarly, digital wallet providers must adhere to the same regulations as payment service providers when offering services that fall within the scope of PSD2.

Payment service providers engaged in currency exchange between virtual and fiat currencies and those offering custodian-wallet services must adhere to the Danish Anti-Money Laundering Act, under which they must conduct customer due diligence and report suspicious transactions to relevant authorities. Further, any business intending to conduct these cryptocurrency-related activities must first register with the FSA prior to initiating operations.

4. Special support to fintechs: does your jurisdiction provide any special programme supporting the fintech ecosystem, in particular fintech startups (eg, regulatory sandboxes, accelerator programmes). Are such programmes supported by the regulator in your country?

Danish policymakers widely acknowledge the significance of fintech as a mechanism for innovation. The Danish government has articulated its commitment to enhancing the fintech sector's ecosystem and has established various initiatives, often coordinated through entities such as the Innovation Fund Denmark (www.innovationsfonden.dk) and the Danish Export and Investment Fund (www.eifo.dk).

These schemes encompass research projects and startup ventures. Additionally, Denmark has entered into global partnerships and alliances through the FSA. These partnerships serve dual objectives: supporting fintech companies engaged in cross-border operations and attracting foreign businesses and talent to the Danish fintech landscape.

Recognising the importance of regulatory clarity, the FSA has instituted a dedicated fintech team. This team works towards mitigating regulatory ambiguities and offers guidance to fintech entrepreneurs during the licensing and authorisation processes.

To enhance its understanding of fintech businesses and the regulatory challenges they face, the FSA introduced an experimental sandbox programme known as FT Lab in 2018. The primary aim of FT Lab is to provide a secure testing environment for fintech firms, enabling them to trial new technologies and business models with customers. The FSA continues to support FT Lab, collaborating with numerous fintech enterprises in the development of innovative technologies and business models over the past few years.

5. Open banking: please advise whether in your jurisdiction there are regulations on open banking. If the response is no, please provide any reference to regulations that may directly or indirectly affect open banking. Please include any foreseen laws and regulations on open banking.

As mentioned in the response given to Question 1, Denmark, like several other European countries, has adopted PSD2 in the Danish Payments Act, which encompasses open banking by establishing rules related to payment initiation and account information services.

Since payment initiation services and account information services fall under the category of payment services according to the Danish Payments Act, operators of these services are obligated to acquire a licence or, in the case of account information services, register with the FSA. Moreover, any third-party entity must secure customer consent before accessing the customer's financial data.

Under the Danish Payment Act, third-party providers are obliged to implement robust security measures for the protection of customer data, following the guidelines outlined in the Commission Delegated Regulation (EU) 2018/389. Furthermore, they must ensure compliance with data protection regulations, including the General Data Protection Regulation (GDPR).

Finland

Tarja Wist
Wist Attorneys, Helsinki
tarja.wist@wistattorneys.fi

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

The fintech industry encompasses a large variety of new financial technologies and new services based on financial technologies within the field of banking, insurance, financial, investment and payment services. According to the Helsinki Fintech Farm, Finland has more than 210 fintech companies in the fields of payments, cryptocurrencies, blockchain, insurance, security and compliance, APIs and platforms, data and analytics, customer services and acquisition, financial software, wealth management, investing, and financing. Financial software, back-end technologies, financing, and payments are some of Finland's strongest fields.

There is no single legal framework for all fintech companies in Finland, but the regulation of fintech companies depends on the field on which they operate. For example:

- Fintech companies receiving deposits, must be licensed as deposit banks (ie, credit institutions with the right to receive deposits) under the Credit Institutions Act.[1]
- Fintech companies granting loans must be licensed as credit institutions if the lending is funded by repayable funds raised from the public.
- Fintech companies granting loans from private funds or otherwise from funds other than[2] repayable funds raised from the public, do not require a licence. However, also in such cases, fintech companies providing consumer credits must be registered with the Finnish Financial Supervision Authority(the 'Fin-FSA').
- Fintech companies operating peer-to-peer lending platforms must be registered with the Fin-FSA.
- Fintech companies operating crowdfunding platforms must be licensed as crowdfunding service providers.
- Fintech companies engaged in the execution of payment transactions, issuing of electronic money (eg, prepaid cards), money remittance, payment initiation services or account information services must be licensed as payment institutions under the Payment Institutions Act.[3]
- Fintech companies engaged in any types of investment services, including securities brokerage and dealing, asset management, investment advice, underwriting and the operation of

1 *Laki luottolaitostoiminnasta* 610/2014.
2 *Laki joukkorahoituspalvelun tarjoamisesta* 203/2022.
3 *Maksulaitoslaki* 297/2010.

multilateral trading facilities or OTF venues, must be licensed as investment firms under the Investment Services Act.[4]

- Fintech companies engaged in insurance sales or brokerage must be registered with the Fin-FSA.[5]
- Fintech companies issuing virtual currencies or engaged in exchange or wallet services for virtual currencies must be registered with the Fin-FSA (see section 2 below for further discussion on crypto currencies) under the Virtual Currency Act.[6]

A fintech company licensed in another European Union or European Economic Area Member State may usually operate in Finland under the so-called passporting regime provided in the applicable EU legislation.

Fintech companies that are licensed or registered with the Fin-FSA are subject to the provisions of the Act on Preventing Money Laundering and Terrorist Financing,[7] which impose obligations such as the requirement for a risk assessment on money laundering and terrorist financing, customer due diligence and ongoing monitoring as well as reporting of suspicious transactions. Also, under the Act on Bank and Payment Account Monitoring System,[8] fintech companies qualifying as, for example, payment institutions, e-money institutions or virtual currency service providers must deposit certain customer data in a specific register and credit institutions must maintain a data system transmitting real-time data to the authorities.

The future development of the Finnish legal and regulatory framework of the fintech industry is dictated by the EU Digital Finance Package, a comprehensive EU law framework aimed at fostering of innovation and competition in the financial services while ensuring consumer protection and financial stability. Among others, the following pieces of EU legislation will take effect in the near future:

- the Markets in Crypto Assets Regulation (MiCAR)[9] entered into force in June 2023 and will take effect during 2024, in parallel with a range of technical standards. See Question 2 for further discussion on crypto assets;
- the Digital Operational Resilience Act (DORA)[10] entered into force on 16 January 2023 and will apply as of 17 January 2025. The DORA focuses on strengthening the cybersecurity of the financial industry and on harmonising the rules relating to the operational resilience for the financial sector;
- the Payment Services Directive 3 (PSD3) and the Payment Services Regulations (PSR) proposals are expected to be finalised by late 2024 with the new legislation to take effect in or around 2026.

4 *Sijoituspalvelulaki* 747/2012.

5 *Laki vakuutusten tarjoamisesta* 234/2018.

6 *Laki virtuaalivaluutan tarjoajista* 572/2019.

7 *Laki rahanpesun ja terrorismin rahoittamisen estämisestä* 444/2017.

8 *Laki pankki- ja maksutilien valvontajärjestelmästä* 571/2019.

9 Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937.

10 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

PSD3 and PSR aim to enhance the safety and security of electronic payments and transactions while providing a greater choice of payment service providers on the market; and

- the Financial Data Access Regulation (FIFA)[11] was introduced in conjunction with the proposals for PSD3 and PSR and has the primary objective of boosting digital transformation in the financial sector by speeding up the adoption of data-driven business models and the development of open finance. FIFA will establish full control for customers over their data, include an obligation for customer data holders to make data available to other data users (eg, fintech firms), and provide for the standardisation of customer data and the required technical interfaces. FIFA is expected to take effect in or around 2027.

In addition, the implementation of the proposed EU Artificial Intelligence Act[12] and related legislative initiatives are expected to have an impact on the fintech companies exploiting AI, as new requirements for so-called general purpose AI systems will be introduced. AI-based creditworthiness assessments, as well as pricing and risk assessments in life and health insurance, are considered high-risk AI use cases, and will therefore have to comply with heightened requirements for such AI applications.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

The provision of virtual currency services is regulated in Finland under the Virtual Currency Act, which was introduced in 2019 and seeks to improve the detection of suspicious transactions and activities. The Virtual Currency Act is largely based on the Fifth EU Anti-Money Laundering Directive (AMLD5),[13] but goes somewhat beyond it.

Under the Virtual Currency Act, virtual currency is defined in line with AMLD5 to mean a digital representation of value that is not issued by a central bank or a public authority and is not a legal currency, but which can be used a means of exchange and be transferred, stored and traded electronically.

Pursuant to the Virtual Currency Act, providers of virtual currency services must be registered with the Fin-FSA. Virtual currency services are defined to include:

- the issuance of virtual currencies (except for electronic money);
- the provision of virtual currency exchange services; and
- the provision of custodian wallet services for virtual currencies.

Exemptions from the registration obligation apply, however, for virtual currency services which are provided within a limited network only or which are provided occasionally in connection with other professional activities that require a licence, registration or prior authorisation.

Under the Virtual Currency Act, registration of a virtual currency service provider is subject to the following prerequisites being fulfilled:

11 Proposal for a Regulation of the European Parliament and of the Council on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554.

12 Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.

13 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

- the service provider having the right to carry out business in Finland (which for entities means that they must be established in Finland or have a registered branch in Finland);
- the service provider not being bankrupt or, if the service provider is a natural person, that they are not under custodianship; and that
- the service provider and, in the case of the entity, the directors, significant shareholders and general partners of the service provider, are considered reliable.

The Fin-FSA's Regulations and Guidelines for Virtual Currency Providers include further instructions on the holding and safeguarding of client assets (including the virtual currency), customer due diligence and risk management systems.

MiCAR and the related technical standards will, once effected, become directly applicable in Finland and replace the national legal framework.

MiCAR defines crypto assets in line with AMLD5 as 'a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology' and will apply both to the issuance of crypto assets and the services provided on the secondary market or crypto asset services, including:

- providing custody and administration of crypto assets on behalf of clients;
- operation of a trading platform for crypto assets;
- exchange of crypto assets for funds;
- exchange of crypto assets for other crypto-assets;
- execution of orders for crypto assets on behalf of clients;
- placing of crypto assets;
- reception and transmission of orders for crypto assets on behalf of clients;
- providing advice on crypto assets;
- providing portfolio management on crypto assets;
- providing transfer services for crypto assets on behalf of clients.

MiCAR will introduce an authorisation requirement for the issuers of crypto assets and crypto asset service providers, provide rules for transparency and disclosure requirements for the issuance of and trading in crypto assets, and impose requirements for the business organisation of crypto asset issuers and crypto asset service providers. MiCAR also addresses investor and consumer protection for the issuance, trading in and custody of crypto assets and provides for the prevention of market abuse on crypto currency exchanges. The authorisation requirements and provisions regarding ongoing supervision of issuers and crypto asset service providers and most of the other provisions of the MiCAR will apply from 30 December 2024, while the provisions on asset-referenced tokens and e-money tokens have applied since 30 June 2024. The implementation of MiCAR in the Finnish national legislation has not yet commenced.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

The legal framework in general

In Finland, payment services and e-money/digital wallets are regulated in the Payment Services Act,[14] which includes service-specific provisions on, for example, transparency of conditions and information requirements, the execution of transactions and liability of payment service providers, and in the Payment Institutions Act, which provides for the authorisations requirements and other institutional provisions, in accordance with the Second Payment Services Directive (PSD2).[15]

Licensing of payment services

Providers of payment services must be licensed under the Payment Institutions Act unless a specific exemption applies.

Payment services are defined in the Payment Services Act in line with PSD2 to include:

- services enabling cash to be placed on or withdrawn from a payment account as well as the operations required for operating and provision of a payment account;
- execution of payment transactions by means of account transfers, transfers of funds on a payment account, direct debit or a payment card or a similar device;
- issuing of payment instruments;
- approval and handling of a payment transaction based on an agreement with the recipient of the payment, resulting in the transmission of payment to the recipient;
- money remittance;
- payment initiation services; and
- account information services.

There are, however, many exemptions.

First, excluded services include:

- physical money transports;
- services whereby payments are made in cash directly from the payer to the payee in connection with the acquisition of goods or services;
- services based on specific payment instruments;
    - that can be used only in a limited way;

14 *Maksupalvelulaki* 290/2010.

15 Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

- that can be used for the purposes of acquiring goods or services only in the premises of the issuer or within a limited network of service providers under direct commercial agreement with the issuer;
- that can be used only to acquire a very limited range of goods or services; or
- that are valid only in a single Member State and are provided at the request of an undertaking or a public sector entity and regulated by a national or regional public authority for specific social or tax purposes to acquire specific goods or services from suppliers having a commercial agreement with the issuer.

Certain payment transactions are excluded, most notably payment transactions from the payer to the payee through a commercial agent authorised to negotiate or conclude the sale or purchase of goods or services on behalf of the payer or the payee only, and payment transactions related to securities asset servicing by licensed investment service providers or custodians as well as payment transactions within the same group of companies.

Further, under the Payment Institutions Act, payment services may be provided without a licence where:

- the monthly average of the preceding 12 months' total value of payment transactions executed does not exceed €50,000 for a natural person or €3m for a legal person; and
- the payment services are not offered in another Member State of the EEA.

Also, no licence is required for the provision of account information services only.

Payment service providers which are exempted from the licensing requirement must, nevertheless, be registered in the Payment Institutions Register maintained by the Fin-FSA.

In order to be granted a licence, a payment institution must fulfil the operational and financial requirements set out in the Payment Institutions Act, and its founders and owners must meet the prescribed requirement for reliability.

The operational requirements for payment institutions encompass, among others:

- the prudent organisation of the payment institution's activities and internal control functions;
- professional management and the requirements to establish adequate risk management systems to control the operative and security risks relating to the payment services which the payment institution provides; and
- to establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents.

A payment institution must also not have close links to natural or legal persons in jurisdictions outside of the EEA where the applicable laws, regulations or administrative provisions prevent the effective exercise of the supervision.

The minimum capital requirements for payment institutions range from €20,000 for payment institutions only providing money remittance and, respectively, €50,000 for payment institutions only providing payment initiation services, to €125,000 for payment institutions providing other

payment services. Payment institutions must, in addition, have their own sufficient funds, as further detailed by Fin-FSA.

For any owner, who, directly or indirectly, holds a qualifying holding of 10 per cent of more of the payment institution's capital or voting rights, a fit and proper test applies. Similarly, any persons intending to acquire a qualifying holding in a payment institution must notify the Fin-FSA of the intended acquisition and not complete the acquisition before the Fin-FSA has approved it or before the statutory time for approval has lapsed.

Payment institutions are subject to a set of the code of conduct rules of the Payment Institutions Act, such as the prohibition against the provision of inaccurate or misleading information or the use of otherwise inappropriate means of conduct in connection with marketing, a prohibition against unreasonable or unrelated terms and conditions, a confidentiality obligation and know-your-customer requirements. Further, an obligation to segregate customer funds applies.

The service-specific provisions of the Payment Services Act

The Payment Services Act includes the service-specific provisions and sets out, for example, the requirements for the information to be provided by the payment services provider to the payment service users, both prior to concluding a framework contract and before and after the execution of a payment transaction.

The Payment Services Act also includes detailed provisions concerning the authorisation and execution of payment transactions, including the refusal and irrevocability of payment orders, the obligation of the payment service provider to carry out the payment instructions and to provide evidence on its execution as well as the procedure for the rectification of unauthorised or incorrectly executed payment transactions. Further, the execution time and value date are regulated in the Payments Services Act, as are the time and prerequisites for a payment transaction to be considered effective in relating to the payee and the payer's creditors and other third parties.

With regard to payment instruments, the Payment Services Act provides for the payment service user's obligation to take good care of the payment instrument, sets out the procedure in the event of loss or forfeiture of the payment instrument and the right and obligation of the payment service provider to block and, thereafter unblock, the payment instrument, and regulates the fees which the payment service provider may charge for the use of the payment instrument.

Rules on the access to and use of payment account information in the case of account information services are also included in the Payment Services Act.

Finally, the Payment Services Act regulates the liability of the payment service provider and, respectively, the payment service user, and provides for the joint supervision of compliance by the Fin-FSA and the Consumer Ombudsman.

Electronic money institutions and wallets

Electronic money (e-money) is a digital alternative to cash. It allows users to make cashless payments with money stored on a card or a phone, or over the internet.

E-money is defined as a monetary value which is (1) stored electronically, including magnetically, as represented by a claim on the issuer, (2) issued on the receipt of funds for the purpose of making payment transactions and (3) accepted as payments by one or several persons.

Issuers of e-money must be licensed as electronic money institutions under the Payment Institutions Act, except where the total value of the e-money issued by the issuer does not exceed €5m.

The minimum capital requirement for an electronic money institution is €350,000, and the funds of an electronic money institution must be equal to the minimum of 2 per cent of the average amount of the e-money issued by it, calculated over the preceding six months.

Otherwise, electronic money institutions are generally subject to the same requirements as payment institutions under the Payment Institutions Act. However, ownership control is triggered only for a qualifying holding of 20 per cent.

Future developments

PSD3 is designed particularly to regulate electronic payments within the EU and to foster competition in electronic payments, and the Finnish legal framework for payment services and issuers of e-money will change accordingly when PSD3 and PSR take effect.

The implementation of PSD3 and PSR is expected to bring the following key changes:

- granting non-bank payment service providers access to all EU payment systems;
- improving the legal framework for open banking, particularly concerning the performance of data interfaces, and removing barriers to open banking services;
- new initial capital, own funds and licensing requirements for payment and e-money institutions;
- more extensive, strong customer authentication (SCA) regulations and stricter rules on access to payment systems and account information; and
- improving consumer protection.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

There are no special regulatory programmes for the fintech ecosystem or fintech startups in Finland, and no special sandboxes or accelerator programmes exist.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

Open banking was introduced in Finland in connection with the implementation of PSD2 in 2018 when the scope of application of the Payment Services Act was extended by bringing third-party providers

(TPPs) within the scope of the regulation and supervision. Pursuant to the Payment Services Act, account servicing banks must provide TPPs access to customer accounts with the explicit consent of the customer. The payment initiation service provider and the account information service provider have the right to utilise strong customer authentication procedures provided to the customer by the account servicing bank.

The legislative landscape for open banking both in Finland and across the EU will change in the coming years when PSD3 and PSR take effect. Further changes will be introduced by FIFA, which has the primary objective of boosting digital transformation in the financial sector by speeding up the adoption of data-driven business models and the development of open finance.

France

Jean-François Adelle[1]
Jeantet, Paris
jfadelle@jeantet.fr

Olivier Lyon-Lynch[2]
Jeantet, Paris
olyon-lynch@jeantet.fr

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

In France, there is no single set of regulation for fintechs. There is also no legal definition of fintechs. They are generally considered to be companies carrying innovative technologies in digital, artificial intelligence and data processing (big data) applied to the finance industry, where they play a role of accelerator of change, often disruptive.

These technologies are typically deployed in the field of payments, digital assets (cryptocurrencies, tokens, stablecoins), financing (crowdfunding platforms), management of insurance products (insurtech), assistance with risk management and compliance (regtech) and the management of financial contracts (smart contracts), where their application sometimes precedes the adaptations of the law and regulations to the new problems raised.

Fintechs and their activities will accordingly be potentially concerned by a diverse set of laws and regulations from French and EU sources, and guidelines. These essentially comprise:

- Regulation on payment services (Articles L314-1 à L314-16) and intermediaries in banking and payment services regulation (Articles L519-1 à L519-17) of the Monetary and Financial Code;
- Regulation of issue and management of electronic money (Articles L315-1 à L315-9) of the Monetary and Financial Code;
- Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020, on European crowdfunding service providers for business;
- Regulation of services providers of digital assets (Articles L54-10-1 à L54-10-5 of the Monetary and Financial Code), Decree No 2019-1213 of 21 November 2019 relating to issuers of tokens (Articles L551-1 to L552-7 of the Monetary and Financial Code) and Articles 721-1 *et seq* of the General Regulation of the Financial Markets Authority (AMF);
- Regulation on e-marketing, hawking and distance delivery of financial services (Articles L341-1 to L343-2 of the Monetary and Financial Code);

1 Co-Chair of the IBA Banking and Financial Law Committee (2023–2024).
2 Contributor to the 2024 updated edition.

- Regulation on providers of data communication services (Articles L549-1 to L54 of the Monetary and Financial Code);
- Regulation on intermediaries in miscellaneous assets (Articles L551-1 à L551-5 of the Monetary and Financial Code);
- Ordinance No 2017-1674 of 8 December 2017, on the use of a shared electronic recording device for the representation and transmission of financial securities;
- Delegated Regulation (EU) No 2018/389, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR);
- Law on monetisable digital objects and gaming companies, adopted on 10 April 2024 within the context of a law on digital space and web user protection (SREN); and
- Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (published in the Official Journal of the European Union on Friday 9 June 2023), (the MiCA regulation) which came into force on 29 June 2023. Most of its provisions will apply from 30 December 2024. From that date, a harmonised European framework will replace the existing national frameworks to govern in particular:
    - the public offering and admission to trading of tokens,
    - the provision of crypto asset services by service providers,
    - the prevention of market abuse in crypto assets.

Further regulation is being contemplated, namely:

- the Proposal for a Regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 (published in the Official Journal of the European Union on 27 December 2022, the DORA regulation came into force at the beginning of 2023 and will apply from 2025);
- the Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto assets No 2021/0241 (COD); and
- the Proposal for a Regulation of the European Parliament and of the Council on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554.

Soft law also complements the above laws and regulations. The regulators have issued the following guidelines on this subject:

- the Prudential Control and Resolution Authority (ACPR) issued sector-specific implementing principles for digital asset service providers, as of November 2022; and
- the AMF issued Q&A on the digital asset service providers regime, updated on 3 August 2023.

As regards artificial intelligence (AI), a regulation in this regard that would further complete the contemplated EU Proposal on AI is not envisaged to be put forward in France, although the regulators are carefully scrutinising the emergence of risks associated with the use of algorithms. However, the ACPR published a white paper in June 2020 titled *Governance of artificial intelligence algorithms in the financial sector*, which provides practical guidelines on algorithms' evaluation and governance requirements. It identifies interdependent criteria to be implemented in the design and development of an AI algorithm in the financial sector and makes recommendations concerning integration of AI in processes of business lines.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

France was a pioneer in establishing a legal framework for crypto assets.

The first step was Ordinance No 2016-520 of 28 April 2016, regulating certain uses of blockchain technologies – notably, a shared electronic recording device for minibond and financial securities not admitted to the operations of a central securities depository.

The Law on the Growth and Transformation of the Companies (*Loi Pacte* or Pact Law) of 22 May 2019 (codified in the Monetary and Financial Code) then provided a comprehensive regulation of crypto assets. It purported, without waiting for European regulations, to offer a regulatory framework that both protects investors and is flexible to allow for changes. The regulation addresses digital assets, digital services and digital services providers.

The Pact Law divides digital assets into two subsets – utility tokens and virtual currency.

Utility tokens

This means any digital assets representing one or more rights that can be issued, recorded, stored or transferred by means of a distributed ledger technology enabling the owner of the asset to be identified, directly or indirectly, excluding those meeting the characteristics of a financial instruments and the saving bonds.

Therefore, the assets covered by this definition must be usable for non-financial purposes. In other words, the token 'must be able to be used to access goods or services. They give their holder a privileged right of digital access to the services or products offered by the issuer'. The parliamentary work that preceded the adoption of the Pact Law indicated that the token must grant 'a right of use to its holder enabling him to use the technology or services offered'.

It also means that 'security tokens', understood as a token that may represent financial securities, are excluded from the French Digital Asset regulations and are therefore subject to financial instruments regulations.

Virtual currency

This means any digital representation of value that is not issued or guaranteed by a central bank/public authority, that is not necessarily attached to legal tender and that does not have the legal status of 'money', but that is accepted by natural or legal persons as a means of exchange and that can be transferred, stored or traded electronically.

Non-fungible tokens (NFT) are not defined in French law. According to the AMF, a case-by-case approach shall be adopted in order to determine whether or not the NFT constitutes a digital asset within the meaning of Pact Law.

Pact Law also provides a specific regime for public offerings of tokens (initial coin offering or ICO) which may be defined as a fundraising operation carried out through a shared electronic recording device (DEEP or blockchain) that results in the issuance of tokens that can then be used to obtain products or services. This regime, which is designed to encourage the development of ICOs, does not apply to the issue of security tokens, but only to the issue of utility tokens. Issuers may apply for an optional visa from the AMF, which is a label of the seriousness and quality of the offer, or, subject to a warning before the realisation of the ICO indicating that the operation presents financial risks. The AMF publishes the list of ICOs that have received its visa.

The Pact Law has set up a specific regime for certain services related to investing in crypto assets and set forth a regulation applying to financial intermediaries providing those services named digital asset service providers (DASP). Such services include:

- the custody of crypto assets or access to crypto assets (via private encryption keys, for example);
- the purchase/sale of crypto assets against currencies being legal tenders (euros, US dollars, etc);
- the exchange of crypto assets for other crypto assets;
- the operation of crypto asset trading platforms;
- the reception and transmission of orders on crypto assets;
- portfolio management of crypto assets;
- advising investors in crypto assets;
- the underwriting of crypto assets; and
- the guaranteed placement and the unsecured placement of crypto assets.

A DASP must be registered with the AMF to be able to offer the following four services:

- custody of crypto assets or access to crypto assets;
- purchase/sale of crypto assets against legal tender currencies;
- exchange of crypto assets for other crypto assets; and
- operation of a crypto asset trading platform.

Registration is required for service providers that are established in France or provide services to (or even target) customers in France. Registration is based solely on the relevance of the mechanisms for combatting money laundering and the financing of terrorism, as well as on the quality and good repute of the managers. Unregistered DASPs risk being publicly blacklisted by the AMF.

DASPs wishing to market one of these nine types of services can also apply for a license from the AMF. This licence is optional. It entails more stringent obligations. Only DASPs licensed by the AMF have the right to solicit new customers in France. CFDs on crypto assets may only be marketed by a service provider licensed as an investment services provider.

Since 1 January 2024, enhanced registration is fully in force, with stricter requirements for new players wishing to provide the four digital asset services subject to compulsory registration (Law no 2023-171 of 9 March 2023 containing various provisions for adapting to EU law in the fields of the economy, health, labour, transport and agriculture (DDADUE), Article 8).

The new, enhanced registration procedure came into effect pending the introduction of European CASP (crypto assets service provider) authorisation under the MiCA (Markets in Crypto-Assets) Regulation on 30 December 2024.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

The French regulation of payment service providers and wallets is derived from EU Directives 2007/64/EC and 2015/2366 on payment services.

Payment services are essentially:

- the execution of fund transfers and direct debits;
- the transmission of funds;
- services enabling the payment or withdrawal of cash; and
- the transmission of a payment account, the execution of transactions for which the payer uses a telecommunications, digital or computerised device.

Payment services are regulated.

Payment services are a subset of banking operations, which can still be provided by credit institutions, but which are open to a new category of regulated providers – 'payment institutions'. Payment institutions may also provide related services, including granting of loans under certain conditions. Payment services can also be provided by electronic money providers.

Payment institutions must be licensed by the ACPR. However, only registration as an account information service provider is required if the only payment service provided is the account information service. Furthermore, simplified payment institution licence is available for payment institutions whose payment volume is not expected to exceed a monthly average of €3m and which do not plan to provide the money transmission service.

There is an exemption from the licensing requirement for undertakings which provide 'payment services based on means of payment which are accepted for the acquisition of goods or services only on the premises of that undertaking or, under a commercial agreement with it, in a limited network of persons accepting those means of payment or for a limited range of goods or services'.

Examples include gift cards issued by commercial networks which are only accepted for payment in the stores of that network, or other types of payment cards (eg, public transport cards). The exemption is granted by the ACPR, which verifies that the conditions are met, and the arrangements ensure the security of the means of payments and consumer protection.

The service provider may start operating before filing for an exemption until the total value of executed payment transactions or electronic money outstanding within the previous 12 months exceeds €1m.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

The French fintech sector is experiencing rapid growth. It brings together approximately 950 companies totalling 50,000 jobs in October 2023.

The French regulators are particularly aware of challenges related to the rapid evolution of the financial sector, especially regarding the fintech ecosystem. The AMF, the ACPR and Banque de France have created special fintech development units with high-level experts to attend and support the development of fintechs; they have put forward a common cell, the 'Fintech Pole' (*Pôle Fintech*). The ACPR runs the FinTech Forum alongside the AMF, which brings together professionals several times a year to discuss regulatory and supervisory issues related to fintech and innovation, analyses more cross-sectoral innovations and monitors the digitalisation of French financial companies.

To closely monitor the efficacy of the legal framework for fintechs, French authorities have set up a ministerial delegation and a commission on finance, general economy and budgetary control.

On the regulatory side, to provide an adequate regulation facilitating the development of fintechs while protecting the fintech development, France has elected a 'proportionality of regulation system', offering a panel of regulated regimes adapted to the needs of fintechs ranging from licences to registrations, and including an optional visa.

In areas of joint authority of the regulators such as licensing DASPs (the mandatory registration of DASPs is carried out by the AMF, subject to the assent of the ACPR), to ensure swift and smooth review applications, the ACPR's and the AMF's departments exchange views on all aspects of an application and appoint a team of analysts from both authorities for each application.

To facilitate the fintech licensing process, the ACPR has issued a charter targeting fintechs with startup projects. It aims to present an overview of the main authorisation procedures for fintechs under the supervision of the ACPR, and provide greater visibility regarding processing time and exchanges of information. A toolkit of useful documents providing assistance in filling in the applications is available on the ACPR's website.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

There is no single regulation on open banking. However, the practice of banks sharing data on their customers with other services providers falls under several existing regulations that affect open banking.

The second Payment Services Directive (PSD2), replacing and superseding the first PSD Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market, requires banking institutions to open their information systems to third parties and created the status of agent of payment institutions (PIs) and of electronic money institutions (EMIs). It further strengthens payment security in the era of electronic payment, and provided the framework for two new payment services related to 'open banking':

- account information service providers (AISPs), who can only provide the service of collecting information on one or more payment accounts (eg, aggregating payment accounts to analyse a company's cash flow or allowing consumers to view their various bank accounts on a single platform); and
- payment initiation service providers (*prestataires de services d'initiation de paiement* – PISPs), who initiate a payment order for an account held with another provider at the user's request.

In their development of application programming interfaces (APIs), platforms must comply with the regulatory technical standards (RTS) adopted in March 2018 by Delegated Regulation (EU) No 2018/389, which are directly applicable in domestic law.

Open banking is also subject to regulations on data protection (RDPR).

In a press release dated 15 March 2022, the ACPR commented that the emergence of agents licensed by authorised PIs or EMIs that market or develop new services has led to two changes in distribution: (1) the establishment of large-scale physical retail networks alongside banking agencies (offices, booksellers, lottery agencies), which are in charge of the customer relationship, while the PI or EMI performs the service; and (2) an increasing 'platform' of the sector, with innovative players having the status of agents developing their own service offering under the supervision of the entities that mandate them.

Going further, open banking fosters specific risks (cybersecurity, consumer data protection, etc.) that are not yet adequately addressed by existing regulation. In its press release, the ACPR recalls that authorised institutions remain fully responsible for their external providers, including agents, and must have systems in place that ensure ongoing supervision and oversight.

The upcoming EU Digital Operational Resilience Regulation (DORA) will address some of these risks, under new obligations applicable to financial entities dealing with cloud service providers and new rules regarding their supervision. DORA will set conditions related to the geographical link of cloud service providers to the territory of the EU, and a prohibition on financial entities using cloud service providers that are not established in the EU. It will also strengthen the contractual obligations of cloud service providers. Published in the Official Journal of the European Union on 27 December 2022, the DORA regulation came into force at the beginning of 2023 and will apply from 2025.

Other risks will need to be considered in the forthcoming review of PSD2.

A concern has been recently expressed on the French market on the potential adverse effects of the oligopolistic structure of the cloud market, combined with the technological dependency of banks on the expertise of cloud service providers, which led to their deep interconnection with the entire financial system. Indeed, this is likely to reverse the traditional balance of power between customers and service providers.

Cloud service providers are not subject to the rules imposed on the banking sector, especially regarding the protection of sensitive information and personal data. They are a small number of companies, mainly American and Asian, to whom the regulations of the banking profession do not apply. This introduces a certain disequilibrium in the contractual relationship, but the lack of conformity of certain clauses in the outsourcing contracts exposes banks to risks of administrative sanctions and liability issues, particularly with respect to their clients.

A new legal framework is under discussion which aims at extending the open banking, introduced by PSD2, to open finance.

If open banking has enabled the development of new value-added services based on payment data, such as real-time credit risk analysis, streamlining of the identification process when entering into a relationship with third party providers, payment initiation, and aggregation of payment accounts, this new set of forthcoming regulations is now planning to go further, and is raising the issue of opening up all financial data (such as savings, insurance, investments, etc) which would enable a multiplication of value-added services.

To this end, the European Commission has proposed, in June 2023, to:

- amend and modernise the current PSD2, which will become PSD3;
- establish a Payment Services Regulation (PSR); and
- adopt a new directive for a framework for financial data access.

At this stage, the timetable for the implementation of this new legal framework remains highly uncertain.

Germany

Christian Schmies[1]
Hengeler Mueller, Frankfurt
christian.schmies@hengeler.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

There is no specific legal framework for fintech business in Germany. Rather, depending on the services offered, they may qualify as a regulated activity under general German financial regulatory laws. The German Banking Act (*Kreditwesengesetz* or KWG) and the German Investment Institution Act (*Wertpapierinstitutsgesetz* or WpIG) provide for licensing requirements for banking and investment services, and the catalogue of regulated activities in some respects goes beyond the underlying European Directives.

For example, in Germany, any form of lending on a commercial basis, including loans to corporates, is subject to a licensing requirement, as is leasing and factoring business. Payment services are subject to a licensing requirement under the German Payment Services Supervisory Act (*Zahlungsdiensteaufsichtsgesetz* or ZAG) and the management of investment funds is regulated under the German Capital Investment Code (*Kapitalanlagegesetzbuch* or KAGB).

Given the comprehensive and still expanding nature of financial regulation, careful analysis of applicable regulatory regimes is indispensable prior to starting any fintech business in Germany.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

Since 1 January 2020, German law expressly provides that crypto assets, including cryptocurrencies, qualify as financial instruments under the KWG and the WpIG. Entities providing financial or investment services, such as investment advice, principal brokerage business, dealing on own account for others or portfolio management with respect to crypto assets, therefore require a licence as a financial services institution or as an investment institution.

Entities engaging in cryptocustody business (*Kryptoverwahrgeschäft*), eg, by providing certain wallet services, also require a licence as a financial services institution under the KWG. Licensed entities are subject to ongoing prudential requirements, including own funds and business organisation requirements, and supervision by German financial regulators BaFin and Deutsche Bundesbank.

Crypto assets in the meaning of the KWG/WpIG are defined as digital representations of assets which:

1 Christian is a partner in the Frankfurt office of Hengeler Mueller, focusing on banking and financial regulatory matters. He advises credit institutions, investment companies and other financial market participants as well as non-financial enterprises. A particular focus of his work is advising companies on payment services as well as giving advice on innovative technologies in the financial sector (fintech), in particular in payment services and asset management.

- are neither issued nor guaranteed by any central bank or public entity;
- do not have the statutory status of a currency or money; but
- based on agreements or actual practice, are accepted by natural or legal persons as a means of exchange or payment or serve investment purposes; and
- can be transferred, stored or traded electronically.

This definition encompasses security tokens and payment tokens but typically not utility tokens. Offering wallet services for crypto assets will typically qualify as cryptocustody business (*Kryptoverwahrgeschäft*) and therefore require a licence as a financial services institution under the KWG, if provided commercially or on a scale that requires a commercially organised business undertaking. Cryptocustody business is defined as the safekeeping of crypto assets, the administration and safeguarding of crypto assets or private keys which serve to hold, store or transfer crypto assets for others, and the safeguarding of private keys, which serve to hold, store or transfer crypto securities within the meaning of the German Electronic Securities Act (*Gesetz über elektronische Wertpapiere* or eWPG). In addition, operators of cryptocustody businesses are subject to ongoing regulatory requirements, including minimum capital requirements, the need to establish a proper business organisation and governance (eg, suitability of managing directors, establishment of internal control functions, etc) and certain disclosure requirements.

Moreover, both payment services providers and cryptocustodians are subject to AML regulations under the German Money Laundering Act (*Geldwäschegesetz* or GwG). As such, they are obliged to establish effective risk management, including the performance of a risk analysis and the establishment of internal security measures, which, among others, requires the appointment of a money laundering reporting officer (MLRO). Furthermore, obliged entities must perform KYC checks, engage in proper transaction monitoring and file suspicious activity reports with the German Financial Intelligence Unit.

Whereas the requirements described in the preceding paragraph implement the Directive (EU) 2015/849 (the Anti-Money Laundering Directive or AMLD) and closely mirror the European template, German lawmakers on a national level had implemented in the German crypto asset transfer regulation the travel rule as proposed by the Financial Action Task Force (FATF) on 21 June 2019.

The travel rule is essentially a regulatory instrument to track the flow of crypto assets requiring operators of crypto services involved in the transfer of crypto assets, such as cryptocustodians, to exchange (personal) information with other operators of such crypto services. With the amendment of the European Money Transfer Regulation and the inclusion of crypto transfers therein, the national regulation ceases to apply.

Particularly since the introduction of licensing requirements for cryptocustody business, crypto service providers have gained increased regulatory attention. Over time, BaFin has increased resources and developed a good understanding of the crypto market, its major players and business models. In terms of priorities, it seems that BaFin has taken a particularly close look at the AML compliance of crypto service providers.

While there are no proposed amendments to the current laws or regulations by German lawmakers that would materially impact the existing regime as described above, the European Regulation on Markets in Crypto-Assets (MiCA) substantially affects the current regulatory regime in Germany. As MiCA provides for a uniform regulatory regime of operators of crypto services, it also targets, among others, cryptocustodians which, as is already the case today in Germany, become subject to an EU-wide licence and ongoing prudential and good conduct requirements. In contrast to today's national regulation, this licence can then be passported to other Member States.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

Payment services require a licence under the ZAG. The ZAG sets out an exhaustive list of regulated payment services, all related to money in cash, bank accounts or e-money. For such business activities, ZAG sets out certain requirements, inter alia, as to the qualification of management, capital requirements and risk management.

Additionally, in the administrative practice a number of minimum requirements regarding IT security and IT risk management of payment service providers have been established (BaFin circular on Payment Services Supervisory Requirements for the IT of Payment and E-Money Institutions (*Zahlungsdienstaufsichtliche Anforderungen an die IT von Zahlungs- und E-Geld-Instituten* or ZAIT)). Germany has not made use of the option of Article 32 of the second EU Payment Services Directive (PSD2) to introduce a simplified form of PSP.

In principle, the general licensing requirements for all types of payment services providers are the same, with the exception that companies providing exclusively account information services do not require a licence but a mere registration with BaFin. By the end of 2022, there were 81 companies domiciled in Germany with a licence for payment services or e-money business. Credit institutions, ie, banks, are still major players in the market for payment services in Germany, which may account for the relatively small number of companies licensed under the regime for payment service providers.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

There are no special programmes supporting fintech and fintech startups. Neither German legislators nor the German regulators have created a special sandboxing regime for fintechs and rather follow the approach 'same business, same risks, same regulation'.

However, financial regulators and policymakers are generally receptive to fintech innovation and technology-driven new entrants to the financial services markets. This has manifested itself in various ways. In 2017, the German Ministry of Finance established the German FinTech Council, which advises the Ministry on fintech matters. Moreover, the Ministry of Finance documents its interest in fintech, among others, by organising events. BaFin has also significantly intensified its fintech-related

activities recently and, among others, provides dedicated information for various fintech business types on its website.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

The term 'open banking' generally refers to the opening of payment accounts for data-based payment services of third-party service providers. The ZAG implements PSD2, which, among others, addresses open banking by establishing rules referring to payment initiation and account information services.

As payment initiation services (*Zahlungsauslösedienste*) and account information services (*Kontoinformationsdienste*) qualify as payment services under the ZAG, any operator of these services is required to obtain a licence or, in case of account information services, registration.

Moreover, under the ZAG and the specifying Commission Delegated Regulation (EU) 2018/389, providers of payment initiation and account information services are obliged, inter alia, to meet a high standard of customer data protection and to ensure secure communication via appropriate interfaces.

Greece

Dimitris E Paraskevas
Paraskevas, London
dparaskevas@paraskevaslaw.com

1. Fintech regulatory framework: please provide a description of the most relevant laws and regulations on fintech and financial innovation in your country. Please also refer to any new law or regulation foreseen in the near future or any bill on fintech and financial innovation in your jurisdiction.

The fintech landscape is evolving rapidly and the Greek legal framework shows a gradual alignment with international standards and practices. The European Union, of which Greece is a member, is actively working to create a harmonised regulatory environment for fintech companies. This includes directives such as the second Payment Services Directive (PSD2), which has had a significant impact on open banking and fintech innovation across Europe.

In Greece, the regulatory approach for digital wallets, payment services and crypto assets, for example, has been cautious but forward-looking. The Greek government and financial regulators are working to create an enabling environment for fintech growth, while ensuring strong risk management and consumer protection measures.

Upcoming legislation and expected changes in the fintech sector in Greece are likely to focus on enhancing digital innovation, improving cybersecurity, and integrating new technologies such as blockchain and artificial intelligence into financial services. These changes are expected to align with broader trends observed in the global fintech landscape, where there is an increasing emphasis on leveraging technology for financial inclusion and efficiency.

The fintech landscape in Greece is poised for significant growth, driven by technological innovation and a supportive regulatory environment. As fintech continues to evolve, the regulatory framework in Greece will need to be continuously adapted to ensure that it remains relevant, effective and conducive to innovation. Upcoming changes in legislation and regulation are expected to further strengthen the fintech ecosystem in Greece, positioning it as a key player in the European financial technology landscape.

2. Regulations on crypto assets: please provide a summary of the legal framework of crypto assets in your country and how crypto assets are regulated in your jurisdiction

In Greece, as in many countries, the legal definition and status of crypto assets is still evolving. In the country, crypto assets are mainly seen as a digital representation of value that can be traded digitally and functions as a medium of exchange, unit of account or store of value.

Regulatory guidelines and supervision by competent Greek authorities

Regulatory oversight of crypto assets in Greece involves various authorities, including the Bank of Greece and the Hellenic Capital Market Commission. These bodies monitor and regulate the use of crypto assets, particularly with regard to anti-money laundering (AML) and combatting the financing of terrorism (CFT). The approach taken by the Greek authorities is aligned with international standards set by bodies such as the Financial Action Task Force (FATF) and the EU's anti-money laundering guidelines.

The Greek legal framework for crypto assets is also influenced by EU regulations. For example, the Fifth Anti-Money Laundering Directive (AMLD5), which Greece has transposed into national law, includes provisions on crypto assets. It mandates that platforms and wallet providers engaged in exchange services between cryptocurrencies and fiat currencies, as well as custodian wallet providers, are subject to AML and CFT regulations.

The Greek government is working to incorporate crypto assets into its tax framework. Capital gains from the sale of cryptocurrencies are subject to tax. However, the implementation of these taxes can be complex, given the volatility and unique nature of these assets. As part of the wider EU, Greece is also affected by EU efforts to create a more harmonised tax approach towards crypto assets.

The evolution of regulatory frameworks in Greece is also driven by the recognition of the potential benefits of blockchain technology, which underpins many crypto assets. Greek authorities, in line with global trends, are exploring how blockchain can be used to improve financial services, improve transparency and reduce fraud.

The regulatory landscape for crypto assets in Greece is in a state of development, reflecting broader global trends in fintech regulation. The Greek government and regulators are working to create a framework that balances the need for innovation with the imperatives of investor protection and financial stability. As the market for crypto assets continues to evolve, it is expected that Greek regulations will also adapt, providing clearer guidance and strong frameworks for the operation and use of these digital assets.

3. Special support to fintechs: does your jurisdiction provide any special programme supporting fintech ecosystems, in particular fintech startups (eg, regulatory sandboxes, accelerator programmes). Are such programmes supported by the regulator in your country?

One of the main ways to support fintechs is through legislative and regulatory frameworks that encourage fintech innovation while ensuring consumer protection and financial stability. The implementation of EU directives such as PSD2, has been an important step in this direction, providing a regulatory environment conducive to the development of digital banking and payment services. In addition, the Greek government is working to incorporate EU guidelines on crowdfunding and alternative financing models, which are crucial for startups and small businesses in the fintech sector.

Regulatory sandboxes are a remarkable initiative that has gained traction globally and are being considered in Greece. These sandboxes allow fintech startups to test and develop their innovations in a controlled environment with regulatory oversight, thereby reducing barriers to entry and fostering innovation. While Greece is still in the early stages of implementing a full regulatory sandbox, the concept is gaining attention among policymakers as a tool to promote fintech innovation.

In addition to potential regulatory sandboxes, Greece has seen the emergence of accelerator programmes and incubators focused on fintech. These programmes, often in collaboration with private sector partners, provide startups with mentoring, funding opportunities and networking platforms to connect with investors and industry experts. Such initiatives are vital for early-stage financial technology companies that need support to navigate the complex financial and technological landscape.

The sandboxes allow fintech startups to test new products and services in a controlled environment, providing valuable insights for both innovators and regulators. This approach reflects a global trend where regulators are increasingly adopting flexible and adaptive regulatory mechanisms to keep pace with the rapid evolution of financial technologies.

Evaluating the effectiveness and impact of support programmes

The effectiveness and impact of government and regulatory support programmes for fintech in Greece can be assessed on several fronts. First, the adoption of EU regulatory frameworks has provided a solid foundation for fintech operations, ensuring compliance with international standards and enhancing consumer confidence. This alignment with EU regulations has enhanced Greece's attractiveness as a fintech hub in the region.

Second, acceleration programmes and potential regulatory sandboxes represent important steps towards creating an enabling environment for fintech innovation. These initiatives provide startups with the necessary resources and guidance to develop and scale their solutions, contributing to the overall growth of the fintech industry in Greece. However, the impact of these programmes also depends on broader economic and political factors in Greece. The success of fintech support initiatives is intertwined with the country's economic stability and investment climate. Therefore, continued efforts to strengthen the economy and create an enabling business environment are an integral part of the long-term success of the fintech ecosystem in Greece.

4. Regulation of payment service providers and digital wallets

Applicable laws and regulations for payment service providers in Greece

In Greece, the regulation of payment service providers (PSPs) is mainly influenced by EU directives, in particular PSD2, which Greece has transposed into national law. PSD2 has significantly reshaped the payments industry across Europe, including Greece, by promoting competition, enhancing consumer protection and boosting innovation in the payments sector. The Directive requires PSPs to adhere to strict operational and security standards, ensuring the safety and integrity of payment transactions.

The Bank of Greece plays a central role in the regulation and supervision of PSPs. It ensures compliance with relevant EU directives and national legislation by overseeing the operations of various payment institutions. This includes monitoring their compliance with AML and CFT regulations, as outlined in the EU's Anti-Avenue Directives, which are vital to maintaining the integrity of financial transactions.

Specific requirements and oversight for digital wallet services

Digital wallet services in Greece must comply with specific regulatory requirements, particularly with regard to customer data protection, transaction security and operational resilience. Under PSD2, digital wallet providers are required to implement strong customer authentication (SCA) measures to improve transaction security. This aligns with the EU's broader agenda for securing digital payments, which includes ensuring data privacy under the General Data Protection Regulation (GDPR).

In addition, it requires digital wallet providers to have robust risk management processes and contingency plans in place to address operational and security risks. Providers are also required to maintain transparent and fair business practices, including clear communication with customers regarding fees, terms and conditions of service.

Future regulatory trends and possible changes

Looking ahead, the regulatory landscape for PSPs and digital wallet services in Greece is expected to evolve in response to emerging trends and challenges in the fintech sector. One potential area of growth is the regulation of new payment technologies and platforms, including blockchain and cryptocurrencies. As these technologies become more integrated into the mainstream financial system, Greek regulators may develop specific guidelines and standards to govern their use in payment services.

Another trend that may influence future regulations is the increasing focus on cybersecurity and data protection. With the increasing frequency of cyber attacks and data breaches, Greek authorities are expected to strengthen regulations on data security and privacy, requiring PSPs and digital wallet providers to adopt more advanced security measures. In addition, the concept of open banking, promoted by PSD2, is likely to continue to shape the regulatory framework for digital payments in the country. Open banking promotes a more integrated and competitive financial services environment, which may lead to the introduction of new regulations governing data sharing and interoperability between banks and financial technology companies.

The regulation of PSPs and digital wallets in Greece is a dynamic field, closely aligned with EU directives and influenced by global fintech trends. As the digital payments landscape continues to evolve, driven by technological developments and changing consumer behaviours, Greek regulators are expected to update and improve the regulatory framework to ensure a secure, efficient and innovative payments ecosystem.

5. Open banking in Greece

Regulations and guidelines for open banking in Greece

In Greece, the primary regulatory framework governing open banking comes from PSD2. The Directive, which Greece has transposed into national law, obliges banks to provide third party providers (TPPs) with access to their customers' accounts and data, with the customer's consent. This access is mainly facilitated through secure APIs, enabling the development of new financial services and enhancing competition in the financial sector.

The Bank of Greece and the Hellenic Capital Market Commission oversee the implementation of these regulations. They ensure that banks and TPPs comply with PSD2 requirements, in particular regarding customer data protection, transaction security and the reliability of services provided. In addition, these principles require compliance with the General Data Protection Regulation (GDPR) to ensure the privacy of consumer data within the open banking framework.

Future perspectives and possible legislative developments in open banking

The future of open banking in Greece looks promising, with potential for further integration and innovation in the financial services sector. The current framework, based on PSD2, sets the stage for a more competitive and diverse banking ecosystem, enabling fintech startups and traditional financial institutions to develop new, customer-centric services.

Future legislative developments in Greece are likely to focus on enhancing the security and efficiency of data sharing. This could include standardisation of APIs and the development of more robust data protection and fraud prevention protocols, aligned with broader EU initiatives.

In addition, there is scope for legislative evolution towards a more comprehensive digital finance strategy, which would include not only open banking but also other aspects of digital finance, such as digital currencies, blockchain technology and digital identity systems. Such developments could position Greece as a leader in digital finance in the European context.

Moreover, as open banking matures, Greek regulators may explore more advanced regulatory technologies (RegTech) to effectively oversee the open banking ecosystem. This could include the use of artificial intelligence and machine learning for monitoring and compliance purposes, ensuring that the open banking infrastructure operates safely and efficiently.

Open banking in Greece, shaped by EU directives and national initiatives, is poised for growth and innovation. The Greek approach, while similar to other European models, has its unique aspects and challenges. Future legislative developments are expected to further improve and strengthen the open banking framework, leading to the creation of innovative financial services and strengthening a more dynamic banking sector in Greece.

Ireland

Josh Hogan[1]
McCann FitzGerald, Dublin
Josh.Hogan@mccannfitzgerald.com

John Boyle[2]
McCann FitzGerald, Dublin
John.Boyle@mccannfitzgerald.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

Ireland does not have a regulatory regime that is specific to fintech or fintech companies. In all cases, it is necessary to look to the underlying service provided to determine whether it is subject to Irish financial services regulation.

The main Irish legislation that may typically apply to the activities of fintech companies includes:

- the European Union (Markets in Financial Instruments) Regulations 2017, which implement Directive 2014/65/EU (MiFID II) in Ireland;
- the European Union (Payment Services) Regulations 2018 (the Irish Payment Services Regulations), which transpose the EU's revised Payment Services Directive 2015/2366 (PSD2) into Irish law; and
- the European Communities (Electronic Money) Regulations 2011 (the Irish E-Money Regulations), which transpose the EU's Electronic Money Directive 2009/110 (EMD2) into Irish law.

In addition, investment and lending activities of fintech companies may fall within scope of Irish domestic legislative regimes, including the Investment Intermediaries Act 1995, the Central Bank Act 1997 and the Consumer Credit Act 1995, which set out regulatory regimes for investment business firms, retail credit firms, credit servicing firms and high-cost credit providers.

The above enactments prescribe certain activities as regulated activities, meaning an entity must be appropriately authorised to conduct such activities in Ireland. Typically, this means that an entity must hold an authorisation from the Central Bank of Ireland (the Central Bank) or, where the activity is subject to EU passporting rights, from another EU regulator. In all cases, there may be possible exemptions or exclusions available, or methods of structuring activities to ensure they do not fall within scope of regulated activity.

In recent years, further regulatory regimes that may govern the activities of fintech companies have been introduced. In 2021, amendments to Ireland's anti-money laundering (AML) framework (under the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010), introduced a

1 Josh Hogan is a partner at McCann FitzGerald, specialising in financial services regulation and fintech. He is an officer of the Banking Law Committee of the International Bar Association. Josh is a member of the governing council of the Fintech & Payments Association of Ireland and co-chairs its regulatory working group.

2 John Boyle is an associate at McCann FitzGerald and works with Josh Hogan on financial services regulatory and fintech matters.

regulatory regime for virtual asset service providers (VASPs) (discussed in Question 2). Also in 2021, the European Union (Crowdfunding) Regulations 2021 (the Irish Crowdfunding Regulations) were transposed into Irish law, which give effect to the EU's Crowdfunding Regulation, and introduce a regulatory regime for crowdfunding service providers.

The Central Bank is the entity with principal responsibility for Irish financial services regulation in Ireland (including fintechs). The Central Bank has a significant role in the conduct of business of regulated entities and has issued a number of codes and regulations including the Consumer Protection Code 2012, the Central Bank (Supervision and Enforcement) Act 2013 (Section 48) (Lending to Small and Medium-Sized Enterprises) Regulations 2015 (commonly known as the SME Lending Regulations), and the Minimum Competency Code 2017. The Central Bank also has significant enforcement powers, both in relation to the prosecution of financial crime, and under its administrative sanctions procedure (permitting it to carry out investigations and inquiries, and impose sanctions if it determines that firms or individuals have committed a prescribed contravention).

The Central Bank has repeatedly emphasised its commitment to being open and engaged with respect to fintech, and this is demonstrated through engagement with industry. The enhancements to the Central Bank's Innovation Hub, carried out in April 2024 and expected to continue throughout the year, along with the intended establishment of the Central Bank Innovation Sandbox Programme expected to commence in Q4 2024, reinforce this commitment. Tangibly, the Central Bank's process for registering virtual asset service providers is now well established and the Central Bank recently took the important step of permitting a type of regulated fund under Irish law (a qualifying investor alternative investment fund or QIAIF) to hold exposures to crypto of up to 20 per cent for open-ended funds and up to 50 per cent for close-ended funds.

Payment services

In general, fintech companies which provide payment services such as the execution of payment transactions, issuance of payment instruments, acquiring of payment transactions, money remittance, payment initiation services and account information services will fall within the regulatory regime set out in the Irish Payment Services Regulations, and will require authorisation to provide such services unless an exemption is available.

In relation to open banking, under the Irish Payment Services Regulations, payment service providers are required to permit third parties, who are authorised under those regulations, to access relevant account information. There are specific rules governing this activity set out in those regulations.

Lending

Under the Central Bank Act 1997, a person who meets the definition of a retail credit firm, or who performs the regulated activity of 'credit servicing', may be required to obtain authorisation from the Central Bank. Similarly, under the Consumer Credit Act 1995, a person who meets the definition of a high-cost credit provider (typically lending at an interest rate of 23 per cent or more), may be required to obtain authorisation from the Central Bank.

However, there may be reasons as to why these particular regimes would not apply in the context of the proposed activity of borrowing/lending (for example, if the lending is to a professional client for MiFID II purposes, or to a regulated financial service provider), and lending activities could be structured, if possible, so as not to fall within these regimes.

Buy now, pay later

The Consumer Protection (Regulation of Retail Credit and Credit Servicing Firms) Act 2022 was commenced in May 2022, giving effect to one of the most significant expansions to Irish financial services authorisation requirements for many years. Authorisation from the Central Bank is now required in relation to a broader scope of 'credit' (which no longer only applies to cash loans, and which following enactment includes deferred payments and other similar financial accommodation). This broader definition of credit is intended to bring buy now, pay later providers within scope of the regulatory regime governing retail credit firms.

Deposit taking

Deposit taking is only permitted by entities which have been authorised as a credit institution by the Central Bank, and which are therefore subject to the full extent of banking regulation.

Crypto assets

See Question 2.

Crowdfunding

Pursuant to the Irish Crowdfunding Regulations, the Central Bank has been designated the national competent authority for crowdfunding regulation in Ireland and is responsible for the authorisation and supervision of crowdfunding service providers (CSPs). CSPs that facilitate either peer-to-peer business lending or investment-based crowdfunding via its platforms need to be authorised by the Central Bank. Once authorised, they will be able to provide crowdfunding services across the EU on a cross-border basis in line with the requirements outlined in the EU's Crowdfunding Regulation.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

Ireland has chosen to follow EU developments relating to crypto rather than create a standalone domestic regulatory regime. Depending on the nature of the activities relating to crypto assets, such activities could fall within scope of: (1) Ireland's anti-money laundering framework, the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (the CJA 2010), and (2) existing Irish financial services regulatory regimes (as set out in Question 1 above), and (3) the EU's Regulation on markets in crypto assets (MiCA).

CJA 2010

CJA 2010 transposes the EU's Fifth Anti-Money Laundering Directive 2018/843 (MLD5) into Irish law, though the amendments, introduced under the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2021, go further than required by MLD5, to also take on board additional Financial Action Task Force recommendations relating to crypto.

The amendments apply broadly to virtual asset service providers (VASPs), a term which means a person who by way of business carries out one or more of the following activities for, or on behalf of, another person:

1. exchange between virtual assets and fiat currencies;
2. exchange between one or more forms of virtual assets;
3. transfer of virtual assets, that is to say, conduct a transaction on behalf of another person that moves a virtual asset from one virtual asset address or account to another;
4. custodian wallet provider;
5. participation in, and provision of, financial services related to an issuer's offer or sale of a virtual asset or both.

Crypto-asset activities such as the exchange of assets, custody, borrowing/lending and yield/staking could all fall within the activities listed at (1) to (5) above.

Significantly, under the VASP regime, a person falling within the definition of a VASP must not only comply with AML obligations but must also register with the Central Bank. This registration is not merely a formality and the Central Bank may refuse a registration application, including on the grounds that the applicant fails to satisfy fitness and probity criteria. The registration procedure itself involves a number of steps, which are set out on the Central Bank's website.

As a further enhancement to the AML framework for crypto assets, the EU has enacted a Regulation (EU 2023/1113) on information accompanying transfer of funds and certain crypto assets which is directly applicable in Ireland from 30 December 2024. This Regulation replaces the existing Wire Transfer Regulation (EU 2015/847) and will increase the traceability of crypto asset transfers. The Regulation requires crypto asset service providers to ensure that transfers of crypto assets are accompanied by certain information on the originator and beneficiary of the transfer: eg, the originator's name and address.

MiCA

Following approval by the Council of the EU and the European Parliament, MiCA was published in the Official Journal on 9 June 2023 and entered into force on 29 June 2023. As an EU Regulation, no transposition is required by Ireland and MiCA has direct effect as part of Irish national law. That said, there are certain national discretions that are left to be implemented by each Member State and other ancillary matters which will require some supplementary Irish law measures, most likely in the form of regulations made by the Minister for Finance.

MiCA provides for three types of crypto asset:

- asset-referenced tokens (ARTs),
- electronic money tokens (e-money tokens or EMTs) and
- other crypto assets – neither ARTs nor e-money tokens, including utility tokens.

MiCA prescribes uniform requirements for the offering and admitting to trading of these types of crypto assets and prescribes requirements for crypto asset service providers (CASPs). This encompasses transparency and disclosure requirements for the admission to trading of crypto assets, authorisation and supervision requirements, requirements for the protection of holders of crypto assets and the clients of CASPs, and measures to prevent market abuse such as insider dealing or market manipulation.

Under MiCA, CASPs are entities that provide crypto asset services to clients on a professional basis. They must be authorised by a national competent authority in order to operate in the EU. In Ireland, this is the Central Bank.

MiCA does not apply to crypto assets that 'are unique and not fungible with other crypto assets' or to crypto assets that also qualify as one or more of:

- financial instruments as defined in MiFID II;
- deposits, including structured deposits, as defined in the Deposit Guarantee Scheme Directive;
- funds, except if they qualify as e-money tokens, as defined in PSD2;
- securitisation positions;
- non-life or life insurance products or reinsurance and retrocession contracts; or
- certain pension products, social security schemes and officially recognised occupational pension schemes.

Notably, non-fungible tokens (NFTs) are not covered by MiCA rules.

MiCA will mostly apply from 30 December 2024 but the requirements relating to ARTs and EMTs will apply from 30 June 2024.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

Payment service providers

Payment institutions are regulated under PSD2, as transposed into Irish law by the Irish Payment Services Regulations, and related measures. Regulation 6(1) of the Irish Payment Services Regulations provides that a person shall not provide a payment service (as set out in Schedule 1 – Payment Services of those Regulations) in Ireland unless that person is authorised, either under Irish law or the law of a member state of the EEA as a credit institution, an electronic money institution or a payment institution, subject to certain exceptions.

The Central Bank is responsible for the authorisation, prudential regulation and supervision of payment institutions in Ireland. There are eight payment services under the Irish Payment Services Regulations, mirroring those set out in PSD2.

If activities comprise regulated payment service activities in Ireland, there are a number of exemptions under the Irish Payment Services Regulations which should be considered, including for example, a 'commercial agent' exemption (which may apply if acting on behalf of the payer only or the payee only) and a 'limited network' exemption. The activities could then be structured, if possible, to avail of these exemptions and thus not require authorisation as a payment institution. However, there are certain limitations in relying on these exemptions.

Digital wallets

The provision of digital wallet services may fall within the meaning of electronic money services (an e-money service) requiring authorisation under the Irish E-Money Regulations. Authorisation as an e-money institution is broader than authorisation as a payment institution, as it permits an entity to provide both payment services and e-money services.

The Central Bank places significant emphasis on the safeguarding of users' funds. An e-money institution (and payment institutions) must have a safeguarding risk framework in place, approved by its board, which ensures that relevant client funds are appropriately identified, managed and protected on a day-to-day basis. There must be oversight of this framework by an applicant's second line of defence (risk and compliance functions) and third line of defence (internal audit).

In Ireland, an e-money institution (and payment institution) would have the choice of safeguarding users' funds in either of two ways: (1) by depositing the funds in a separate bank account in a credit institution or by investing the funds in assets accepted by the Central Bank as secure and low risk, or (2) by insuring the funds with an insurance company or having them guaranteed by a credit institution. Where the funds are deposited in a separate bank account, the Irish E-Money Regulations provide legal protections for the e-money users in the event of the e-money institution's insolvency.

In 2023, an external audit of safeguarding requirements is required by the Central Bank for e-money institutions (and payment institutions) who safeguard users' funds. While this audit applies only for 2023, depending on the outcome of the audit, it is possible that similar audits may be required in the future.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

Promoting fintech is a key part of IFS2020 (Ireland's International Financial Services Strategy) which is a whole-of-government approach to driving the growth and development of international financial services in Ireland. Financial innovation remains a key focus of regulatory attention and is likely to continue to do so for the immediate future.

In Ireland, the Central Bank has chosen to focus on facilitating regulatory contact between innovators and the Central Bank as an initial step, instead of immediately establishing a sandbox. The Central Bank has set up its own Innovation Hub as well as an industry engagement programme for fintech firms.

The Central Bank's Innovation Hub allows fintech firms to engage with the Central Bank outside of existing formal regulatory/firm engagement processes. The purpose of the Innovation Hub is to act as a resource to help innovators navigate the regulatory landscape by providing information on:

- relevant parts of the regulatory regime;
- specific supervision rules and policies; and
- navigating the Irish supervisory and regulatory landscape.

The Innovation Hub is open to enquiries from individuals, new fintech firms and existing firms which provide or intend to provide financial products or services that are innovative and sufficiently mature. A financial product or service will be innovative if it is based on new technology which:

- does not already exist in the Irish market or has not been rolled out on a significant scale; or
- materially changes the manner in which an existing product or service is constructed or delivered.

To be mature, the relevant firm must be able to show an appropriate amount of thought in developing the idea.

Aside from Ireland's position as a fintech hub, there are a number of advantages to being authorised in Ireland, including:

- a strong regulatory framework with a credible and experienced regulator, the Central Bank;
- a favourable passporting regime with the ability to passport to other European Economic Area Member States either on a branch or a cross-border services basis;
- a favourable tax regime, due to a combination of a 12.5 per cent corporate tax rate and an exceptionally extensive and comprehensive set of double tax agreements; and
- access to a sophisticated financial services ecosystem with a deep pool of staff, managers, professional advisers, regulators and service providers including not only native English speakers but a sizeable international population.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

As noted in Question 1, the main legislation relevant to open banking is the Irish Payment Services Regulations. These Regulations do not 'regulate' open banking: rather they provide the framework within which open banking is facilitated (through the regulation of payment initiation service providers (PISPs) and account information service providers (AISPs).

Third parties seeking to access account data for open banking purposes must register as an AISP (an entity which collects information on one or more payment accounts and aggregates account details

such as balances or outgoings and displays them on a single platform) or be authorised as a PISP (an entity that initiates a payment order for an account held with another provider at the user's request) with the Central Bank. The activities of AISPs and PISPs are highly regulated to ensure consumer protection, and informed consent from consumers is required before data is shared.

While registration as an AISP is considered a lighter form of authorisation than providing some other payment services, an AISP is still undertaking payment services and is supervised by the Central Bank in the same way as firms providing other payment services.

On 23 June 2022, the EBA published an opinion (Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)) which, among other things, suggested a move from 'open banking' to 'open finance' meaning an expansion from access to payment accounts data towards access to other types of financial data (such as savings, investments and insurance data).

On 28 June 2023, the EU Commission proposed a package of measures (which are not yet law) relating to payment services. One of these measures was a legislative proposal for a Regulation on a Framework for Financial Data Access to establish clear rights and obligations to manage customer data sharing in the financial sector beyond payment accounts. Under the proposal, customers will have the possibility (but no obligation) to share their data with financial institutions or fintech firms in a secure machine-readable format for customers to receive new, cheaper and better data-driven financial and information products and services, such as financial product comparison tools and personalised online advice. If enacted into law at EU level, this Regulation would be directly applicable in Ireland.

Italy

Alessandro Portolano*
Chiomenti, Milan
alessandro.portolano@chiomenti.net

Jasmine Mazza
Chiomenti, Milan
jasmine.mazza@chiomenti.net

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

Fintech regulation still lacks a uniform and harmonised legal framework at the Italian national level. The Italian legislator, to date, has mostly adapted existing rules that apply to traditional banking and financial services.

The most relevant areas in which financial innovation has been regulated in Italy (in addition to the areas that have already been regulated under EU law) are described below.

Crowdfunding

In accordance with global trends, Italy has witnessed a move towards new funding instruments capable of effectively channelling the necessary economic resources towards the production system, thus favouring the emergence of alternative financing channels for the banking system. Among these channels we can find crowdfunding – a technique for raising resources on the basis of a direct relationship between demand and supply of credit, without making use of the typical function of the banking system, and in a completely disintermediated manner.

Italy has arguably been the first European Union Member State to provide a specific regulation for equity crowdfunding (namely, the Commissione Nazionale per le Società e la Borsa (CONSOB)'s regulation On the Collection of Capital via Online Platforms, adopted by means of Resolution No 18592 of 26 June 2013, as amended).

The EU Commission subsequently adopted the Regulation on European Crowdfunding Service Providers (EU) 2020/1530 (the 'EU Crowdfunding Regulation'), aiming to harmonise the different EU jurisdictions and to introduce a common framework for all (investment

* Alessandro is a partner at Chiomenti, a leading Italian law firm, and has 25+ years of experience in the field of financial regulations. He has previously worked at the Bank of Italy, within the Supervisory Department in Rome. He heads the Financial Regulations Practice and advises financial institutions in relation to all areas of the banking, financial, insurance, payment services and asset management regulations. His experience includes assistance in both ordinary and extraordinary transactions, proceedings before Italian and European regulators, structuring of business models, and entry into new markets. He has assisted regulators in relation to complex and innovative matters. Alessandro is ranked in the top tier Band 1 in the financial services regulations ranking by all main specialist research institutes, including Chambers and Partners, Legal 500 and LegalCommunity.
Jasmine Mazza joined the firm in 2016. During 2020, Jasmine worked at the European Banking Authority, in the Fintech Team of the Banking Markets, Innovation and Product Unit. Jasmine provides legal assistance in matters concerning banking, insurance and financial markets, with a particular focus on legal issues related to the impact of technology on the business and operational models of supervised entities, such as structuring the customer journey in full-mobile mode, and the drafting and negotiation of outsourcing contracts. During her time at the European Banking Authority, Jasmine participated, inter alia, in the preparatory work on the DORA and MiCAR Regulations and the preparation of the EBA's report on digital platforms.

and lending-based) crowdfunding platforms operators. The Italian legislator has recently implemented the EU Crowdfunding Regulation at national level.

Under the new rules, crowdfunding services, whether loan-based or investment-based, can be provided by supervised intermediaries (banks, intermediaries under Article 106 of the Consolidated Banking Law, payment institutions, electronic money institutions (EMIs) and investment companies) or by crowdfunding providers other than supervised intermediaries providers, subject to authorisation by the competent authorities. As per the domestic implementation, with regard to the first-level legislation, the Italian government, as entrusted by Law No 127 of 4 August 2022 (*Legge di delegazione euopea 2021*), published Legislative Decree No 30 of 10 March 2023.

Pursuant to this Decree, the national competent authorities under the EU Crowdfunding Regulation are the Bank of Italy and CONSOB. The Bank of Italy and CONSOB, in their capacity as national competent authorities, have therefore established a second level of regulation.

On 17 May 2023, the Bank of Italy launched a public consultation on the new supervisory guidelines for specialised crowdfunding service providers (the 'Supervisory Guidelines'), outlining its expectations of how crowdfunding providers other than supervised intermediaries should comply with the provisions related to corporate governance, internal controls, assessment of suitability of responsible individuals and project assessment. The consultation concluded on 16 June 2023 and was followed by the publication of the Supervisory Guidelines on 2 August 2023.

On 1 June 2023, with Resolution No 22720, CONSOB – having regard to the Supervisory Guidelines – adopted the new regulation on crowdfunding services (the 'CONSOB Regulation'). This implements the EU Crowdfunding Regulation, repealing CONSOB Resolution No 18592 of 26 June 2013.

CONSOB has established an office dedicated to crowdfunding, reachable via legal mail by providers for the sake of application, communications, transmission of documents and information.

On 22 November 2023, the Bank of Italy launched another public consultation in relation to the provisions on the disclosure obligations for crowdfunding service providers towards the competent authorities (the 'BoI Regulation'). The consultation concluded on 22 January 2024 and was followed by the publication of the BoI Regulation on 8 May 2024.

Below are the most relevant areas in which the domestic regime deviates or adds to the EU regulatory framework. In line with the EU framework, the regulatory framework does not cover peer-to-peer lending for the benefit of consumer and invoice trading, which are allowed to the extent that the platform is able to ensure compliance with national rules on credit brokerage and granting of finance.

Marketing rules applicable to both Italian and EU providers

The CONSOB Regulation sets some additional marketing rules applicable to both Italian and EU providers targeting Italy without prejudice to the provisions under the EU Crowdfunding Regulation. Firstly, the marketing communications related to crowdfunding services must be in Italian and must disclose the provider's name and online platform. Secondly, such communications must highlight – in an appropriate graphic layout – the risks associated with crowdfunding investments. Furthermore, certain essential disclaimers must always be incorporated, including in the context of marketing

communications utilising audio and video media. These include a disclaimer cautioning investors to review the key information sheet.

Corporate governance, internal controls, assessment of suitability of responsible individuals, and project assessment applicable to crowdfunding providers different from supervised intermediaries

The Supervisory Guidelines offer guidance to providers on establishing corporate governance and internal control systems designed to ensure sound and prudent management. These include:

- the implementation of strong corporate governance structures with clear decision-making processes and well-documented organisational hierarchies and responsibilities;
- the creation of an effective internal risk management and control system;
- the establishment of efficient internal communication channels to keep the corporate bodies updated on the overall structure;
- the development of policies and procedures to ensure the adequate qualification and training of staff; and
- the adoption of administrative and accounting policies and procedures that enable the prompt submission of accurate balance sheets and similar documentation to authorities in compliance with relevant regulations.

Outsourcing is allowed, contingent upon the provider's continuous oversight of the entrusted third party, which must meet rigorous qualifications tailored to the outsourced activity. Nevertheless, the Bank of Italy cautions against providers transforming into mere 'empty shells', thus providers must maintain substantial operations.

The Supervisory Guidelines are not strictly binding, but any deviation must be communicated and justified to the Bank of Italy.

Reporting obligations for crowdfunding service providers towards the national competent authorities

The BoI Regulation provides that all crowdfunding service providers comply with specific reporting obligations, in addition to the prudential reports under Bank of Italy Circular No 286 of 17 December 2013 and Bank of Italy Circular No 154 of 22 November 1991.

Crowdfunding service providers must promptly notify the Bank of Italy and CONSOB of the date when they began using their authorisation, as well as any interruptions and resumptions in the provision of crowdfunding services. They must also communicate any substantial changes in the conditions of their authorisation.

In particular, by 25 January of each year, intermediaries supervised by the Bank of Italy must send to the Bank of Italy the information referred to in Article 16, paragraph 1 of the EU Crowdfunding Regulation: namely, a list of projects funded through its crowdfunding platform, specifying for each project:

- the project owner and the amount raised;
- the instrument issued; and
- aggregated information about the investors and invested amount broken down by fiscal residency of the investors, distinguishing between sophisticated and non-sophisticated investors.

By 30 April of each year, crowdfunding providers other than supervised intermediaries must send to the Bank of Italy the information concerning any changes related to existing outsourcing agreements.

In addition, crowdfunding providers different from supervised intermediaries must send to the Bank of Italy information inter alia related to:

- any changes in qualifying holdings (eg the acquisition or increase of a stake that results in reaching or exceeding 20 per cent of the capital or voting rights in the provider, or that enables the acquirer to exercise control over the latter); and
- the proof that the natural persons involved in the management are of good repute and possess sufficient knowledge, skills and experience to manage the prospective crowdfunding provider and commit sufficient time to the performance of their duties.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

The Italian legislator is currently working on the domestic implementation of the EU Markets in Crypto-Assets Regulation (MiCAR).

Considering that under the Italian regulatory framework, crypto assets are not currently subject to any specific regulatory framework – except for anti-money laundering regulation that has introduced the domestic virtual asset service provider (VASP) registration regime (see below) – the implementation of MiCAR will have a disruptive impact.

Qualification of crypto assets within the financial space

Without prejudice to the above, crypto assets may fall within the traditional categories set out under the financial market regulation depending on their features and purpose, and may therefore be characterised, alternatively, as (1) financial instruments and (2) financial products.

The possible qualification of a crypto asset as a financial instrument or as a financial product may trigger the application of specific rules, such as the investment services rules and/or public offering rules. While the notion of 'financial instrument' is harmonised at the EU level,[1] the category of 'financial product' is a purely domestic legal concept, set out by the Italian Consolidated Financial Act (TUB). It includes: 'financial instruments and any other form of investment having financial nature'.[2]

1 Directive 2014/65/EU (MiFID II) defines 'financial instruments' by providing a list of assets that includes, inter alia, transferable securities, money market instruments, UCITS and derivatives. Indeed, the offering of financial instruments to the public is subject to a set of transparency and reporting obligations, the most important of which is the requirement to publish the so-called prospectus. Moreover, distributing financial instruments on behalf of the issuer qualifies as an investment service under MiFID II and the Italian Consolidated Financial Act and, therefore, is reserved to duly licensed entities (eg, investment companies or banks).

2 According to Art 1, para 1, let (u), of the Italian Consolidated Financial Act. Hence, this is a broad category that, in light of CONSOB's consolidated interpretation, encompasses any investment products characterised by the following main features: (1) the investment of capital; (2) the promise/expectation of a financial return deriving from the capital invested; and (3) the assumption of a financial risk directly connected and related to the investment.

The current VASP registration regime

By implementing Directive 2018/843 (AMLD 5), Italian law[3] extended the scope of application of the rules on the prevention of the use of the financial system for the purposes of money laundering, or terrorist financing to 'providers of services relating to the use of virtual currencies' (Article 1, Paragraph 2, let. ff) of the Legislative Decree No 231/2007 (AML Decree). Virtual currency is defined under the AML Decree as a 'digital representation of value, not issued or guaranteed by a central bank or public authority, not necessarily linked to a fiat currency, used as a medium of exchange for the purchase of goods and services or for investment purposes and transferred, stored and traded electronically'.

A provider of services relating to the use of virtual currencies is defined as:

> 'Any natural or legal person that provides to third parties, on a professional basis, services (including online services) that are functional to the use, exchange, and storage of 'virtual currency' and their change from or into fiat currencies or digital assets, [...] as well as issuing, offering, transfer and clearing and any other service functional to the acquisition, trading or brokerage in the exchange of those currencies.'

This includes digital wallet service providers.

When a crypto asset qualifies as 'virtual currency' in accordance with the AML Decree, the providers of services relating to the use of virtual currencies are subject to several obligations, including obligations concerning customer due diligence, record-keeping, reporting of suspicious transactions and other requirements linked to anti-money laundering/countering the financing of terrorism (AML/CFT) risk prevention.

Italy has introduced a special domestic registration framework for entities providing services related to virtual currencies in Italy, also through digital means. Legislative Decree No 90/2017 amended Legislative Decree No 141/2010 by introducing, in Article 17-bis, paragraph 8-bis, the obligation for VASPs and digital wallet service providers operating in Italy to be registered in a special section of the registry of money changers kept at the Body of Agents and Mediators (Organismo Agenti e Mediatori or OAM), and to be supervised by Guardia di Finanza.

By virtue of paragraph 8-ter of the same article, the Italian Treasury published the Decree of 13 January 2022 containing the modalities and timelines for the communication by the aforementioned entities of their operations in Italy (even if carried out online via app/website).[4]

After the activation of the VASP register, operators complied with quarterly reporting providing OAM with data on their operations in Italy. This detailed information is useful in making a first assessment on the crypto asset market's response to the registration regime in Italy. At the end of the second quarter of 2023, this is very concentrated, with large exchanges handling the majority of cryptocurrency transactions: 89.7 per cent of clients operate on large exchanges, 10.1 per cent on medium-sized exchanges, and

3 Legislative Decree 90/2017.

4 The OAM proceeded to activate the special section of the registry on 16 May 2022, specifying that those who already conduct business, including online business, in Italy and meet the legal requirements will be able to continue to do so but will have to apply for registration with the registry within 60 days after 16 May. Failure to meet the deadline or denial of registration by the body results in any activity being considered abusive. Among the requirements for registration of entities other than individuals is to have a registered administrative office in Italy or, for EU entities, a permanent establishment in the territory of the Republic.

0.2 per cent on small exchanges. At the end of June 2023, out of 1.235 million clients, 72 per cent held cryptocurrencies in their portfolios. The total value of cryptocurrency portfolios held by Italian clients at the end of Q2 2023 was €1.233bn.

The implementation of MiCAR

On 24 June 2024 the Italian government approved a legislative decree to adapt domestic regulations to MiCAR (the 'MiCAR Decree'), which introduces a regulatory framework for cryptocurrency service providers (CASPs) operating in Italy, which will replace the rules currently in place for VASPs and will impose compliance standards significantly higher than those currently in place for Italian operators.

In this respect, the MiCAR Decree provides for a 12-month transitional period lasting until 30 December 2025, for those VASPs which:

- are regularly registered in Italy as of 27 December 2024;
- are in good standing with the OAM; and
- will apply for authorisation to operate as CASPs in accordance with MiCAR, either in Italy or in another EU Member State, by 30 December 2024.

On 22 July 2024, the Bank of Italy published a new communication regarding the implementation of MiCAR in Italy providing for important information around its supervisory focus and major areas of attention during the implementation phase of MiCAR in Italy, namely that:

- crypto assets other than asset-referenced tokens (ARTs) and electronic money tokens (EMTs) – especially when 'unbacked' and lacking intrinsic value, real economic backing, or redemption rights – are considered unsuitable for payment purposes due to their high-risk profiles; and
- particular attention shall be paid in relation to the offering of ARTs as a means of payment.

Within the aforementioned communication, the Bank of Italy also specifies that virtual asset service providers (VASPs) currently enrolled in the register held by the OAM still apply the provisions of the current AML regulatory framework in the context of the transition to the new regime.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

The Italian regulatory framework has seen significant changes over the last decade, particularly regarding the regulation of the entities authorised to provide payment services. Many new operators were introduced by the European legislator in the payment services market alongside the banks.

More specifically, as a result of the transposition of Directives No 2000/46/EC, No 2000/28/EC and No 2009/110/EC, Title V-bis (dedicated to electronic money institutions), and Title V-ter of the Italian Consolidated Law on Banking (TUB) (concerning payment institutions) were introduced into TUB.

Lastly, with the transposition of Directive No 2009/110/EC, Title V-bis of TUB was further amended, aligning the EMIs regulation with the rules on payment institutions (PIs) to ensure a level playing field for all the providers of payment services and homogeneous supervisory regimes.

Due to these innovations, the definition of payment service providers now includes banks, Poste Italiane, EMIs, PIs and any other entity authorised to offer payment services.

In addition to their core businesses, PSPs are entitled to provide services that are ancillary to payment services. They can also provide digital wallet services through a mobile app or a web browser.

Digital wallets are online payment tools that allow: (1) immediate payments (staged wallets); and/or (2) credit, debit and/or prepaid card transactions (pass-through wallets). The functioning of the pass-through wallets is normally based on the agreement between the wallet operator (usually a tech company), the issuer of the payment instrument (PSP) and the acquirer of the online merchant. In the case of staged wallets, the customer and the online merchant both have a payment or e-money account held by the provider of the wallet (the PSP). In such case, the customer selects the wallet as the payment method and orders a money transfer, similar to a credit transfer, from their account to the merchant's account, entering the credentials for strong authentication, if any.

If digital wallets are used, PSPs must apply the security standards provided for in the second Payment Services Directive (PSD2) and transposed in Legislative Decree No 11/2010, such as strong customer authentication (SCA).

Adding a payment card to a digital wallet as well as initiating an electronic payment transaction or accessing the payment account (via the mobile app) are actions that may pose a risk of payment fraud or other abuse, and therefore require the application of SCA.

On 28 October 2022, the Bank of Italy published a communication addressing certain aspects of 'Buy Now, Pay Later' (BNPL) services and describing the two main forms of BNPL. It is noted by the Bank that, despite the growing popularity of BNPL among consumers, it currently operates in a regulatory grey area within the Italian legal framework. There are no ad hoc rules to this kind of lending activity and applicable regulation is to be assessed on a case-by-case basis.

As per the main different schemes of BNPL, all of them essentially involve three key players: the merchant, the consumer and the bank (or financial intermediary).

One BNPL model sees a bank entering into an agreement with a merchant, allowing consumers to purchase the merchant's goods and services by being granted a credit by the bank. In this scheme, the 'lending relationship' is between the bank and the consumer, thus relevant safeguards to consumer lending apply provided that the consumer pays a fee for the BNPL service and the granted sum is over €200.

Another BNPL model occurs when the payment deferment is granted to the costumer directly by the merchant, the latter – immediately after – transferring the credit with the said consumer to a bank. In such scenario, safeguards associated with a bank-customer relationship do not apply between the merchant and the consumer, since the payment deferral does not entail the provision of credit services per se by the merchant (eg, a shoe shop). However, there is room to argue that

some additional element of risk for consumers arises, as it becomes more challenging to identify the party responsible for the payment deferment and to understand the precise role of financial intermediaries in the transaction. Accordingly, the Bank of Italy recommends higher cautions and has committed to closely monitoring BNPL trends.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

The Italian Ministry of Economy and Finance has set out the 'FinTech Committee rules and experimentation' in Decree No 100/2021: ie, the regulatory sandbox of fintech activities through which Bank of Italy, CONSOB and IVASS (respectively, the banking, securities, and insurance supervisors) will facilitate the development of innovative products and business models in the banking, financial and insurance fields.

The regulatory sandbox aims to create a controlled space in which the latest technologies for the banking, financial and insurance sectors are tested in the market without prejudice for competition rules and consumer protection. To facilitate the development of such innovations, the authorities permit developers to operate in a privileged and simplified regulatory space which provides for special waivers for the test's purpose (eg, simplified requirements that are proportionate to the activities to be carried out, timeline for the granting of authorisations, and admissible corporate structures).

Access to the sandbox depends on meeting requirements regarding both the nature of the operator (ie, the subject) and the characteristics of the innovation (ie, the object).

As per the subjective requirements, the operators admitted to the regulatory sandbox are mainly those who want to test a particular activity subject to authorisation or registration in any list kept by one of the supervisory authorities, or who want to test an activity that is generally restricted (eg, lending activities not carried out vis-à-vis the public).

As per the objective requirement, the activities admitted to the sandbox are those leveraging innovative technologies in the provision of services, products or processes useful in the banking, financial and insurance fields (eg, application programming interfaces (APIs), digital ID and authentication systems or natural language processing). When applying for the sandbox, operators are asked to demonstrate the novelty of the project through internal analyses and/or market analyses.

Once admitted to the sandbox, operators can start testing the innovations under the guidance of the authorities. They are asked by the competent authority to submit a report after the termination of the testing period, which corresponds to the ceasing of the simplified regime.

The first-round sandbox was opened between 15 November 2021 and 15 January 2022. The projects chosen during that period are still undergoing testing under the oversight of the Bank of Italy. The second-round sandbox was opened between 3 November 2023 and 5 December 2023. The sandbox framework is expected to be revised in the near future to take into account market feedback on the functioning of the sandbox.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

Italy has not adopted a comprehensive legislation on open banking. The real revolution in the payments system has, thus, been represented in Italy by the implementation of PSD2 – with the Legislative Decree of 15 December 2017, No 218 and the Italian Legislative Decree of 27 January 2010, No 11 – which gave full legal recognition in Europe to open banking models based on the sharing of bank data among different operators.

Article 5-ter and Article 5-quater of the Italian Legislative Decree of 27 January 2010, No 11 require banks to allow third-party providers (TPPs) access to payment accounts.

PSD2 draws a fundamental distinction between payment initiator service providers (PISPs), which are enabled to provide payment initiation services, and account information services providers (AISPs), which are enabled to provide accounting information services. To gain access to accounts, each TPP must obtain a specific authorisation from the Bank of Italy demonstrating that it meets the necessary requirements, following a path similar to that which a PI must follow to obtain a licence.

Lithuania

Ieva Dosinaitė*
Ellex Valiunas, Vilnius
ieva.dosinaite@ellex.legal

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

There are no specific laws or regulations for fintechs in Lithuania. Nevertheless, there are certain pieces of regulations that indirectly relate to technology applied to financial innovation, the most relevant of which are summarised below.

Law on Electronic Money and Electronic Money Institutions

This law applies to people entitled to issue electronic money in the Republic of Lithuania and establishes conditions for: the issuance and redemption of electronic money; the procedure for the licensing, operation, termination and supervision of electronic money institutions; and branches of electronic money institutions in foreign countries. It ensures the system of electronic money institutions is stable, reliable, efficient and secure.

Law on Payment Institutions

This law lays down the procedures for the licensing, operation, closure and supervision of payment institutions in order to ensure that the system of payment institutions is stable, sound, efficient and safe.

Law on Financial Institutions

This law establishes:

- what services are considered to be financial services;
- the requirements for the founders, participants and managers of financial undertakings and credit institutions engaged in the provision of financial services;
- their rights and obligations;
- the conditions, procedures and peculiarities for the establishment, operation, termination and resolution of financial institutions; and
- the conditions, procedures and specifics of the supervision of the activities of financial institutions licensed as providing financial services.

* Ieva is a partner who, during her professional career, has represented and advised on complex financial transactions, regulatory and capital markets-related issues for the following: banking and financial institutions, insurance companies, trading companies inter alia EBRD, EIB, Lithuania's largest private business groups and state-owned enterprises, and global fintech companies operating in the Baltics. She has significant experience managing pan-Baltic legal projects and is noted for solving legal issues with international institutions.

This law applies to all financial institutions – legal entities of Lithuania and branches of foreign financial institutions operating in Lithuania and engaged in the provision of financial services set out in this law.

Law on Payments

This law regulates:

- the activities and responsibilities of payment service providers;
- payment services, the conditions for their provision and the informational obligations related thereto;
- the authorisation and execution of payment transactions;
- authentication, operational and security risk management;
- the rights and obligations of users of payment services and providers of payment services in relation to payment services where the provision of payment services is a business;
- the rules on transparency and comparability of fees charged to natural payment service users for payment accounts;
- the rules on the transfer of payment accounts;
- the rules and conditions for the opening and use of a basic payment account; and
- the rights and powers of the supervisory authority in the supervision of compliance with the provisions of this Law and the out-of-court settlement of consumer disputes.

Law on Prevention of Money Laundering and Terrorist Financing

The purpose of this law is to establish measures for the prevention of money laundering, including certain requirements for institutions, inter alia, fintechs, and/or terrorist financing and the institutions responsible for the implementation of measures for the prevention of money laundering and/or terrorist financing.

Bank of Lithuania positions and guidelines

The Bank of Lithuania, when needed, releases positions, guidelines, opinions and explanations of relevant local legal acts and decisions on the application of European Union guidelines, all of which are relevant for supervised financial market participants.

Open banking

In the EU, of which Lithuania is a member, the second Payment Services Directive (PSD2) requires banks to enable authorised third-party providers to access the accounts maintained by those banks in order to provide the account information and payment initiation services. Please see Question 5.

Other fintech-related laws at the EU level

There is no piece of EU legislation which covers all aspects of fintech. Fintech companies providing financial services (eg, lending, financial advice, insurance or payments), must comply with the same laws as any other companies offering such services. Therefore, different laws apply depending on the activity (eg, payment services or crowdfunding), such as Directive 2000/31/EC (e-commerce), Directive 2002/65/EC (distance marketing of consumer financial services), Directive 2009/110/EC (electronic money), Directive (EU) 2015/2366 (payment services), etc.

Crowdfunding

The Law on Crowdfunding provides a regulatory framework for equity crowdfunding.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

Crypto assets-related activity is not regulated in Lithuania. There is also no statutory obligation to get authorisation from the Bank of Lithuania for crypto assets-related activity. However, a status registration procedure to engage in crypto-related activities is required, which includes: (1) establishment of a local entity; (2) notification of the Commercial Register of Legal Entities about its activities; and (3) employment of a local money laundering reporting officer. Upon the status registration, the said legal entity becomes an obliged entity under relevant anti-money laundering (AML) laws, and must follow local laws and report to the Financial Intelligence Unit.

It is important to note that the Law on the Prevention of Money Laundering and Terrorist Financing of the Republic of Lithuania (AML Law) includes virtual currency exchange and e-wallet service providers in the list of undertakings that are subject to anti-money laundering requirements, such as customer identification and verification, transaction monitoring and suspension, reporting to competent authorities and provision of information upon a separate request, etc. Moreover, these regulations impose specific obligations on initial coin offering (ICO) offerors as well – in particular an obligation to identify a customer in certain cases or provide information to authorised institutions.

The Bank of Lithuania has stated its position on virtual currencies and ICOs: when offered coins have features of securities, a prospectus should be drawn up and approved by the regulator and the coins should follow other requirements of the Law on Securities of the Republic of Lithuania. Moreover, depending on the nature of the offering, statutory requirements for crowdfunding, collective investment and provision of investment services, the secondary market or the formation of a financial market participant's capital would similarly apply to an ICO.

Nevertheless, on 30 June 2022, the Council and the European Parliament reached a provisional agreement on the markets in crypto assets (MiCA) proposal which aims to support market integrity and financial stability. The MiCA Regulation (Regulation (EU) 2023/1114) was published in the Official Journal of the European Union on 9 June 2023. The MiCA Regulation establishes uniform requirements for the offer to the public and admission to trading on a trading platform of crypto assets excluding asset-referenced tokens and e-money tokens, as well as for asset-referenced tokens and e-money tokens. Additionally, it sets out requirements for crypto asset service providers, defined

as legal persons or other undertakings whose occupation or business involves providing one or more crypto asset services to clients on a professional basis. The new regulation of the crypto asset market entered into force on 30 December 2024, with the requirements for asset-referenced token issuers and e-money token issuers being applied from 30 June 2024.

Main requirements for offerors of crypto assets other than asset-referenced tokens or e-money tokens include publishing an information document (a crypto asset white paper) containing mandatory disclosures, relevant marketing communication, identification, prevention, management and disclosure of conflicts of interest, safekeeping of clients' crypto assets and funds, along with an appropriate management body. In addition to complying with all the aforementioned requirements, asset-referenced token issuers will also have to:

- confirm the content of the crypto asset white paper with the Bank of Lithuania;
- obtain appropriate authorisation/licences;
- meet the capital requirements;
- prepare a redemption plan of the tokens to ensure that the rights of the holders of the asset-referenced tokens are protected where the issuers are not able to comply with their obligations;
- meet the requirements for safeguarding the client's crypto assets and funds; and
- establish and maintain an 'asset reserve', as well as meet the liquidity requirements for the reserve of assets.

E-money token issuers must adhere to all the same requirements as asset-referenced token issuers, with the exception of confirming the content of the crypto asset white paper with the Bank of Lithuania. Furthermore, it's important to note that the holders of e-money tokens and asset-referenced tokens will have a right of redemption. Crypto asset service providers are required to meet capital requirements, obtain the necessary authorisation/licence, implement measures for identification, prevention, management, and disclosure of conflicts of interest, ensure the safekeeping and protection of clients' crypto assets and funds, and establish an appropriate management structure.

Before the start of their operations in Lithuania in accordance with the MiCA Regulation, offerors of crypto assets other than asset-referenced tokens or e-money tokens must complete several essential steps. They will be required to submit the crypto asset white paper, their marketing communications, a legal opinion confirming that the crypto asset does not qualify as an asset-referenced token or an e-money token, as well as a list of any host Member States where they intend to offer their crypto assets to the public or seek admission to trading to the Bank of Lithuania no later than 20 working days before the start of their operations. Additionally, they will have to make the crypto asset white paper publicly available on their website at the start of their operations.

E-money token issuers intending to operate in Lithuania under the MiCA Regulation must follow specific steps before starting their activities. These steps include notifying the Bank of Lithuania at least 40 working days before offering e-money tokens to the public or seeking their admission to trading, notifying the crypto asset white paper to the Bank of Lithuania at least 20 working days

before publication, and making the crypto asset white paper for e-money tokens publicly available on their website at the start of their operations.

Asset-referenced tokens can be issued by credit institutions or legal persons, or other undertakings established in the Union and authorised by the competent authority of its home Member State. A credit institution wishing to issue asset-referenced tokens must first receive the approval of the Bank of Lithuania regarding the crypto asset white paper and the programme of their operations. A legal person or other undertaking established in the Union and wishing to issue asset-referenced tokens must first submit a complete application and get the authorisation from the Bank of Lithuania. Asset-referenced token issuers meeting either of the following criteria may commence their operations in Lithuania upon the completion of a crypto asset white paper and by notifying both the crypto asset white paper and, upon request, any marketing communications to the Bank of Lithuania. These criteria are as follows: (1) the issuer's average outstanding value of the asset-referenced token does not exceed €5m or the equivalent amount in another official currency over a 12-month period, calculated at the end of each calendar day, and the issuer has no affiliation with a network of other exempt issuers; or (2) the offer of the asset-referenced token to the public exclusively targets qualified investors, and such tokens can solely be held by qualified investors.

Crypto asset services can be provided professionally by legal persons, credit institutions, central securities depositories, investment firms, market operators, electronic money institutions, UCITS management companies, or alternative investment fund managers that are allowed to provide crypto asset services pursuant to Article 60 of the MiCA Regulation. Licensed entities wishing to offer crypto asset services must notify the Bank of Lithuania 40 working days prior to commencing operations.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

In Lithuania, there are two types of payment service providers defined by legal acts (in general, the Law on Electronic Money and Electronic Money Institutions and the Law on Payment Institutions): (1) payment institutions (PIs); and (2) electronic money institutions (EMIs).

A PI is defined by the regulations as a market participant providing payment services and licensed by the Bank of Lithuania. A payment institution may carry out money transfers, payment operations, cash deposits or withdrawal services, direct debit or credit transfers, etc, but may not accept deposits from retail market participants or issue electronic money. In addition to payment services, it is entitled to provide ancillary services closely related to these services, such as foreign exchange.

A payment institution may also hold a restricted licence. If a payment institution holds a restricted licence, it is subject to lighter requirements for management – no capital and shareholder eligibility requirements apply – but it is subject to the restrictions on the turnover of payment transactions laid down in the Law on Payment Institutions. Such an institution may only operate in Lithuania. A payment institution may hold a licence as a payment institution providing an account information service. This licence is valid in other EU Member States, but is not subject to capital and shareholder eligibility requirements, requirements for the protection of funds, intermediaries and the transfer of

operational functions. A payment institution holding an unlimited licence may operate throughout the EU.

On the other hand, an EMI is defined by the regulations as a company which has been issued with an electronic money institution licence, or an electronic money institution limited activity licence granting the right to issue electronic money in the Republic of Lithuania and/or other EU Member States. An electronic money institution may also carry out money remittances, payment transactions, cash deposit and withdrawal services, direct debit and credit transfers, etc.

The Lithuanian financial market and its participants are supervised by the Bank of Lithuania. In Lithuania, financial market supervision is based on a risk-based supervisory model. This means the Bank of Lithuania focuses its resources on the most systemically important financial market participants, or financial services and products that pose the greatest risk to consumers. The Bank of Lithuania periodically carries out examinations (inspections and investigations) of financial market participants. As mentioned in Question 1, the Bank of Lithuania, when needed, releases positions, guidelines, opinions and explanations of relevant local legal acts, decisions on the application of EU guidelines, all of which are relevant for supervised financial market participants.

Furthermore, on 28 June 2023, the Commission published a proposal to amend and modernise the current Payment Services Directive (PSD2) which will become PSD3 and establish, in addition, a Payment Services Regulation (PSR). Both will likely enter into force by the end of 2026. It updates and clarifies the provisions relating to PIs and integrates former EMIs as a sub-category of PIs (and consequently repeals the second Electronic Money Directive, 2009/110/EC). The main goals of the new legal framework include combatting and mitigating payment fraud, improving consumer rights, further levelling the playing field between banks and non-banks, improving the functioning of open banking, improving the availability of cash in shops and via ATMs, and strengthening harmonisation and enforcement.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

In 2018, the Bank of Lithuania launched its own regulatory sandbox, which was meant to facilitate the introduction of financial innovation in the Lithuanian financial market, especially where the regulation of financial innovation is insufficient or unclear. It was also intended to enable the Bank of Lithuania to understand in advance the potential impact of financial innovation on consumers and the financial system; to identify emerging risks and potential regulatory gaps in the financial market related to the application of financial innovation; and to seek to address or mitigate, within the scope of its competence, such regulatory gaps and the potential negative impact of financial innovation.

The sandbox allows potential and existing fintech companies to test financial innovations in a live environment under the guidance and supervision of the regulator. Participation in the sandbox has many advantages, such as continuous consultation with the regulator, access to real consumers for testing new products and services, exemptions from certain regulatory requirements

during participation (ie, no obligation to have a licence in hand) and, except when necessary, no enforcement measures under legal acts applicable either to the participant or its managers.

Fintech companies may enter the regulatory sandbox if their financial innovation meets the following criteria:

1. it is new to Lithuania's market;
2. if implemented, it would bring more convenient, safer and cheaper financial services or other identifiable benefits to consumers;
3. its testing in a live environment is objectively necessary and may contribute to the implementation of the said financial innovation;
4. the financial market participant has carried out an assessment of its adaptability, allocated sufficient resources, carried out a risk analysis; and
5. it will be further developed in Lithuania.

Furthermore, the Bank of Lithuania's Newcomer Programme helps potential financial market participants evaluate their opportunities in Lithuania and gives an insight on legislative and licensing requirements for businesses aiming to start their activities in the country. It is a one-stop shop for meetings and consultations with potential financial market participants, basic information about licensing and financial services opportunities in Lithuania, requesting meetings, consultations via email or phone on launching a business or a new product and checking whether your future plans are in line with legislative and licensing requirements.

From a tax perspective, Lithuania offers several tax incentive schemes for small/medium-sized businesses and tech/fintech businesses:

- small-sized entities whose average number of employees does not exceed 10 people and whose income during a tax period does not exceed €300,000 are exempted from corporate income tax during the first tax period. These companies are taxed at a rate of 5 per cent during other tax periods compared to the standard rate of 15 per cent. In order to benefit from such tax incentive, shareholders of an entity should be natural persons;
- Lithuania offers the possibility to reduce the taxable profit by actual costs incurred for the investments in fundamental technological renewal. Taxable profits may be reduced by up to 100 per cent, and the costs exceeding this amount may be carried forward to reduce the amount of taxable profits calculated for the subsequent four tax periods. Such tax relief may be used for the tax periods of 2009–2023; and
- Lithuania also promotes alternative financing by exempting collective investment undertakings, private equity and venture capital undertakings from corporate income tax – ie, income, dividends and other distributed profits are not taxed. It should also be noted that legal entities' incomes from the increase in the value of assets, dividends and other distributed profits, received from units, shares or contributions held by collective investment undertakings are also not taxed.

There is also a plethora of both national and EU-wide public and private accelerators that startups may freely apply to. Lastly, the community is also quite unified – Fintech HUB LT unites fintech

industry participants in Lithuania, helping them to create the best conditions for their activities, whilst FINTECH Lithuania also brings together fintechs, developers of IT solutions, service providers for fintechs, legal, licensing and regulatory compliance consultants, banks and other ecosystem participants.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

In the EU, of which Lithuania is a member, PSD2 requires banks to enable authorised third-party providers to access accounts held by banks in order to provide account information and payment initiation services. However, the framework does not define a single standard for achieving this.

There are different API standardisation groups across Europe working towards harmonisation of the PSD2 API standard, such as the Berlin Group, PolishAPI, STET. The Berlin Group is the leading API standardisation group which unites almost 40 banks, associations and payment service providers. The majority of banks in Lithuania have decided to develop the PSD2 API in accordance with the Berlin Group standard that will enable access to customer data for all participants.

Luxembourg

Marc Mouton*
Arendt & Medernach, Luxembourg
marc.mouton@arendt.com

Philippe Dupont†
Arendt & Medernach, Luxembourg
philippe.dupont@arendt.com

1. Fintech regulatory framework: Please provide a description of the most relevant laws and regulations on fintech and financial innovation in your country. Please also refer to any new law or regulation foreseen in the near future or any bill on fintech and financial innovation in your jurisdiction.

In Luxembourg, the fintech regulatory framework is based on a combination of rules of European Union origin and rules of a purely domestic origin. The legal framework fosters innovation, in relation to the use of digital ledger technology. The Luxembourg financial supervisory authority, the Commission de Surveillance du Secteur Financier (the CSSF) is open to innovation and has issued helpful guidance in this field whilst maintaining the integrity of the financial sector, with a particular emphasis on protecting investors and market confidence, as well as a robust anti-money laundering approach.

The following legislation is the most relevant framework ruling in this space.

Virtual asset service providers

In March 2020, Luxembourg implemented a dedicated regulatory framework subjecting virtual asset service providers (VASPs) to anti-money laundering and counter-terrorism financing (AML/CTF) requirements. Under this regime, VASPs are required to register with the CSSF.

Under the law of 12 November 2004 on the fight against money laundering and terrorist financing (the AML/CTF Law), persons established in Luxembourg or offering virtual asset services in Luxembourg are required to complete a CSSF registration process, as well as adhering to the professional obligations set forth in the AML/CTF Law. Once registered, VASPs are supervised by the CSSF but only in respect of compliance with AML/CTF requirements.

The AML/CTF Law defines virtual assets as digital representations of value, encompassing virtual currencies, which can be digitally traded or transferred and utilised for various purposes, such as payments or investments. It is worth noting that the definitions used in the AML/CTF Law are broader than the definitions used in the relevant EU AML/CTF Directives.

---

* Marc Mouton is a partner in the Banking & Financial Services practice. He advises financial institutions such as banks, investment companies, payment institutions and electronic money institutions. He is an expert in financial regulatory matters, mergers and acquisitions in the financial sector, financial litigation and general banking law. Marc further specialises in emerging sectors such as fintech and the digitalisation of payment services and assists both new market entrants and established financial institutions.

† Philippe Dupont is a Founding Partner of Arendt & Medernach. He is a member of the Banking & Financial Services practice and specialises in banking and finance with a focus on bank regulatory, lending, structured finance, securities laws and litigation.

However, certain exceptions apply, notably in cases where virtual assets qualify as electronic money in accordance with the Payment Services Act, and where virtual assets qualify as financial instruments as per point (19) of Section 1 of the Financial Sector Act of 5 April 1993 (the LFS). In these cases, the broader regulatory framework for activities linked to electronic money and financial instruments respectively, applies.

The CSSF has also published helpful guidance on VASPs.

Virtual assets

Before the application of the EU-wide Regulation 2023/1114 on Markets in Crypto Assets (MiCA), there was no other specific domestic legal framework which applies to services linked to virtual assets.

However, the CSSF has issued the following two very helpful guidance documents:

1. FAQ – Virtual assets (UCIs); and
2. FAQ – Virtual assets (Credit institutions).

These guidance documents explain under which conditions for example credit institutions can provide custody services in relation to virtual assets and confirms their off-balance sheet treatment. The CSSF requires banks to follow a similar approach to Directive 2014/65/EU of 15 May 2014 on markets in financial instruments (MiFID II) to protect investors.

In these FAQs, the CSSF also provides guidance on the use of virtual assets in the investment funds sector including, eg, designation of the types of funds that may invest in these types of assets, and the conditions under which service providers like management companies and depositaries may engage in activities linked to this type of assets.

Payment services

According to the Payment Services Law, payment institutions, as well as electronic money institutions, must be authorised by the CSSF, while account information service providers only need to be registered.

Fintechs operating in the payment sector need to meet the regulatory standards set in the Payment Services Law.

We will further elaborate on this regulatory framework in Question 3.

Distributed ledger technology, blockchain and the DLT pilot regime

Luxembourg has actively been supporting the adoption of distributed ledger technology (DLT) in the financial sector.

The Law of 1 August 2001 on the circulation of securities, as amended, has been updated by a law of 1 March 2019, commonly referred to as Blockchain Law I, in order to allow banks and investment firms which offer securities custody services to keep securities accounts on DLT technology. An important feature of this law is that it assimilates successive transfers of securities registered on a DLT

platform to transfers between securities accounts, which means that the transfers on the DLT also result in a transfer of ownership in the relevant security. This law greatly increases legal certainty for keeping and transferring securities using DLT.

In a second step on 22 January 2021, Blockchain Act II amended the LFS and the Law of 6 April 2013 on dematerialised securities, enabled securities issuance accounts to be kept on a DLT platform and allowed foreign EU credit institutions and investment firms to act as central account keepers in relation to non-listed debt securities.

From 23 March 2023 onwards, the regulatory framework of the Regulation (EU) 2022/858 of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology (the DLT pilot regime), has been implemented in Luxembourg by the Law of 15 March 2023 (Blockchain Law III). The Blockchain Law III further modified the definition of financial instruments of the LFS and the Law of 30 May 2018 on markets in financial instruments (the MiFID II Law), clarifying that this concept includes financial instruments booked in securities accounts held on a DLT platform, ie, financial instruments within the meaning of MiFID II, which are issued, recorded, transferred and stored using DLT. This law also confirmed that financial collateral arrangements on securities held in securities accounts on the DLT benefit from the very protective regime of the law of 5 August 2005 on financial collateral arrangements, as amended.

The Circular CSSF 23/832's purpose is to apply the Guidelines of ESMA on standard forms, formats and templates to apply for permission to operate a DLT Market Infrastructure (Ref. ESMA70-460-213), published on 8 March 2023.

Additionally, and in light of the many questions surrounding DLT and blockchain, the Luxembourg regulator published on 24 January 2023 a white paper on DLT and blockchain to share its advice on assessing the risks when designing or implementing a project using DLT.

As regards the possibility to keep registers of nominative securities on DLT, which is particularly relevant in the investment funds industry, a position paper coordinated by the Luxembourg House of Fintech and prepared by the leading local law firms confirms the conditions under which this is possible. This possibility has also been recognised by the CSSF in the context of specific projects.

Crowdfunding

To develop crowdfunding platforms within the EU, Regulation (EU) 2020/1503 of 7 October 2020 on European Crowdfunding Service Providers for business (the Crowdfunding Regulation) has been adopted. The Crowdfunding Regulation has been directly applicable in all Member States since 10 November 2021 and was implemented in Luxembourg law by the law dated 25 February 2022.

The provision of crowdfunding services in Luxembourg requires a licence as European Crowdfunding Service Provider (ECSP). An ECSP providing services in Luxembourg is subject to the prudential supervision of the CSSF. If an ECSP intends to expand its scope to include payment services in addition to crowdfunding services, it may be necessary to apply for a distinct licence under the Payment Services Law.

To further foster the fintech environment in Luxembourg, the regulator complements the existing laws with soft law regulations, such as white papers, FAQs, non-binding guidance, position papers, etc. Some that are worth mentioning are in relation with the following subjects.

Artificial intelligence

The Luxembourg regulator has undertaken a comprehensive research initiative aimed at gaining a deeper understanding of artificial intelligence (AI) and its associated risks. The outcome of this effort is a non-binding white paper published on 21 November 2018, crafted to provide basic knowledge insights into AI, its various categories and practical applications relevant to the financial industry.

Moreover, the study encompasses an examination of the primary risks inherent in AI technology and provides recommendations for consideration when integrating AI into operational processes. Recognising the growing importance of AI adoption within the financial sector and the lack of practical guidance, the CSSF has opted to make the findings of this study accessible to the public, with the aim of benefiting the financial industry and foster constructive dialogues between the actors.

In October 2021, the CSSF and the Banque Centrale du Luxembourg launched a joint survey to gather information about the usage of AI, particularly in relation to machine learning. On 3 May 2023, the *Thematic review on the use of Artificial Intelligence in the Luxembourg Financial sector* was published, offering insight on the level of adoption and implementation of AI by the supervised institutions, as well as its challenges and trustworthiness.

Robo-advice services

Even though there is no commonly accepted definition and regulation of robo-advice, in Luxembourg, the provision of such digital financial advice services is subject to the same regulatory requirements as investment advice services provided via traditional means such as authorisation requirements from an investment firm and the rules of conduct deriving from MiFID. The Luxembourg regulator recognises, in its position paper on robo-advice published on 27 March 2018, that the emergence of such services needs further appropriate supervisory approaches.

Fintech support initiatives

With its long history of innovation, Luxembourg is committed to developing new ideas and fintech companies on its territory – not only through the environment of its pioneering regulatory framework, but also by providing rich support to fintech pioneers in the financial industry. Thus, Luxembourg has a dedicated national fintech platform, the Luxembourg House of Financial Technology (the LHoFT), bringing together innovators, financial institutions, researchers and academics, and also public authorities, in order to foster the development of this industry.

Working groups run by industry associations such as the Association of the Luxembourg fund industry (ALFI) and the Luxembourg Bankers' Association (ABBL), engage in the further development of such industry.

There are already quite a few examples in which Luxembourg financial institutions have developed their own fintech programmes.

2. Regulations on crypto assets: please provide a summary of the legal framework of crypto assets in your country and how crypto assets are regulated in your jurisdiction.

In terms of crypto assets, different legal frameworks apply to 'traditional' crypto assets (such as Bitcoin) – ie, not qualifying as financial instruments – and crypto assets qualifying as financial instruments.

For 'traditional' crypto assets, Luxembourg has implemented European directives on the fight against money laundering and terrorism financing and part of the Financial Action Task Force (FATF) recommendations in the AML/CTF Law. The AML/CTF Law has introduced a registration requirement for any natural or legal person, including entities already holding a financial licence, providing services in relation to crypto assets (ie, operating an exchange platform, custody of crypto assets, etc) and are subject to the same anti-money laundering requirements as traditional financial service providers. The CSSF supervision is limited to AML/CTF matters and the registration does not grant passporting rights to provide services into other EU countries.

The CSSF has also published two very helpful FAQ documents clarifying how credit institutions and investment funds (UCIs) may engage in activities linked to crypto assets.

In the FAQ document relating to credit institutions, the CSSF clarifies that credit institutions may offer custody services in relation to crypto assets and that customer crypto assets held in custody must be booked off balance sheet. The CSSF also explains how credit institutions may work with sub-custodians and how this impacts the liability towards clients. The CSSF also confirms that virtual assets do not amount to financial instruments, but that credit institutions are expected to apply a similar level of investor protection measures, eg, in terms of best execution, suitability and appropriateness and risk information. The CSSF also requires that credit institutions that offer services or transact in virtual assets need the corresponding knowledge, competence and expertise, infrastructure and human resources, at the operational, internal control and management levels. The CSSF also provides details on how credit institutions may act as depositaries for regulated investment funds investing in virtual assets.

In the FAQ document relating to undertakings for collective investments (UCIs), the CSSF clarifies which types of investment funds may invest in virtual assets, as well as the conditions for a Luxembourg investment fund manager to be able to act as such for investment funds investing in virtual assets. Finally, these FAQs also contain considerations on AML/CTF aspects.

Finally, in 2024, two pan-European regulations will enter into application: Regulation 2023/1114 on Markets in Crypto Assets (MiCA) and Regulation 2023/1113 on information accompanying transfers of funds and certain crypto assets. MiCA will provide an EU-wide comprehensive regulatory framework for crypto asset services and providers, as well as for the issuance of crypto assets other than financial instruments. MiCA will be the cornerstone of crypto asset services regulation and will bring a yet largely unregulated industry into the regulated space. Henceforth, crypto asset service providers will be regulated and benefit from cross border passporting rights throughout the

European Union while being obliged to apply wide-ranging investor protection rules, eg, in the area of custody and safekeeping of crypto assets.

For crypto assets qualifying as financial instruments, the Luxembourg legislator has adopted three 'blockchain laws' to streamline the issuance, custody, transfer and collateral arrangements on financial instruments booked on DLT, as described in more detail above in Question 1. These laws are not of EU origin and are thus unique to Luxembourg. They allow regulated entities like banks and investment firms to use DLT while benefiting from legal certainty. Major international banking groups have already used these laws for major bond issuances.

In addition to the blockchain laws, there is a very helpful publication prepared jointly by all major law firms which confirms the possibility to hold registers of registered securities on DLT. This is a view which is also shared by Luxembourg authorities including the CSSF. As a result, this opens up numerous possibilities for the asset management industry to keep fund registers using DLT and use DLT in the fund distribution space. It is worth noting that the CSSF has already granted a license to a regulated registrar agent to keep fund registers using DLT.

Accordingly, there is not only an adapted legal and regulatory framework in Luxembourg for the use of DLT by the financial industry, but also already several concrete projects by major market participants making use of the possibilities offered by such laws.

3. Payment service providers and digital wallets: please describe how payment service providers and/or digital wallets are regulated in your country. Please mention any foreseen law or regulation in this respect.

Payment institutions (PI), electronic money institutions (EMI) and account information service providers (AISP) are regulated by the Payment Services Law. The Payment Services Law was amended by the Law of 20 July 2018 which transposed Directive (EU) 2015/2366 of 25 November 2015 on payment services in the internal market (PSD2) into Luxembourg law.

The Payment Services Law permits for an exemption from the licensing requirement in relation to a 'specific payment instrument that can be used only in a limited way'. Such a specific payment instrument is defined as instrument enabling either (1) the purchase of goods or services exclusively within the issuer's premises or within a restricted network of merchants or (2) the acquisition of a very limited array of goods or services, such as gift cards, meal vouchers or membership cards.

Notification requirements apply in certain circumstances when making use of this exemption. With the publication of the CSSF Circular 22/812 adopting the EBA Guidelines on limited network exclusion under Directive 2015/2366 (EBA/GL/2022/02), the CSSF wishes to highlight the obligation imposed on issuers of specific payment instruments that can be used only in a limited way on their obligation to notify the Luxembourg regulator of their use of the limited network exclusion as per the Payment Services Law.

For instruments that can be used from and in Luxembourg for which the total value of the payment transactions executed over the last 12 months exceeds the amount of €1m, there is a notification obligation regardless of whether the issuer of such instrument is under the supervision of the CSSF or not, as well as whether it is part of the financial sector or not.

The proposal for the Payment Services Directive 3 (PSD3) is currently being prepared at the level of EU institutions. This will have an impact on Luxembourg payments laws and regulations in the next two to three years.

4. Special support to fintechs: does your jurisdiction provide any special programme supporting fintech ecosystem, in particular fintech startups (eg regulatory sandboxes, accelerator programmes). Are such programmes supported by the regulator in your country?

The support of fintechs in Luxembourg is levied by different associations.

The LHoFT is in charge of building and fostering the fintech ecosystems. The LHoFT brings together financial institutions, fintech innovators, research, academia and public authorities to help drive forward the development of (financial) products, which meet specific industry needs. The LHoFT hosts over 175 companies revolving around the fintech sector.

The Luxembourg Blockchain Lab is a common initiative between Infrachain, the LHoFT, LIST, SnT and Letzblock to create and nurture the blockchain ecosystem in Luxembourg. The call for project is the first initiative launched to start building the collaboration and have a dedicated entity. The aim is to promote blockchain in Luxembourg and help reduce inefficiencies via the use of blockchain.

In addition to the foregoing, there are dedicated working groups initiated by industry associations of traditional finance, such as the Association of the Luxembourg Fund Industry (ALFI) and the ABBL.

There are several other accelerators and incubators present in Luxembourg. The University of Luxembourg also leads several research projects in the fintech space.

The Luxembourg regulator, the CSSF, also actively engages with fintech topics and promoters of fintech projects and provides helpful guidance to the local industry.

There is no sandbox programme available in Luxembourg considering the limited size of the local market.

5. Open banking: please advise whether in your jurisdiction there are regulations on open banking. If the response is no, please provide any reference to regulations that may directly or indirectly affect open banking. Please include any foreseen laws and regulations on open banking.

There is no separate regulation on open banking. However, the practice of banks sharing data on their customers with other services providers falls under several existing regulations that affect open banking.

PSD2 requires institutions offering payment accounts which are accessible online to offer access to account related data to third party providers upon request of the client. PSD2 also introduced a framework for two new payment services related to 'open banking':

- account information service providers (AISPs), who can only provide the service of collecting information on one or more payment accounts (eg, aggregating payment accounts to analyse a company's cash flow or allowing consumers to view their various bank accounts on a single platform); and
- payment initiation service providers (PISPs), who initiate a payment order for an account held with another provider at the user's request.

In their development of application programming interfaces (APIs) to enable the access to account data, institutions must comply with EU-wide regulatory technical standards (RTS) adopted in March 2018 by Delegated Regulation (EU) No 2018/389, which are directly applicable in domestic law. Helpful guidance has also been provided by the EBA.

Open banking is also subject to the General Regulation on Data Protection (GDPR).

Although not specifically linked to open banking, it is worth mentioning that the upcoming EU Digital Operational Resilience Regulation (DORA) will introduce new requirements to manage cyber risks and increase resilience against such risks.

The open banking rules are expected to increase in scope. With the proposal for a Regulation on a framework for Financial Data Access (FIDA) at EU level, the sharing of financial data will become the norm and go well beyond mere payment account data. FIDA will not only bring additional regulated entities in scope (eg, banks, management companies, AIFMs) but also increase the type of data that will be subject to mandatory sharing in relation to loans, investments in financial instruments, insurance-based investment products, crypto assets, real estate and other related financial assets. Data collected for the purposes of carrying out an assessment of suitability and appropriateness and credit assessments will also be in scope.

There are also first proposals for PSD3 and the Payment Services Regulation (PSR). PSR will contain rules on open banking which will take over certain PSD2 rules and related RTS, while amending them on specific points. Some of the key shifts of PSR will be to require account servicing payment service providers to offer users a permission dashboard to easily manage and withdraw permissions for access to their data. Some requirements will be eased: eg, account servicing payment service providers will no longer need to offer an additional backup interface for possible disruptions.

Malta

Leonard Bonello*
Ganado Advocates, Valletta
lbonello@ganado.com

James Debono†
Ganado Advocates, Valletta
jdebono@ganado.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

Having been one of the first European jurisdictions to devise a comprehensive fintech regulatory framework, in Malta one finds various pieces of legislation which relate to financial innovation. Some of the said legislation originated domestically at the initiative of the Maltese legislator, while others have served to give effect to various European Union regulations and directives. The most relevant among such legislation are summarised below.

Virtual Financial Assets Act, Chapter 590 of the Laws of Malta (VFAA)

The VFAA regulates initial virtual financial asset offerings and services which are provided in relation to virtual financial assets (VFA). Such term is defined in the VFAA and generally refers to crypto assets which depend on or use distributed ledger technology (DLT) and which do not qualify as a financial instrument, electronic money or a virtual token, ie, an unlisted, unconvertible utility token.

The Malta Financial Services Authority (MFSA) has introduced a bespoke financial instruments test, which facilitates the determination of whether a DLT asset qualifies as a VFA or otherwise and therefore whether such asset falls either:

- within the purview of the VFAA;
- within the purview of the Financial Institutions Act which in turn regulates electronic money;
- whether it qualifies as a financial instrument and falls within scope of the Prospectus Regulation (Regulation (EU) 2017/1129) and/or the Markets in Financial Instruments Directive II (2014/65/EU) (MIFID II); or
- whether it is out of scope of any domestic or European legislation.

---

* Leonard Bonello is a partner within Ganado Advocates' banking and finance team, assisting credit institutions, electronic money institutions and payment institutions in regulatory and other matters including ongoing capital markets issues. Leonard also heads the fintech group at the firm and is involved in assisting a number of blockchain-based projects. He assists financial institutions extensively in financing transactions and other banking operations with a particular focus on derivative contracts. Leonard is also a visiting lecturer and examiner at the University of Malta.

† James Debono is an associate within Ganado Advocates' banking and finance team, assisting institutional as well as start up clients on various regulatory matters, particularly in the fintech space, particularly payment and e-money institutions, credit institutions, blockchain and crowdfunding platforms. Besides being involved in financing transactions, James advises clients on corporate matters including formation of companies, corporate governance, and general company law.

Akin to virtual tokens, the issuance, admitting to trading or the provision of services in relation to non-fungible tokens (NFTs) which display clear characteristics of uniqueness and non-fungibility, are excluded from the VFA framework.

Under the VFAA, for an issuer to offer a VFA to the public in or from within Malta or to apply for a VFA's admission to trading on a DLT exchange, it must inter alia appoint a VFA agent (a statutory licensed intermediary between issuers or VFA service providers and the MFSA) and prepare a VFAA-compliant white paper which is submitted to the MFSA prior to publication.

The VFAA also regulates the provision of MIFID II-type services in or from Malta and in relation to VFAs, including dealing on own account, portfolio management, custodian and nominee services, investment advice, placing of VFAs, operating a VFA exchange and transferring VFAs. For a person to provide or hold themselves out as providing any of these services in or from Malta (VFA service provider), they must obtain a licence from the MFSA which is subject to several prerequisites including the establishment of a Maltese entity, satisfying specified minimum capital requirements, appointing various functionaries and undergoing MFSA-conducted assessments. In turn, the Virtual Financial Assets Regulations (Subsidiary Legislation 590.1 of the laws of Malta) inter alia set out a number of exemptions from licensing for VFA services.

To supplement the abovementioned legislation, the MFSA has issued a Virtual Financial Assets Rulebook, which is split into three chapters addressing the following:

- Chapter 1: VFA rules for VFA agents;
- Chapter 2: VFA rules for issuers of VFAs; and
- Chapter 3: VFA rules for VFA service providers

On 16 May 2023, the EU Council formally approved the new Markets in Crypto Assets Regulation (MiCAR) which aims to establish a harmonised regulatory framework for crypto assets at EU level. Malta does not envisage any major headaches relating to the direct applicability of MiCAR, since the Maltese framework and MiCAR share several comparable principles and provisions. VFA service providers in Malta are expected to transition effortlessly from their current VFA licence to the new MiCAR-compliant licence. In anticipation of MiCAR coming into force, the MFSA has already issued a consultation document and a draft Chapter 3 of the Virtual Financial Assets Rulebook updated with provisions aligning the framework with MiCAR.

Crowdfunding Service Providers Act, Chapter 637 of the Laws of Malta (CSPA)

Following the coming into force of Regulation (EU) 2020/1503, the previous crowdfunding regulatory regime was replaced by a licensing and regulatory framework specifically targeting investment-based and lending-based crowdfunding service providers. Malta has also recently introduced the CSPA as a tailor-made regime for the regulation of crowdfunding, which essentially gives effect to Regulation (EU) 2020/1503. Reward-based and donation-based crowdfunding remain unregulated in Malta.

The CSPA sets out the authorisation requirements for the provision of crowdfunding services in Malta. It also sets out the ongoing obligations of crowdfunding service providers and project owners,

delineates the requirements relating to the operation of crowdfunding platforms, and provides for transparency and marketing communications in relation to such services in the EU.

Prior to the CSPA coming into force, the MFSA had issued the MFSA Crowdfunding Rules which set out technical standards and marketing requirements. These Rules continue to supplement the current legislative framework. Furthermore, the European Securities and Markets Authority (ESMA) has published the draft technical standards on crowdfunding under Regulation (EU) 2020/1503.

The Financial Institutions Act, Chapter 376 of the Laws of Malta (FIA)

The FIA sets out the licensing and ongoing obligations of non-banking institutions. The activities of such institutions may be classified into two categories:

1. payment services or the issuance of electronic money; and
2. activities such as lending, financial leasing, the provision of guarantees and commitments, foreign exchange services and money brokering.

The FIA, and the subsidiary legislation enacted thereunder, transposed into Maltese Law Directive (EU) 2015/2366 (PSD2) and Directive 2009/110/EC (EMD2). The MFSA was at the forefront during the transposition of EU Directives and has been involved in the regulation and supervision of various fintech-related products. Malta currently has 52 licensed financial institutions (be it payment institutions or e-money institutions) with a number of additional institutions in the pipeline.

Akin to the VFAA framework, financial institutions providing the payment services listed under PSD2, electronic money services as outlined in EMD2, or other services listed under the FIA (such as lending), in or from Malta on a regular and habitual basis are also subject to an authorisation requirement by the MFSA. Such licence is subject to a number of conditions, including the establishment a local presence in Malta, appointment of a number of functionaries and statutory capital requirements.

The Banking Act, Chapter 371 of the Laws of Malta

The Banking Act regulates credit institutions carrying out the 'business of banking' in or from Malta. The 'business of banking' is defined as (1) the acceptance of deposits of money from the public that are withdrawable or repayable on demand or after a fixed period or after notice; (2) the borrowing or raising money from the public for the purpose of using such money, in whole or in part, to lend to others; or (3) otherwise investing for the account and at the risk of the person accepting this money.

The Investment Services Act, Chapter 370 of the Laws of Malta (ISA)

The Markets in Financial Instruments Directive II (2014/65/EU), which was transposed into Maltese law via the ISA, harmonises the requirements with which MIFID II firms are bound at EU level. The ISA regulates the services outlined therein when they are transacted in or from Malta and in relation to one or more 'instruments' as is defined in the ISA. It also outlines the regulatory

requirements of operators setting up investment services undertakings and collective investment schemes in Malta.

The Insurance Business Act, Chapter 403 of the Laws of Malta (IBA)

The IBA regulates the business of insurance: namely, effecting and carrying out contracts of insurance for long-term business or general business. The IBA also deals with the authorisation for carrying on the business of insurance, as well as the conditions which are imposed for carrying on such business.

The Innovative Technology Arrangements and Services Act, Chapter 592 of the Laws of Malta (ITAS)

ITAS provides for the regulation of designated innovative technology arrangements (ITA) and services found in the Act, and for the exercise of regulatory functions by the Malta Digital Innovation Authority. ITAS describes the type of ITA falling within its purview and includes smart contracts, software which is used in designing and delivering DLT, and software and other architecture used as a stand-alone solution or part thereof in sectors which are deemed to be of a risky or critical nature. One can apply for a voluntary certification of such agreements or services for one or more specified purposes, these being: qualities, features, attributes, behaviours or aspects. Once certified, one is obliged to adhere to the rules set out in the ITAS and in the MDIAA. ITAS also stipulates requirements for the registration of persons offering innovative technology services which include technical administrators and system auditors whose role it is to confirm the compliance of ITAs with certain standards.

The Malta Digital Innovation Authority Act, Chapter 591 of the Laws of Malta (MDIAA)

In 2018, the MDIAA established the Malta Digital Innovation Authority whose main objectives and policies include the deployment of ITA within the public administration, fostering and facilitating the advancement and utilisation of ITA, promoting education on ethical standards of innovative technology, harmonising practices, etc. This authority serves as the regulator who is inter alia responsible for processing applications for the voluntary certification of ITA and services relating thereto.

Artificial intelligence (AI)

Currently, AI remains unregulated in Malta. Nevertheless, the Maltese government established a Malta AI task force, which introduced the Strategy and Vision for Artificial Intelligence in Malta 2030. This initiative has positioned Malta as one of the leading jurisdictions with a significant national AI program. Meanwhile, the EU has released its Proposal on Artificial Intelligence, wherein the use of artificial intelligence in the EU will be regulated by the AI Act, the world's first comprehensive AI law.

Data protection

The processing and transmission of personal data is regulated under the Data Protection Act, Chapter 586 of the Laws of Malta. This Act incorporates the provisions of the EU General Data Protection Regulation (Regulation (EU) 2016/679) and is complemented by Subsidiary Legislation 586.01 of the laws of Malta which addresses the processing of personal data within the realm of electronic communications. This subsidiary legislation transposed EU Directive 2002/58/EC into Maltese Law.

Cloud computing

Several initiatives, both at local and European levels, aim to regulate the development of cloud computing. However, these initiatives are not necessarily tailored to the financial services sector. Locally, the Malta Communications Authority has released a guidance document called *Cloud Computing Guidelines for SMEs and Microenterprises* which outlines factors that small and medium-sized enterprises and microenterprises should consider when evaluating the suitability of using cloud computing in their businesses. The document also analyses the contractual implications of engaging with cloud computing service providers.

The MFSA has issued a guidance note titled *Technology Arrangements, ICT and Security Management, and Outsourcing Arrangements* which sets forth requirements regarding the adoption of cloud computing resources and services. Additionally, the MFSA has provided guidance on software-as-a-service as an outsourcing arrangement, offering practical recommendations for licence holders in their approach to this matter. Furthermore, the ESMA Guidelines on Outsourcing to Cloud Service Providers have been incorporated into various MFSA Rulebooks.

In compliance with EU Directive 2016/1148/EU, Subsidiary Legislation 460.35 defines cybersecurity standards and establishes the Critical Information Infrastructure Protection Unit (CIIP Unit).

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

Malta's reputation as the 'Blockchain Island' primarily hinges on it having been a pioneer in regulating Distributed Ledger Technology and cryptocurrency, namely through the enactment of the VFAA, the MDIAA and ITAS. A thorough analysis of these legislations can be found in Question 1.

Anti-money laundering (AML)

The regulatory framework governing AML in Malta primarily constitutes of the Prevention of Money Laundering Act, Chapter 373 of the Laws of Malta (PMLA) and the Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR), Subsidiary Legislation 373.01. These are buttressed by the Implementing Procedures published by the Financial Intelligence Analysis Unit. Such laws transposed the EU's Fourth Anti-Money Laundering Directive as amended by the Fifth Anti-Money Laundering Directive (AMLD5) into Maltese Law. Through AMLD5 the European

Union extended the scope of its AML regime to cover providers of exchange services between virtual currencies and fiat currencies, and custodian wallet providers. Maltese law is already in line with the provisions of the Sixth Anti-Money Laundering Directive. The PMLFTR stipulates that VFA issuers (both within the context of a public offer and an admission to trading of VFAs) and VFA service providers qualify as subject persons, therefore must abide by AML legislation, and must have in place measures, policies and procedures in place (including the appointment of a money laundering reporting officer) to address identified AML risks.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

As outlined above, the main legislation regulating payment service providers and electronic money services in Malta is the FIA which transposes PSD2 and EMD2 into Maltese law. The First and Second Schedule to the FIA set out a list of activities which are licensable under the FIA and which, amongst other services, transposes Annex I of PSD2 into Maltese law and provisions of EMD2.

An entity intending to provide such activities regularly or habitually in or from Malta must first obtain a licence from the MFSA, unless it has already been validly authorised to carry out such activities by the relevant regulator in another EU Member State and is passporting its activities to Malta. By way of exception, no licence is required by an entity which intends to solely transact account information services, but such entity must nevertheless obtain a registration granted by the MFSA. The FIA also sets out a list of activities which are exempt from the abovementioned licensing requirements.

Similarly, electronic money institutions require a licence granted by the MFSA or a regulator within the EU to carry out any of the activities listed in the Third Schedule to the FIA which sets out the activities that may be undertaken by financial institutions which issue electronic money. By way of example, the FIA provides that apart from the issuance of electronic money, an electronic money institution may also provide: (1) payment services as listed in the Second Schedule to the FIA; (2) operational services and closely related ancillary services in respect of the issuing of electronic money or to the provision of payment services; (3) the operation of payment systems; and (4) business activities other than the issues of e-money.

The payment regulatory landscape in the EU is currently undergoing an internal re-evaluation and assessment to revamp the ecosystem and keep up with technological advancements. The European Commission launched three consultation documents in May 2022 to collate information and evidence in pursuance of revising PSD2; the European Banking Authority (EBA) had issued an Opinion and Report in June 2022 which included more than 200 proposals covering different areas for the revision of PSDII, which include merging PSD2 and EMD2, clarifying the application of strong customer authentication (SCA) and the transactions in scope and adjusting specific prudential requirements.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

Fintech Regulatory Sandbox

The Fintech Regulatory Sandbox was introduced by the MFSA back in 2020 through MFSA Rule 3 – The MFSA Fintech Regulatory Sandbox, which provides for an environment where regulated and unregulated fintech service providers, as well as technology providers, may test their innovation from a regulatory perspective for a specified period within the financial services sector, under certain prescribed requirements, while being in close contact with the regulator. This allows for a better understanding of the adoption and implications of the fintech product within the financial services market and creates an environment in which one can monitor the product's adherence with legal requirements so that regulatory gaps or risks can be identified and addressed effectively.

To participate in the sandbox, one must demonstrate that the solution being proposed is technologically enabled, innovative, and that there is a genuine need to test the solution in the sandbox. Additionally, the product in question must provide identifiable value and be economically sustainable.

Having received feedback from the industry regarding the sandbox and consolidated best practices adopted by other regulatory sandboxes, the MFSA has recently published revisions to the Fintech Regulatory Sandbox.

MFSA Fintech Adoption Study

The MFSA conducted a Fintech Adoption Study which focused on digital transformation and financial technology adoption within the Maltese financial services sector. The study analysed 390 authorised persons, allowing the MFSA to further understand whether such authorised persons have a digital transformation strategy and, if so, which technologies and innovations they employ.

The Malta Gaming Authority's Sandbox Regulatory Framework

In 2019, the Malta Gaming Authority (MGA) launched a sandbox framework for the acceptance of cryptocurrencies and the use of DLTs by its licensees. This allows authorised persons to accept VFAs as a payment method and permits them to use ITAs, DLT platforms and smart contracts. In 2023, the MGA also published an updated policy on the use of DLTs by authorised persons. This further regulates DLT assets, ITAs and smart contracts to strengthen the role of DLTs in the gaming industry.

The ITA Sandbox

The Malta Digital Innovation Authority (MDIA) launched the Technology Assurance Sandbox back in 2021. This sandbox caters for startups, smaller players or other entities seeking to

develop their innovative digital product or service, by enabling such entities to work closely with the MDIA in identifying technological gaps in the product and reviewing its functional correctness and reliability and the underlying operational processes. This is intended to increase confidence in stakeholders.

MFSA's fintech and innovation function

Expanding upon the MFSA's 2019 fintech strategy, the MFSA has set up a dedicated fintech and innovation function which is responsible for the regulatory framework dealing with technology-enabled financial innovation. Such function is responsible for offering regulatory guidance, putting forward initiatives which facilitate innovation and collaborating with stakeholders.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

Despite the lack of laws promoting competition among financial institutions through the use of available data, the concept of open banking has locally been introduced through the FIA by regulating third-party payment service providers – namely, payment initiation service providers and account information service providers, which services are in turn based on access by third party providers (TPPs) to customer data.

In its PSD2 review, the EBA suggests moving from the concept of open banking to that of open finance, which in turn refers to the expansion from access to payment accounts data towards access to other types of financial data (such as savings, investments and insurance data). The EBA has highlighted that this move will foster advancements within the financial industry, ultimately serving consumers and the broader financial environment.

The Netherlands

Jibraeel Mussani
Stibbe, Amsterdam
jibraeel.mussani@stibbe.com

Roderik Vrolijk
Stibbe, Amsterdam
roderik.vrolijk@stibbe.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

As a principle, legislation in the Netherlands is technology neutral. Financial regulatory laws are based on the same activity, same risk and the same regulatory principle. Activities are regulated irrespective of the use of technology by the service provider. Accordingly, the Dutch fintech regulatory framework lacks a uniform and harmonised character. To date, the Dutch legislator has mostly adapted the existing rules applicable to traditional banking and financial services and implemented European Union Directives directed at particular segments of the fintech industry (eg, crypto asset services providers, electronic money institutions and payment institutions).

The key laws and regulations that apply to fintech companies in the Netherlands (in addition to EU regulations which apply directly (eg, the GDPR and the EU Crowdfunding Regulation)) are:

- the Dutch Financial Supervision Act (*Wet op het financieel toezicht* or WFT), which governs the oversight of the entire financial sector in the Netherlands. The WFT includes rules and regulations for financial markets, including licensing and information requirements, as well as their supervision. The WFT also implements various EU sectoral directives (eg, the second Payment Services Directive (PSD2), Solvency II, and the fifth Capital Requirements Directive (CRD V));
- the Dutch Anti-Money Laundering and Anti-Terrorist Financing Act (*Wet ter voorkoming van witwassen en financieren van terrorisme* or WWFT) provides rules to prevent the utilisation of the financial system for money laundering or the funding of terrorist activities, and provides for a registration requirement for crypto-asset services providers; and
- the Dutch Sanctions Act 1977 (*Sanctiewet* 1977) is a piece of umbrella legislation under which national and international rules are implemented in compliance with international sanctions regulations.

These laws are supplemented by decrees and guidance of the Dutch financial supervisory authorities the Dutch Central Bank (De Nederlandsche Bank or DNB), the Netherlands Authority for the Financial Markets (Stichting Autoriteit Financiële Markten or the AFM), the Dutch Data Protection Authority (Autoriteit Persoonsgegevens or the DPA), and the Netherlands Authority for Consumers and Markets (Autoriteit Consument & Markt or the ACM).

The regulation of the financial sector is constantly evolving. Future regulations, applicable in the Netherlands, which are of particular interest to the fintech industry are:

- Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA);
- Regulation (EU) 2023/1114 on markets in crypto assets, amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (MiCAR);
- the Proposal for a Regulation on information accompanying transfers of funds and certain crypto assets (recast) (COM/2021/422 final); and
- the Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (the Artificial Intelligence Act).

Given the comprehensive and still-expanding nature of financial regulation, careful analysis of applicable regulatory regimes is indispensable prior to starting any fintech business in the Netherlands.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

The Fifth Anti-Money Laundering Directive (AMLD5) has been implemented in the WWFT. Effective as of 2020, crypto service providers (ie, exchange services and the provision of custodian wallets) must request registration with DNB prior to providing crypto services in or from the Netherlands.

- A provider offers exchange services when it effects transactions or enables customers to effect transactions in which virtual currencies are exchanged for fiduciary currencies or vice versa.
- A custodian wallet provider is defined in the WWFT as an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store, and transfer virtual currencies.

The WWFT defines a virtual currency as:

> 'a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically'.

Crypto service providers are required to register if the services they provide are in scope of the WWFT and are provided in a professional capacity, or on a commercial basis in or from the Netherlands.

The explanatory memorandum clarifies that, for an activity to be carried out in a professional capacity or on a commercial basis within the meaning of the WWFT, it must be more than an occasional activity and the provider must receive remuneration or generate income from it. The activity must therefore be performed systematically or regularly. Occasional or one-off activities do not qualify as activities carried out in a professional capacity or on a commercial basis. The activities do not need to be profitable. Moreover, they do not need to be the provider's main activity to fall

within the scope of the WWFT. Other indicators can be the fact that a provider advertises for the services or provides them to multiple customers.

In principle, entities operating from a country that is not an EU Member State cannot register with DNB. Entities established in a third country that wish to provide these services in the Netherlands must establish a presence in the Netherlands or another Member State and apply for registration with DNB. If they fail to do so, they are in non-compliance with the WWFT, and DNB can take enforcement action.

Further to this, it follows from case law that reverse solicitation cannot be relied upon in the context of crypto services.

As of 2025, MiCAR will substantially affect the current regulatory landscape in the Netherlands and will provide for a uniform regulatory regime for crypto services providers. MiCAR will introduce a licence regime for crypto services providers and will enable crypto services providers to passport their licence across the EU.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

The Netherlands has implemented the second Payment Services Directive (PSD2) and the second Electronic Money Directive (EMD2). In general, the Dutch implementation of PSD2 closely mirrors the wording of the directive. PSD2 only provided for a few Member State options and the Netherlands opted to use only a few of those.

Anyone providing payment services in the Netherlands must have obtained prior authorisation from DNB, or must have been exempted from the authorisation requirement. Authorised banks and electronic money institutions are permitted to provide payment services to the extent that this is permitted under the authorisation concerned; they do not require separate authorisation for the provision of payment services.

It should be noted that DNB is not the only supervisory authority that supervises compliance with PSD2 in the Netherlands. The DPA, AFM and ACM are also relevant in this regard. The AFM supervises compliance with business conduct rules, the DPA monitors compliance with the GPDR, and the ACM is in charge of supervision in respect of compliance with PSD2 from a competition law perspective. This makes compliance with PSD2 particularly complex.

Further regulation is being contemplated, namely:

- the Proposal for a Directive of the European Parliament and of the Council on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC and a related regulation (PSD3). The implementation of PSD3 is not expected to take place before 2026.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

In July 2020, the former Dutch Minister of Finance presented the FinTech Action Plan to the Dutch House of Representatives based on the first Dutch FinTech Census 2019. The action plan contains three different lines of action, which in their turn have been divided into more concrete goals and points of action:

1. putting the Dutch fintech sector on the map, both nationally and internationally;
2. ensuring good access to knowledge and talent for fintech companies;
3. ensuring regulations are ready for the future and offer room for innovation.

In 2021, the Dutch Minister of Finance announced that a large proportion of the announced actions have made progress and a number of actions have even been completed.

Following the Fintech Action Plan, DNB, the AFM and the ACM established the InnovationHub. The InnovationHub is not a regulatory sandbox in which laws and regulations are (temporarily) set aside or waived. However, the InnovationHub:

- provides explanation and consultation on specific supervisory rules and policies in each stage of a company's innovation process;
- helps companies to get in touch with the right regulator;
- provides information on the scope of supervision; and
- provides insight into innovative developments within the regulators that could potentially support a company's innovations, for example innovation in information exchange between the company and their regulators.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

There is no specific regulation on open banking in the Netherlands in addition to the limited European regulation in this field.

The practice of banks sharing data in respect of their customers with other services providers falls under several existing regulations that affect open banking, most notably PSD2.

PSD2 was an important first step into open finance, and requires banks to provide mandatory access to payment accounts to providers of payment initiation services and/or account information services. PSD2 draws a fundamental distinction between payment initiation service providers (PISPs), which are enabled to provide payment initiation services, and account information services providers (AISPs), which are enabled to provide accounting information services, as well as account servicing payment service providers which manage the payment account.

In the EU Digital Finance Package, the European Commission identified the creation of a European financial data space as a priority. This will entail a move from 'open banking' to 'open finance'. The EU Digital Finance Package sets the framework for such transition and identifies the hurdles to achieve this. PSD3 is also likely to positively impact open banking across EU Member States.

In 2022, the Dutch Ministry of Finance conducted a national evaluation of the Dutch implementation of PSD2.

The national evaluation of PSD2 led to the following general observations:

- PSD2 has contributed positively to competition in the payments market and to a more unified single European payments market;
- PSD2 has contributed positively to innovation in the payments market;
- PSD2 has contributed positively to the security of the payments chain;
- PSD2 has contributed positively to consumer protection; and
- PSD2, in combination with the General Data Protection Regulation (GDPR), offers adequate protection of privacy.

Based on the aforementioned results of the evaluation, the Dutch Ministry of Finance saw potential improvements to the existing payment data sharing provisions of the PSD2 framework and/or an effective general framework for open finance. These improvements were fed back to the EU legislator with the aim of addressing these shortcomings in PSD3.

Norway

Markus Kjelløkken*
Advokatfirmaet Thommessen, Oslo
mkj@thommessen.no

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation. Please also refer to any new law or regulation foreseen in the near future or any bill on fintech and financial innovation in your jurisdiction.

There is no specific legal framework for fintech companies in Norway. Depending on the type of service offered, the service may qualify as a regulated activity, which triggers a licence requirement under general Norwegian financial services legislation. The applicable rules and regulations will depend on the services offered by the fintech company.

Financial services regulation in Norway is based on and transposes the relevant financial services directives and regulations of the EU. In addition, Norway has certain national rules which go beyond what is required under EU directives and regulations.

Given the comprehensive nature of financial services regulation, any fintech business should obtain legal advice prior to launching in Norway.

Below is a list of key activities which trigger a licence or registration requirement. A fintech company intending to engage in one of the mentioned activities in Norway should either obtain such a licence, partner with another company which holds the relevant licence or rely on exemptions.

Financing activity (*finansieringsvirksomhet*)

Any granting of credits or loans as well as guarantees for own account (including financial leasing and factoring) is considered a financing activity which triggers a licence requirement in Norway. The licensing requirement for financing activities applies regardless of how the activity is funded (ie, whether it is funded by equity, bank loans or deposits) and regardless of whether the financing is provided to consumer or corporate borrowers.

There are exemptions from the licence requirements, but these are quite limited in scope. Key exemptions include: providing credit as a seller of goods or services, isolated cases of financing (ie, occasional financings), intra-group financing, investments in bonds/securities, reverse solicitation or being a financial agent/intermediary. Another key exemption is providing loans through a loan-based crowdfunding platform, provided that the total amount of financing provided by the

* Markus is a managing associate at Advokatfirmaet Thommessen. He works primarily with banking and financial services regulation, with a particular focus on fintechs and payment services. Markus regularly advises startups, fintechs, banks, insurers, intermediaries and other players in the financial sector and technology space. He advises clients with respect to fintech, technology, navigating the legal landscape, obtaining licenses, launching new products, negotiating agreements and partnerships, dealing with regulators and ensuring compliance with relevant requirements as well as achieving commercial goals.

lender through the platform does not exceed NOK 1m per year. There may also be other structural solutions to ensure compliance with the licence requirement.

If the licence requirement is triggered, there are extensive requirements, including governance and capital requirements based on the EU's capital requirements regulation (ie, the same capital requirements as ordinary banks).

The relevant legal act is the Norwegian Financial Undertakings Act (*finansforetaksloven*).

Loan mediation

Intermediation of loans, either as an agent for a bank/lender or as an independent broker, triggers a requirement to obtain permission as a loan intermediary (*låneformidler*), pursuant to the Norwegian Loan Mediation Act (*låneformidlingsloven*). The licence is subject to relatively light touch requirements, but includes suitability assessments of management and employees, as well as governance requirements such as internal policies and professional liability insurance.

Mediation of loans to corporates is exempt from the requirements in the Loan Mediation Act and is only subject to a very light touch registration requirement. Furthermore, with respect to corporates, the EUs crowdfunding-regulation is proposed to be adopted into Norwegian law but has not yet been adopted. Once adopted (no date set), this will entail that loan intermediation to corporates through crowd-funding platforms is subject to the EU crowdfunding regulation.

Loan-based crowdfunding

Loan-based crowdfunding is a sub-type of loan mediation (see above).

- *Financing to corporates*: currently only subject to a registration requirement pursuant to the Norwegian Loan Mediation Act, but will be subject to the EU crowdfunding regulation once adopted.
- *Financing to consumers*: subject to a requirement to obtain permission as a loan intermediary pursuant to the Norwegian Loan Mediation Act.
- *Special considerations regarding payment flow*: if the crowdfunding platform shall be an intermediary in the payment flow (eg, receive payment from lenders and forward to borrowers), this will often be considered a payment service triggering a separate requirement to obtain a licence as a payment institution.
- *Special considerations for lenders on the platform*: lenders on the crowdfunding platform may be at risk for providing a financing activity (as described above) and should therefore operate within the exemptions for lending through crowdfunding platforms as described above.

Receiving deposits

Receiving deposits from the public is subject to a requirement to hold a banking licence.

Payment services

Any provision of 'payment services' is subject to a requirement to obtain a licence as a payment institution. The rules in Norway transposes the EU's revised Payment Services Directive (PSD2). In essence, a payment service involves receiving monies from one party and forwarding to another. In addition, account information services and payment information services are regarded as payment services.

Issuing electronic money

Issuing electronic money is subject to a requirement to obtain a licence as an e-money institution. The rules in Norway are aligned with the EU-rules. Electronic money is defined as an electronically stored monetary value, represented by a claim on the issuer, that is issued on receipt of funds with the purpose of carrying out payment transactions, and that is recognised as a means of payment by entities other than the issuer.

Foreign exchange activity

Currency exchange services (eg, physical offices where customers can exchange currencies) is subject to a licence requirement in Norway.

Virtual currencies

A virtual currency is defined as 'a digital representation of value that is not issued or guaranteed by a central bank or a public authority, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically' (eg, Bitcoin). Any services offered in the Norwegian market involving the exchange between virtual currencies and fiat currencies is subject to a registration requirement for anti-money laundering (AML) purposes (due to the EU's AML Directives). Once registered, the company must comply with Norwegian AML rules.

Custodian wallet providers

Entities providing services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies, are subject to a registration requirement for AML purposes (the same as described above for virtual currencies).

Crypto assets

Services related to crypto assets are currently not regulated in Norway (other than virtual currencies and custodian wallet providers).

Certain crypto assets, such as some initial coin offerings and similar, may qualify as 'financial instruments' and thereby be subject to the ordinary Norwegian securities rules.

Crypto asset service providers will, once transposed into Norwegian law, be subject to the EU's Markets In Crypto Assets Regulation (MiCA) (from approximately 1 January 2025). Once transposed into law, MiCA sets out a comprehensive regime for so-called crypto asset service providers – ie, anyone offering defined services with respect to crypto-assets. Crypto assets are defined as 'digital representation[s] of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology'. This does not include non-fungible tokens or assets (NFTs).

Insurance and insurance mediation

Engaging in insurance activities (eg, offering insurance policies) is subject to a requirement to obtain a licence as an insurance company. Being an intermediary with respect to insurance is subject to a requirement to obtain permission as an insurance intermediary (although there are certain exemptions). The rules in Norway are aligned with the EU's Solvency II directive and the EU's Insurance Distribution Directive (IDD).

There are also other regulated activities such as investment services in relation to financial instruments and management of funds.

Generally, legal entities in the EU/EEA which hold a licence subject to EU rules may passport such licence into Norway and therefore do not need to obtain a separate licence in Norway.

If a licence or registration requirement is triggered, the company will need to apply to the Financial Supervisory Authority of Norway (NFSA) to obtain the relevant licence or registration. The company will need to demonstrate compliance with the requirements applicable to the relevant licence. In addition, companies will be expected to operate in line with good business practices vis-à-vis customers, and comply with customer-centric rules such as the Norwegian Marketing Control Act and the Norwegian Financial Contracts Act.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

Crypto assets are not specifically regulated in Norwegian law to this date.

However, providers of virtual currency exchange services and custodian wallet providers (as defined above) are subject to an AML registration requirement (as described above). The registration requirement pursuant to Norwegian AML rules applies if such provider:

- is registered in Norway;
- operates in Norway; or
- targets the Norwegian market.

Such service providers must be registered with the Financial Supervisory Authority of Norway (NFSA) and are subject to the full range of AML obligations including KYC, etc.

Some crypto assets may qualify as financial instruments and thereby be regulated by Norwegian rules and regulations regarding financial instruments (ie, ordinary securities and derivatives).

In terms of new rules, the EU has adopted Regulation (EU) 2023/1114 (Markets in Crypto Assets or MiCA), which is expected to apply in full from January 2025 in the EU. MiCA is expected to be implemented in Norway without significant delay compared to the EU date of effect.

4. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

The offering of 'payment services' is subject to a requirement to obtain a licence as a payment institution. The rules and definitions in Norway are aligned with the EU's revised Payment Services Directive (PSD2). In essence, a payment service involves receiving (ordinary fiat) monies from one party and forwarding to another. Examples include:

- services enabling cash to be placed or withdrawn on an account;
- execution of payment transactions, eg, transfer of funds from a payment account, direct debits, execution of card payments, credit transfers (both when the transaction is based on debit instruments and lines of credit);
- issuing payment instruments (eg, credit cards or other payment cards);
- acquiring payment transactions (eg, merchant acquiring services); and
- money remittance (eg, transfers of money between customers).

In addition, certain new types of open banking services (account information services and payment information services) are regarded as payment services (see Question 5).

To offer payment services, it is necessary to hold a licence as either a payment institution or a bank. Obtaining a licence is subject to compliance with capital requirements and requirements regarding organisational structure and internal procedures as well as governance. Payment institutions are required to safeguard funds by keeping payment funds separate from the service provider's own assets or holding relevant insurances/guarantees.

The following are key exemptions from the requirement to obtain a licence for payment services:

- **the commercial agent exemption**, ie, payment transactions from the payer to the payee through a commercial agent authorised via an agreement to negotiate or conclude the sale or purchase of goods or services on behalf of only the payer or only the payee;
- **technical service providers**, ie, services provided by technical service providers, which support the provision of payment services, without them entering at any time into possession of the funds to be transferred;
- services based on specific payment instruments allowing the holder to acquire goods or services only in the premises of the issuer or within a **limited network of service providers** (eg, gift cards to be used only within one single corporate group operating under the same trademark); and
- payment instruments which can be used only to acquire a very **limited range of goods or services** (eg, fuel cards or only very limited types of cards).

Such exempted services may still be subject to a requirement to notify the NFSA when reaching relevant thresholds connected to the value of payment transactions.

Provision of digital wallets is considered a payment service if the digital wallet includes payment services as defined above. If the provision of the digital wallet entails issuing electronic money (as defined above), the provider must have authorisation as an e-money institution.

The EU has proposed PSD III/the PSR (payment services regulation). Once adopted in the EU, this will thereafter be transposed into Norwegian law.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

Guidance service for fintech companies[1]

The NFSA has established a low-threshold service for guidance to fintech companies. The NFSA offers help to fintech companies regarding regulations, authorisation and filings. Guidance is available through e-mail or meetings with the company. The guidance service cannot process issues of principle, applications, or complaints.

NFSA Regulatory Sandbox[2]

The NFSA operates a regulatory sandbox available for fintech companies, regardless of whether the fintech company is a regulated entity. Both new and existing entities are eligible for the sandbox regime, subject to an application. To enter the regulatory sandbox the service and the entity must fulfil the following criteria:

- the service should be associated to regulated financial services that are supervised by the NFSA;
- the service should be of use to consumers or the financial system as a whole;
- the service should represent a technological innovation or something genuinely new;
- there has to be a need for the participation in the regulatory sandbox; and
- the entity and service must be ready to participate in the regulatory sandbox.

Regulatory Privacy Sandbox[3]

The Norwegian Data Protection Authority (NDPA) operates a sandbox that can be relevant for fintech companies. The sandbox accepts projects relating to privacy-friendly innovation

1 Information from the NFSA can be found at www.finanstilsynet.no/en/topics/fintech-and-regulatory-sandbox/guidance-service-for-fintechs/.

2 Information from the NFSA can be found at www.finanstilsynet.no/tema/fintech/finanstilsynets-regulatoriske-sandkasse/.

3 Information from the NDPA can be found at www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/.

and digitalisation. The NDPA and the NFSA have in the past cooperated in fintech projects accepted to the sandbox.

There are also commercial accelerator programs such as Antler.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

The Open Banking regime in Norway is based on the EU's PSD II. The two key types of fintech service providers meant to facilitate the open banking regime are payment initiation service providers (PISPs) and account information service providers (AISPs), who are third parties that can offer services relating to respectively:

- initiating payment transactions on behalf of the end user with respect to the user's online payment account (eg, in the end user's daily bank); and
- viewing and accessing all account information from the user's online payment accounts (across banks).

PISP/AISPs are permitted to offer open banking services without having any explicit agreement with the bank in question. There are common rules for APIs. The open banking regime is limited to 'payment accounts' and does not cover, for example, pension service providers or investments held in investment accounts, etc.

The technical requirements for AISPs and PISPs are set out in PSD2 and Commission Delegated Regulation (EU) 2018/389, as incorporated in Norwegian law. AISPs and PISPs are subject to light-touch licence requirements. The customer may in accordance with an agreement with an AISP or a PISP use services on their own accounts, provided such accounts are available online. The account provider (eg, banks) cannot set as a condition that there is a direct agreement between the bank and the AISP/PISP. AISP/PISPs may generally not use, store, or in any other way use their access to information for purposes other than to execute the services explicitly requested by the customer.

Other types of open banking services not specifically amounting to PISP or AISP (eg, relating to non-payment accounts or relating to insurance or investments) are not illegal, but may experience difficulties in obtaining access to banking data and banking systems. This is due to banking secrecy rules and the Norwegian ICT regulation (applicable to eg, banks) which requires that external users of a bank's systems are subject to an agreement which shall safeguard relevant IT aspects. However, partnerships and/or cooperation with select banks will typically assist in achieving desired results.

There are various rules addressing IT risks which affect open banking specifically and banking more generally. This includes the Norwegian ICT regulation which subjects most licensed entities in the financial services space to certain IT security standards. The EU has adopted the Digital Operational Resilience Act (DORA) which is meant to safeguard operational resiliency in IT systems used by the financial sector (not yet in force). DORA will also subject certain cloud service providers operating in the EU to supervision from EU financial supervisory authorities. DORA will be transposed into Norwegian law and is expected to replace the Norwegian ICT regulation.

The EU proposed the so-called Financial Data Access Regulation (FiDA) in June 2023. FiDA may ensure widespread data sharing within the financial services sector. FiDA also envisages so-called Financial Information Service Providers (FISPs) as a new type of regulated entity which can retrieve financial data. Financial data is a defined term which includes loans, savings accounts, investment accounts, financial instruments, non-life insurance, insurance-based investment products, but not life insurance and not payments accounts (the latter is already subject to the existing open banking regime). Such financial data may be shared within the regulated financial sector (eg, banks, insurance companies, investment firms) and directly to customers. In addition, the new type of licensed entity, FISP, may retrieve the financial data and for example offer a consolidated overview of all financial data to the customer. The method for sharing data is proposed to be further specified by financial data sharing schemes. If and when adopted in the EU, the same rules are expected to be transposed into Norwegian law.

Poland

Krzysztof Wojdyło*
Wardyński & Partners, Warsaw
krzysztof.wojdylo@wardynski.com.pl

Joanna Werner†
Wardyński & Partners, Warsaw
joanna.werner@wardynski.com.pl

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

At present, there is no single comprehensive piece of legislation that governs the fintech area in Poland. Regulations in this respect are scattered across various legal acts adopted both on the national and EU level. Below we present the most important laws and regulations (both in force and foreseen to be adopted in the future) which relate to fintech.

Payment services providers

Payment services are mainly regulated in the second Payment Services Directive (PSD2)[1] adopted on the EU level and implemented in the Polish legal system in the Act of 19 August 2011, on payment services (PSA).

The PSA not only regulates the manner in which traditional payment services providers (eg, banks, payment institutions) provide payment services to their customers, but also introduces new types of payment services providers and new, innovative types of payment services. The former includes account information services providers (AISPs), whereas the latter covers such services as the already mentioned account information services, payment initiation services (PIS) and services relating to confirmation of the availability of funds (CAF) connected with card-based payment instruments.

The PSA also regulates e-money institutions and issuance of e-money and, as such, has implemented another EU-level legislation, ie, the E-Money Directive.[2] See Question 3.

---

* Krzysztof is a partner at Wardyński & Partners, where he leads the fintech practice. He advises clients with respect to blockchain regulation, smart contracts, fintech, commercialisation of new technologies, telecommunications, robotics and anti-money laundering. He participates in large and innovative projects in the field of broadly defined new technologies. He regularly advises both startups and large players in the new technology sector.

† Joanna advises on regulatory aspects of the operations of financial institutions and fintech companies. She supports clients from the financial and fintech sectors in ensuring that their operations and products comply with legal requirements (regarding such aspects as AML, outsourcing, payment services, consumer credit, blockchain, financial instruments) as well as supervisory guidance. She regularly advises clients from these sectors on legal issues connected with entering the Polish market or developing new, innovative financial products.

1 Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/ EC.

2 Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC.

Open banking

The legal framework for the operation of open banking in Poland is mainly PSD2, the PSA and EU Regulation 2018/389.[3] Under PSD2, the philosophy of access to payment accounts has changed significantly, as authorised third parties (TPPs) can, on behalf of and with the consent of the customer, access account information or order the execution of payments. According to Regulation 2018/389, each account servicing payment service provider (ASPSP) should offer at least one access interface (API) allowing secure communication with the TPP. See also Question 5.

Crowdfunding

Crowdfunding is regulated on the EU level by the ECSP Regulation,[4] which sets out a harmonised framework for investment-based (or share-based) and lending-based crowdfunding services providers in the EU. The ECSP Regulation requires providers to obtain a licence to pursue crowdfunding business in the EU. Providers are supervised by the Polish Financial Services Authority (FSA).

Cloud computing

At present, there is no single piece of legislation which regulates cloud computing. Apart from generally applicable legal acts which apply in relation to cloud-based services (eg, outsourcing regulations, data protection regulations), supervised entities (eg, banks, payment institutions) are also required to follow regulatory guidance in this respect.

On 23 January 2020, the Polish FSA issued a communication on information processing by supervised entities using public or hybrid cloud computing services, which is designed to standardise rules of application of cloud-based systems by supervised entities. In accordance with the communication, it should be applied by the supervised entities instead of any EU-level guidelines or recommendations issued by any of the European supervision authorities (ie, EBA, ESMA or EIOPA).

Digital ID

At present, the basis for electronic identification, authentication and certification is set out in the electronic identification, authentication and trust services (eIDAS) regulation.[5] A need for greater standardisation of electronic identification processes throughout the EU has led the European legislator to publish a proposal for a completely new European Digital Identity Regulation (EDIR),[6] which is designed to address the shortcomings of the eIDAS regulation (inherent limitation to the public sector, limited possibilities for private providers, lack of interoperability of national electronic identification between Member States) and create a European digital ID wallet.

---

3 Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

4 Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937.

5 Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

6 Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity.

In addition to eIDAS, Poland introduced several legal acts that regulate local digital ID means (eg, regulation on the mObywatel application).[7] Furthermore, the Polish FSA and the Polish anti-money laundering (AML) authority has issued several guidelines dedicated to the use of digital IDs for purposes of know your customer (KYC) processes.

Crypto assets

There is currently no exhaustive crypto-specific regulation in Poland. The single Polish legal act that references the crypto assets considered to be virtual currencies is the Polish AML legislation, which introduces the so-called virtual asset service provider (VASP) register.

Capital markets

Capital markets seem to be in an early stage in terms of innovative technology deployment. In particular, there is no single comprehensive legislation that would govern the operations of fintechs on the capital markets.

The most commonly used solutions are algorithmic trading governed by Regulation 2017/589[8] issued under MiFID as well as robo-advisory services. Robo-advisory, being a specific and automated method of providing investment advice, is not subject to separate regulations on the provision of brokerage services. In November 2020, the Polish FSA issued a position paper on robo-advisory in which it clarified the rules of deployment of this service by investment companies.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

At present, there is no exhaustive crypto-specific regulation in Poland. Regulatory guidance in this respect is also limited. Thus, business models involving crypto assets need to be assessed in light of the risk of their classification as traditionally understood regulated services (banking services, payment services, brokerage services, etc), which could result in a licensing requirement being triggered.

The only piece of legislation related to crypto assets and, specifically, to virtual currencies in Poland is the Polish Act of 1 March 2018, on anti-money laundering and terrorist financing (AML Act). Entities rendering some services related to virtual currencies are obliged to register in the register of virtual currency related activities maintained by the Ministry of Finance. Under the AML Act, a VASP is an entity engaged in the business of providing services relating to:

- exchanges between virtual currencies and fiat;
- exchanges between virtual currencies;

7 Commission Delegated Regulation (EU) 2017/589 of 19 July 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards specifying the organisational requirements of investment companies engaged in algorithmic trading.

8 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

- intermediation in the exchanges referred to above; and
- maintaining of crypto wallets.

A failure to register is subject to an administrative fine of up to approximately €21,000 (PLN 100,000).

Moreover, there exists a special tax regime (relating to corporate income tax and personal income tax) relating to trading of virtual currencies in the meaning of the AML Act. Under these regulations, the income tax on profit realised as a result of trading in virtual currencies (19 per cent) is only due when a virtual currency is exchanged into fiat or is used to pay for services or goods, and is not due on exchanges between virtual currencies (such exchanges are tax neutral). Moreover, sale and exchange of virtual currencies is exempt from civil transactions tax.

Notwithstanding the above, there is currently a substantive new piece of legislation adopted at EU level – MiCA.[9] MiCA's objectives are to harmonise the EU crypto assets market and ensure a high level of consumer protection. MiCA introduces a new category of market players – crypto assets service providers (CASPs) – and imposes on them new licensing, capital and consumer protection requirements. Certain new requirements will be imposed on issuers of those crypto assets which refers to another asset to maintain a stable value – ie, an obligation to ensure liquidity at an appropriate level to back those asset-referencing crypto assets that are already in circulation. These entities will also become supervised entities on national levels.

Adoption of MiCA is complemented by changes to the EU AML framework, which expands the so-called 'travel rule' to transfers of crypto assets. In practice, the 'travel rule' that currently applies to traditional payment chains requires providers to collect certain information on the originator and beneficiary of the transfer – in particular, data which allows these entities to be identified in order to verify this data against sanctions lists.

The crypto assets that are deemed to be financial instruments and, as such, do not fall under the scope of MiCA, may benefit from the DLT Pilot Regime.[10] The DLT Pilot Regime is designed to 'allow for certain DLT market infrastructures to be temporarily exempted from some of the specific requirements of Union financial services legislation that could otherwise prevent operators from developing solutions for the trading and settlement of transactions in crypto-assets that qualify as financial instruments, without weakening any existing requirements or safeguards applied to traditional market infrastructures' (see motive 6 of the DLT Pilot Regime). The idea is to accelerate and facilitate the development of a digital securities (either tokenised or native) market in the EU.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

Payment services providers (PSPs) are regulated in Poland by the PSA, which implements PSD2 and the E-Money Directive into the Polish legal system.

9 Proposal for a Regulation of the European Parliament and of the Council on markets in crypto assets, and amending Directive (EU) 2019/1937.

10 Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology, and amending Regulations (EU) No 600/2014 and (EU) No 909/2014 and Directive 2014/65/EU.

The PSA specifies which entities may be PSPs and e-money issuers under Polish law. The former group is broad, and covers both traditional financial institutions (eg, banks) as well as those PSPs which are specifically regulated by the PSA. The latter category includes the following entities.

Payment institutions

These entities are authorised to perform the broadest scope of payment services for their customers (including innovative payment services such as AIS or PIS) and may also act across borders. Moreover, provided that certain additional requirements are met, payment institutions may also issue e-money (although certain territorial and quota limitations apply in such cases). For an entity to become a payment institution, it needs to obtain a licence from the Polish FSA. The process is rather complicated and burdensome and may even take up to 18–24 months to complete.

Small payment institutions (SMIs)

To provide payment services as an SMI in Poland, an entity needs to obtain an entry in the register of SMIs maintained by the Polish FSA. The licensing (or, rather, registration) route is less burdensome compared to the one applicable to payment institutions; however, the scope of services that SMIs may render is also limited.

Namely, an SMI is not authorised to provide AIS and PIS – to do that, it needs to upgrade its licence and become a payment institution. Moreover, SMIs may only pursue their payment business in Polish territory (this limitation is quite conservatively interpreted by the Polish FSA) and they need to observe quota limits for payment transactions effected by them, as well as certain limits on the amount of funds held for one user on their payment account.

Account information services providers (AISPs)

See Question 5 for further details.

Payment bureaux

This is another simplified way of providing payment services in Poland: to be exact, of money remittance services, as payment bureaux are not authorised to perform any other payment services. Like SMIs, payment bureaux can only act in Polish territory and need to observe quota limits on money remittance transactions that they execute. Payment bureaux are supervised by the Polish FSA and commencement of activities such as a payment bureau needs to be preceded by an entry in the relevant register maintained by the regulator.

Apart from the above PSPs, the PSA regulates the terms and conditions of issuing e-money by e-money institutions. E-money institutions are regulated entities licensed and overseen by the Polish FSA. Apart from issuing e-money, e-money institutions may also provide other payment services (to the extent that these are covered by their licence). At present, only one e-money institution licence has been issued in Poland – in 2019, to a company named Billon Solutions.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

The following programmes which aim at supporting the development of fintech ecosystems are currently deployed by the Polish FSA.

Innovation Hub

This program is a legal support programme dedicated to entities who operate or plan to launch their business in the fintech area, provided that the solution that those entities are planning to implement does not easily fit the existing legal and regulatory framework. In such cases the eligible participants may run their innovative ideas past Polish FSA's officers to obtain the regulator's assessment of the innovative business model or product.

Virtual Sandbox

This is a technology testing environment allowing the simulation of selected functionalities and services offered on the financial market. Participants gain access to an IT infrastructure that allows them to verify their business assumptions in controlled conditions. For the time being, the Virtual Sandbox is limited to testing basic PSD2 services: ie, PIS, AIS and CAF. Virtual Sandbox is an extension of the Innovation Hub program and is available to participants of the Innovation Hub.

As well as the above programmes, the Polish FSA has introduced the following tools and initiatives to support fintech.

Interpretations of the Polish FSA

The interpretations that the Polish FSA issues are intended to increase legal and regulatory certainty for entities supervised (or planning to become supervised) by the Polish FSA. Interpretations may be requested by entities planning to engage in activities relating to products and services that are intended to develop financial market innovation.

The fintech working group

The purpose of the working group is to identify legal, regulatory and supervisory barriers to the development of financial innovation in Poland and to prepare proposals for solutions that could eliminate or reduce the identified barriers. The Polish FSA acts as a coordinator of this working group.

Fintech Inter-Ministerial Steering Committee

The aim of the Committee is to coordinate the activities of various state institutions and bodies to support the development of the fintech sector in Poland, to develop common positions and to undertake joint inter-ministerial activities in the field of fintech.

Notwithstanding the above initiatives, it is an expectation of the market that efforts to support the development of the fintech ecosystem in Poland will intensify, in order to further advance the migration to a paperless model of doing business by financial market entities and significantly shorten the duration of the licensing proceedings before the Polish FSA.

More frequent publication of the Polish FSA's interpretations and positions pertaining to innovative business models would also positively contribute to legal and regulatory certainty on the Polish fintech market.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

As already indicated, the main driver of open banking in Poland is PSD2 and its implementing legislation, which allows TPPs to access account information or order the execution of payments on behalf of, and with the consent of, the customer through APIs made available by the ASPSPs.

A key element of the open banking ecosystem is the requirement for ASPSPs to provide open APIs through which TPPs can offer innovative products and services. Detailed requirements relating to such APIs are set out in the Regulation No 2018/389 issued under PSD2. In response to the requirements for open APIs set out both in the PSD2 and in the Regulation No 2018/389, the Polish financial sector under the leadership of the Polish Bank Association (*Związek Banków Polskich*) has developed an interface standard through which banks operating on the Polish market may offer access to their systems to TPPs – the so-called Polish API.

The two main payment services related to open banking are payment initiation services (PIS) and account information services (AIS), both introduced by PSD2. In this context, services relating to confirmation on availability of funds (CAF) should also be mentioned, although these are not formally considered to constitute a separate category of payment services under Polish law (although they are intrinsically connected with payment services relating to card-based instruments and, as such, may only be rendered by authorised PSPs).

Payment initiation services (PIS) are widely used in e-commerce, where PISPs (PIS providers) assist users in the online payment process without taking possession of user funds. PIS is treated as a regulated payment service and its provision to customers is connected to a necessity to obtain an authorisation from the Polish FSA to operate as a national payment institution. At the same time, it should be pointed out that the scope of activities of a national payment institution may be much broader than the provision of PIS alone.

AIS, on the other hand, consists of the provision of consolidated information relating to the user's online payment account or accounts held with one or more other PSPs – eg, aggregated information concerning balances and turnover on such individual accounts. AIS often forms the basis for building many different business models and offering additional services to customers that are not always regulated by the PSA (eg, user identity confirmation services). AIS is a regulated payment service and its provision to customers requires an entry in the relevant register maintained by the Polish FSA. Those providers who limit their payment services to AIS are referred to as account information service providers (AISP). If the AISP intends to provide other payment services on top of AIS, then such provider must obtain a licence from the Polish FSA to operate as a national payment institution.

CAF services enable the user to make payments with a card-based payment instrument (eg, a debit card) issued by a third party other than the one that maintains the user's online payment account (ASPSP). In practice, the user enters into a contract with the CAF service provider who, at the same time, is the issuer of the payment instrument to the user. A CAF service allows the provider to issue such payment instrument without having to open an account for the user, as the payment instrument is linked to the payment account that the user has already set up with a third party ASPSP. CAF services may be provided as part of a service of issuing payment instruments and, as such, requires a licence from the Polish FSA to operate as a national payment institution.

Portugal

Vera Esteves Cardoso*
Morais Leitão, Lisbon
vcardoso@mlgts.pt

Ashick Remetula†
Morais Leitão, Lisbon
aremetula@mlgts.pt

1. Fintech regulatory framework: please provide a description of the most relevant laws and regulations on fintech and financial innovation in your country. Please also refer to any new law or regulation foreseen in the near future or any bill on fintech and financial innovation in your jurisdiction.

Under the Portuguese legal landscape, there is no specific law applicable to fintech enterprises.

There are not, at least at the European Union level and in Portugal, specific licences only applicable to fintechs in a general sense, even though some legal frameworks may seem more attractive to this specific sector.

As such, the key to understanding where fintechs lie, in terms of applicable legal regime, is to comprehend exactly what will that company be offering. The legal framework applicable to the business model and services of that fintech will result from finding those coordinates.

Without prejudice, the main legal and regulatory frameworks applicable to fintechs, bearing in mind the intimate connection with the financial industry, are the ones related with the following:

Payment services and e-money related activities

1. *Payment institutions and e-money institutions*, the activities of which are regulated under Decree-Law No 91/2018, of 12 November 2018 – the Payment Services and e-Money Legal Regime (*Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica* or RJSPME), which transposed Directive (EU) 2015/2366 (PSD2) in Portugal. Under this category, there is an exemption regime established under PSD2 foreseen for 'smaller' payment institutions. The RJSPME adopted this partial exemption for payment institutions who want to perform all payment services with the exception of money remittance and payment initiation services and account information services.[1]

---

* Vera is a consultant within Morais Leitão's banking and finance practice. Vera develops her work primarily in banking law, fintech and crypto asset service providers, with a special focus in market entry and compliance matters. In this field, Vera provides legal advice and consultancy with regards to the regulation and supervision of banks, payment and e-money institutions and other financial entities. Vera also provides consultancy in matters related to payment services specifically in the fintech sector, open banking and limited networks under PSD2.

† Ashick is an associate within Morais Leitão's banking and finance practice. Ashick develops his practice in the fintech area with emphasis on companies dealing with new and emerging technologies, matters related with blockchain, crypto and web 3.0, essentially in the context of attracting and making investments, licensing and regulation. Moreover, Ashick also advises those companies in project management issues, from a legal standpoint.

1 See Question 3.

2. *Open Banking service providers*, such as payment initiation service providers (PISPs) and Account Information Service Providers (AISPs), regulated under RJSPME.

3. *Technical service providers* (TSPs), which support the provision of payment services without entering into possession, at any time, of client funds, regulated under RJSPME.

4. *Limited Network Exemptions*, applicable to entities that provide services based on specific payment instruments that can only be used to a limited extent, such as payment instruments used in limited networks or payment instruments used to pay for a very limited range of goods and services, regulated under RJSPME.

Crypto asset services

Law No 83/2017, of 18 August, as amended, on anti-money laundering and combatting the financing of terrorism (Portuguese AML/CFT Law) sets forth the legal framework applicable to virtual asset service providers (VASPs), when such entities provide certain services with crypto assets, in the name or on behalf of clients. This legal framework foresees both the prior registration and subsequent supervision of such entities, only for anti-money laundering and combatting the financing of terrorism (AML/CFT) purposes. Following the amendment of the Portuguese AML/CFT Act, setting forth the legal framework applicable to VASPs, the Bank of Portugal published two notices completing and further developing the regime:

1. Bank of Portugal's Notice No 3/2021 of 13 April, which regulates the actual registration procedure with the Bank of Portugal. This is applicable to entities that intend to pursue the activities with virtual assets, in Portuguese territory; and

2. Bank of Portugal's Notice No 1/2023 of 24 January, which establishes the necessary aspects to ensure compliance with the duties to prevent money laundering and terrorist financing, within the scope of the activity of entities that carry out activities with virtual assets.

Besides that, at present, there are no specific laws or regulations that govern crypto assets. However, with the enactment of Regulation (EU) 2023/1114 on markets in crypto assets (MiCA), and its direct applicability in Portugal, as an EU Member State, that will change. Nonetheless, even without considering MiCA, one cannot say that there is a regulatory vacuum in this context, since existing laws will need to be assessed on a case-by-case basis to determine whether they apply to a particular crypto asset or related activity.

Credit intermediaries

Considering the less demanding regime of credit intermediaries in comparison with credit institutions, and the range of digital means via which this type of activity may be exercised, some fintechs find this structure appropriate for their business model. A credit intermediary participates in the credit granting process and can, in abstract, provide the following services:

- presentation of credit agreements to consumers;

- proposing credit agreements to consumers;

- assisting consumers in the preparatory stages of credit agreements;
- concluding credit agreements with consumers on behalf of creditors; and
- consultancy.

The credit intermediary is not authorised to grant credit or intervene in the marketing of other banking products or services, such as term deposits or payment services. Even if a credit intermediary intervenes, the credit is always granted by an institution authorised to grant credit (eg, credit institutions).

Crowdfunding

Crowdfunding is a field of the financial services sector that has been significantly influenced by the growth of fintech companies. Bearing in mind that not all businesses have the same access to traditional equity and debt financing, crowdfunding platforms are gaining some more traction. Crowdfunding platforms are regulated by Law No 102/2015, of 24 August, Law No 3/2018 of 9 February, by the Portuguese Securities Market Commission (Comissao do Mercado de Valores Mobiliarios or CMVM) Regulation No 1/2016, and by Ordinance no 344/2015, of 12 October.

The following categories of crowdfunding are permitted in Portugal.

1. *Donation-based crowdfunding*: funds are collected as donations for specific projects or causes, without the expectation of financial return.
2. *Reward-based crowdfunding*: donors contribute financially and receive non-financial rewards in return, such as products or services.
3. *Loan-based crowdfunding*: involves the lending of money by investors to projects or companies, with the expectation of receiving the invested amount plus interest within a specified period.
4. *Investment-based crowdfunding*: investors acquire ownership stakes in companies or projects and have the potential to gain financial returns based on the performance.

There are several requirements and obligations on both crowdfunding platforms and projects or companies seeking funding, namely:

- *Registration with CMVM*: entails compliance with specific rules and obligations, including, among others: (1) identification of the applicant, including identification of the shareholders and identification of the ultimate beneficial owner; (2) identification of the members of the management body; (3) description of the business model; and (4) management report and accounts.
- *Transparency and information*: crowdfunding platforms must provide clear, accurate and transparent information about the projects or companies seeking funding, as well as the associated risks. This includes disclosing information about the project's objectives, the use of raised funds, investment risks, and refund policies.
- *Fundraising limit*: the legislation establishes limits for fundraising in each crowdfunding category.

- *Investor protection*: crowdfunding platforms must assess the suitability of the investment for each investor's profile to ensure they have awareness and understanding of the associated risks.

Other fintech-related products:

Some fintechs build their business model with the primary objective of integrating with traditional financial entities (eg, banks). In many of these cases fintechs step in to aid incumbents in ensuring better and more efficient compliance (eg, credit scoring, onboarding solutions, monitoring and screening, among others). In these scenarios, even with no financial activity specifically carried out, fintechs should pay special attention to the applicable legislation, in order to make their services/products more attractive (and compliant) for incumbents. This may include the compliance with outsourcing requirements, considering national legislation and the guidelines set forth by the European Banking Authority, and the recently enacted Regulation (EU) 2022/2554 on digital operational resilience (DORA).

New legislation and regulation

- *DORA Regulation*: Regulation (EU) 2022/2554 on digital operational resilience sets forth rules not only for financial entities, but also to information and communications technology (ICT) providers of such entities; many fintech providers will be required to comply with the rules established therein if they wish to provide services to those institutions.
- *MiCA*: Regulation (EU) 2023/1114 on markets in crypto assets is the first piece of EU legislation that intends to further regulate and harmonise existing legislation related to crypto assets and related services.
- *DLT Regime*: Decree-Law No 66/2023, of 8 August, implemented the EU provisions on the use of distributed ledger technology (DLT) to issue, trade and settle financial instruments issued through DLT, namely in regard to the issuance of debt instruments. The provisions set forth address the technological challenges linked to the financial disintermediation triggered by the use of DLT, including the form of representation and registration.
- *EU AML Package*: legislation to strengthen the EU's AML/CFT rules, which includes four pieces of legislation:[2]
    - AMLA: a regulation providing for the creation of a new EU-wide AML/CFT authority, the Anti-Money Laundering Authority;
    - AML Directive 6: focusing on supervisory and financial intelligence unit aspects;
    - AML Regulation: a regulation on AML/CFT (essentially focusing on customer due diligence aspects); and
    - a revised version of the 2015 Regulation on Transfers of Funds to trace crypto assets transfers.

2 Under EU legislative procedure.

- *eIDAS 2.0*: An evolution of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS 1). This update builds upon the original eIDAS law and aims to increase the security and reliability of electronic identification and trust services within the EU, with the objective of ensuring a seamless and secure digital environment within the EU by ending the implementation gaps that occurred within different Member States. In addition, the 'European Identity wallet' will be made available to all EU citizens.
- *PSD3*: EU regulation that will evolve the framework set by PSD2, with a special focus on the evolution of open banking to 'open finance', setting out clearer and sturdier regulation for strong customer authentication (SCA) and fraud prevention, among other developments.

2. Regulations on crypto assets: please provide a summary of the legal framework of crypto assets in your country and how crypto assets are regulated in your jurisdiction.

The Portuguese law specifically addressing services provided with crypto assets (or virtual assets in the normative definition) is the Portuguese AML Law, which transposed the Directive (EU) 2018/843 on AML/CFT (AMLD5). This law sets forth a registration procedure mandatory for persons (whether natural or legal) seeking to provide certain services to clients with virtual assets – the so-called VASPs – and their subsequent supervision. Note however that this registration is mandatory only for AML/CFT supervision purposes; hence, it is not the same as a standard licensing procedure carried out, for example, by a regulated financial entity.

According to said law, the following persons will have to be authorised and registered with the Bank of Portugal prior to commencing their activity in Portugal, when the following activities are carried out for and on behalf of their customers:

- providers engaged in exchange services between virtual assets and fiat currencies;
- providers engaged in exchange services between one or more forms of virtual assets;
- providers of services that allow the transfer of virtual assets from one address or wallet to another; and
- providers of custodian wallet services (which allow the safeguarding of private cryptographic keys on behalf of their customers, to hold, store and transfer virtual assets).

In a nutshell, exchange services, transfer services and custodian services in relation to virtual assets are specifically regulated for AML/CFT supervision purposes.

However, this registration procedure is mandatory when the aforementioned services are exercised/operated within the Portuguese territory. The following entities are considered to operate within Portuguese territory:

- legal persons incorporated in Portugal to carry out activities with virtual assets;
- natural persons or legal persons with a domicile or establishment in Portugal engaged in activities with virtual assets; and

- natural persons or legal persons who, due to the exercise of activities with virtual assets, are obliged to submit a statement of start of activity to the Portuguese tax authority.

The Bank of Portugal has been the competent authority in registering and verifying compliance with the applicable legal and regulatory provisions governing AML/CFT by VASPs – being, as of the time of writing and according to the public list published by the Bank of Portugal, 11 registered entities, five of which have not been authorised to commence activities. The registration procedure regulated by the Bank of Portugal's Notice No 3/2021, of 24 April.

Furthermore, more recently, the authority issued Notice No 1/2023, of 24 January, covering matters foreseen in the Portuguese AML Law, the application and execution of restrictive measures approved by the United Nations or by the EU, and establishing the sanctions framework for breaches of said measures.

This new notice is addressed to entities which develop activities with virtual assets within domestic territory, registered as such with the Bank of Portugal. Entities not registered in domestic territory are considered 'entities of equivalent nature' and, while they are not directly subject to the provisions of this new notice, the business relations between them and entities registered in domestic territory are thereby regulated in several aspects, namely in relation to the implementation of enhanced due diligence measures.

The Notice further aims to harmonise national legislation with the international framework on AML/CTF, pre-emptively including some of the content expected to be included in the EU AML Package (the legislative package aimed at AML/CTF). It is also driven by Recommendation 15 of the Financial Action Task Force (FATF), reviewed in 2018 to include provisions on VASPs, as well as by FATF's *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, published in 2021. This is evident, for example, in the inclusion of the travel rule in the notice.

The goal of this notice is to clearly define the procedures, tools, mechanisms, formalities and the provision of information duties, among other aspects deemed necessary to the fulfilment of VASP related AML/CFT duties, a sector which has been identified as being of high risk and in which entities have had less time to develop their experience in adhering to these duties – as the procedures associated to the registration of VASPs with the Bank of Portugal entered into force on 24 April 2021.

Securities laws and regulations

Some crypto assets, due to their intrinsic characteristics, may potentially be qualified as securities and become subject to existing securities regulations, most notably regulations applicable to public offerings of securities and/or securities trading venues.

The CMVM has clarified the elements that may, in abstract, implicate the qualification of tokens as securities, namely:

- if they may be considered documents (whether in dematerialised or physical form) representative of one or more rights of a private and economic nature; and
- if, given their particular characteristics, they are similar to typical securities under Portuguese law.

For the purpose of verifying the second item, the CMVM will take into account any elements, including those made available to potential investors (which may include any information documents, such as a white paper), that may entail the issuer's obligation to undertake any actions from which the investor may draw an expectation to have a return on its investment, such as:

- to grant the right to any type of income (eg, the right to receive earnings or interest); or
- undertaking certain actions, by the issuer or a related entity, aimed at increasing the token's value.

For example, tokens that represent rights and/or economic interests in a predetermined venture, project or company, such as tokens granting the holder a right to take part in the profits of a venture, project or company, or even currency-type tokens, will in principle be subject to securities laws and regulations.

Since the Portuguese jurisdiction, namely the competent authorities, follow the rules and guidelines set by their EU counterparts, it's worth mentioning that the European Securities and Markets Authority's (ESMA) position regarding the regulatory implications when a crypto asset qualifies as a financial instrument is adopted in the Portuguese jurisdiction. In the particular case of ICOs, in general, being subject to securities laws, ESMA provides advice on the potential application of, notably the:

- Directive 2003/71/EC (Prospectus Directive);
- Directive 2013/50/EU (Transparency Directive);
- Directive 2014/65/EU on markets in financial instruments (MiFID II);
- Regulation (EU) No 600/2014 on market in financial instruments (MiFID Regulation) and respective implementing acts;
- Regulation (EU) No 596/2014 and Regulation (EU) No 236/2012 (Market Abuse Regulation and Short-Selling Regulation);
- Directive 2009/44/EC (Settlement Finality Directive);
- Regulation (EU) No 909/2014 (Central Securities Depository Regulation); and
- Directive 2011/61/EU on alternative investment fund managers (AIFM Directive).

All the abovementioned legislation has been transposed into the Portuguese legal framework, and the rules set forth therein are reflected namely in the Portuguese Securities Code.

In this context, if a token is qualified as a security, the relevant national laws shall apply, including, inter alia, those related to:

- the issuance, representation and transmission of securities;
- public offerings (if applicable);
- marketing of financial instruments for the purposes of MiFID II;
- information quality requirements; and

- market abuse rules.

Finally, in the particular case of an ICO or a Security Token Offering (STO), should they qualify as a public offering, a prospectus should be drafted and submitted, along with any marketing materials, to the CMVM for approval, provided that no exemption applies in relation to the obligation to draw a prospectus.

General laws and regulations

As mentioned previously, the lack of specific laws and regulations addressing crypto assets in particular does not mean that crypto assets/tokens that are not subject to the laws and regulations referred to above are completely unregulated and navigating in the void.

Existing legal frameworks shall apply in accordance with the subject matter/characteristics of the crypto asset/token/service in stake. The following regimes may be applied to some crypto assets/services, depending on the specific case at hand:

- the Portuguese Civil Code;
- intellectual property laws with relation to the creation and licensing of underlying intellectual property rights;
- Regulation (EU) 2022/2065 (the Digital Services Act);
- Decree-Law No 7/2004, the e-Commerce Law;
- consumer protection laws, notably Decree-Law No 24/2014, the Distance and Off-Premises Law, and the Decree-Law No 84/2021, the Digital Goods, Content and Services Law;
- the Advertising Code; and
- other sector-specific rules that may be applicable.

Finally, party's autonomy always carries some weight. Hence, parties may contractually agree on some rules, where they do not contradict mandatory legal provisions.

3. Payment service providers and digital wallets: please describe how payment service providers and/or digital wallets are regulated in your country. Please mention any foreseen law or regulation in this respect.

Payment service providers and digital wallets are regulated according to the rules established under the RJSPME, which transposed PSD2 into the national legal framework.

Digital wallets

The provision of digital wallets is also considered a payment service in itself (ie, issuing payment instruments), if the manner in which the digital wallet is provided does not allow for the application of the exemptions foreseen by PSD2.

Nevertheless, entities may provide digital wallets and still not fall under the applicable RJSPME rules if:

1. Providers or issuers of such wallets merely support the 'provision of payment services without at any time coming into possession of the funds being transferred, including data processing and storage, trust and privacy protection services, authentication of data and entities, the provision of communication and IT networks or the provision and maintenance of terminals and devices used for payment services, with the exception of payment initiation services and account information services'; and

2. If the services being provided are based on digital wallets that can only be used on a limited basis and which are:

    a) instruments which only allow the acquisition of goods or services by their holder on the premises of the issuer or on a restricted network of service providers directly linked by a commercial agreement to a professional issuer; or

    b) instruments that can only be used to acquire a very restricted range of goods or services.

However, it is important to note that Bank of Portugal's Notice No 3/2023 regulates further aspects surrounding the limited networks and was based on the EBA Guidelines on the limited network exclusions under PSD2.

Partially exempted payment service providers

Apart from the general legal framework applicable to payment service providers, PSD2 left the door open for EU Member States to allow for 'smaller' payment institutions to be exempt from complying with the aforementioned legal regime. This may, in some cases, be an attractive solution for smaller fintech companies who wish to provide certain services without having to go through all the licensing hurdles. Notwithstanding, these exempted entities may not passport their activity onto other Member States.

However, Portuguese legislation only allows access to a partial exemption for payment institutions who want to perform all payment services except for money remittance and payment initiations services, and account information services.

The scope of the exemption is decided via a case-by-case analysis by the Bank of Portugal, but never includes general verifications regarding its business plan, fit and proper assessment, procedures for safeguarding client funds, governance and risk assessment and management arrangements, and AML/CFT verifications.

For the application for such exemption, payment institutions must have:

- a monthly average of the preceding 12 months (or as projected in their Business Plan) of no more than €3m;

- no person having been appointed as responsible for its management to have been convicted for any financial crimes; and
- an initial share capital of €50,000.

These entities must request, from the Bank of Portugal, a formal decision regarding the possibility of benefitting from this partial exemption.

4. Special support to fintechs: does your jurisdiction provide any special programmes supporting the fintech ecosystem, in particular fintech startups (eg regulatory sandboxes, accelerator programmes). Are such programmes supported by the regulator in your country?

Over the past few years, Portugal has established itself as a prominent fintech hub in Europe. This has led to substantial investments and an influx of founders, entrepreneurs, investors and various other players in the market.

The increased interest in financial technology can be attributed to several factors. Firstly, the digital services sector has witnessed significant growth, creating a favourable environment for the intersection of technology into the traditional financial sector. Additionally, the overall market capitalisation of the fintech sector has been on a consistent upward trajectory. Moreover, there has been an uptick in investment from experienced and more sophisticated market players.

The government, regulators and the general ecosystem has been providing support to fintechs via several initiatives.

Regulatory sandboxes

Decree-Law No 67/2021, of 30 July, sets the framework for the creation of regulatory sandboxes (designated Technological Free Zones). The envisaged sandboxes intend to create 'safe spaces' in which companies can test innovative products, services, business models, without immediately incurring all the normal regulatory consequences related to the activity. Any entity that wishes to apply to create a Technological Free Zone must complete an application or submit a declaration of interest in the website of the National Innovation Agency and follow the relevant formal procedure.[3]

Portugal FinLab

This is an innovation hub/communication channel between market players and the Portuguese regulatory authorities (banking, securities and insurance). Through it, the authorities provide guidelines on how to navigate and operate in the regulatory system. The purpose of Portugal FinLab is to support the development of innovative solutions in fintech and related fields through cooperation and mutual understanding. They come together to give advice on the applicable legal

3 As of this date, the government has approved the creation of two Technological Free Zones to (1) test and experiment with products and services that intend to accelerate the transition to a carbon neutral economy, and (2) test and validate new communications, sensors, artificial intelligence and materials.

frameworks, based on the information provided by candidates. Candidates are selected based on the preliminary information submitted during pitch days. Around five projects are selected: for each, a comprehensive and detailed report with non-binding positions is submitted, with obstacles identified and critical issues highlighted. Portugal FinLab has received positive reviews from its participants and is, for the time being, the most effective way of fintech players obtaining direct advice from regulators and supervisors.

Fintech+ channel

An open channel through which companies may clarify questions related to innovation in financial products and services, as well as a range of relevant information in this field.

Fintech meetings

These are planned and organised by the Bank of Portugal on up-and-coming topics which may impact the fintech sector.

Forum for payment systems and initiatives

Relaunched in 2018, this is an advisory structure organised by the Bank of Portugal that brings together government representatives and the main national stakeholders involved in the supply and demand of payment services. Its mission is to contribute to the implementation of safe, efficient, and innovative payment solutions in the Portuguese market. The Forum seeks to answer to the challenges of the retail payment market, by promoting an atmosphere of cooperation amongst its diverse stakeholders.

Bank of Portugal guidelines/best practices

The Bank of Portugal publishes, from time to time, a set of guidelines in respect to certain topics (eg, digital onboarding). Where these guidelines are not binding, considering that the Bank of Portugal is the entity responsible for the supervision and licensing of certain 'fintech companies', these are a highly accurate representation of the thoughts of the authority.

5. Open banking: please advise whether in your jurisdiction there are regulations on open banking. If the response is no, please provide any reference to regulations that may directly or indirectly affect open banking. Please include any foreseen laws and regulations on open banking.

In Portugal, the legal framework applicable to open banking derives from PSD2, allowing third-party financial service providers to access financial information from banks and other financial institutions via application programming interfaces (APIs).

The two main open banking service providers foreseen under RJSPME are PISPs and AISPs which, under the type of services provided and the principle of proportionality, are subject to lighter licensing and supervision requirements than fully fledged payment and e-money institutions.

As such, for entities wishing to provide only these two services, and no other payment services, there are different licensing and supervision requirements applied: ie, the general regulations applicable to PIs aren't fully applicable to PISPs and AISPs

PISPs and AISPS, when exclusively providing one or both services, are not subject to capital requirements applicable to PIs as they will not hold client funds. For this reason, all general requirements and information related to this point, are not applicable.

For AISPs, the simplification of the applicable requirements is carried out directly by having a specific licensing framework applicable to them, which is not the case for PISPs.

When accessing licensing applications for AISPs and PISPs, the Bank of Portugal (along with other EU competent authorities for this purpose) must adapt the level of detail required to the particular service or services that the applicant intends to provide – namely their nature, scope, complexity and riskiness, and to the institution's size and internal organisation.

This is the case for AML/CFT requirements – not applicable for AISPs, and largely not applicable for PISPs. However, for both types of entities, security and data protection requirements are applicable, (namely regarding SCA and secure communications (SCS)).

Even though AISPs and PISPs have no own fund requirements, the fulfilment of their responsibilities must be ensured through the compulsory subscription of a professional liability insurance or an 'equivalent guarantee', which is a necessary condition for their authorisation and registration. At times, this may not be straightforward as the insurance policies cannot have a determined insurance deductible: they must be revolving and also have an extensible period of at least two years, raising the probability of applicants having to obtain tailor-made insurance policies.

All marketing and advertising efforts by these entities must adhere to the general rules applicable to financial institutions. This means that marketing and advertising materials must clearly identify the entity responsible for the offering or advertising and ensure that consumers can easily understand the main features and terms of the promoted products or services.

Spain

José F. Canalejas Merín*
Gómez-Acebo & Pombo, Madrid
jfcanalejas@ga-p.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

As of today, fintech is not expressly regulated in Spain and a neutral technology principle has been adopted, following the European approach. Therefore, fintech is only currently subject to any laws of general application and certain pieces of regulation that have been passed in recent years to update and adjust the legal framework. Within these regulations, different measures have been adopted to promote and enable fintech to develop its activities, as well as to address the challenges and risks connected with digital transformation.

The Covid-19 crisis strongly highlighted how important all aspects of digital transformation are for society. The future of finance is digital and digital transformation will be key for relaunching the Spanish and European economies.

After the 2018 FinTech Action Plan, in September 2020 the European Commission adopted a comprehensive package on digital finance, including several strategies and legislative proposals on crypto assets and digital resilience. This financial package is a major step towards the comprehensive regulatory framework for financial services that will support the rise of fintech and the modernisation of the European economy across all activity sectors.

Digitally active users, market conditions and an innovation-friendly environment allow the Spanish market to be considered very attractive for the development of fintech businesses. In fact, as stated above, steps towards the due implementation of a legal framework that will foster these activities have already been taken. For instance, crowdfunding activities have been regulated in Spain since the approval of Law No 5/2015 of 27 April on Promotion of Business Finance, and a regulatory sandbox was implemented by Law No 7/2020 of 13 November on Digital Transformation of the Financial System.

Furthermore, in December 2022, Law No 28/2022 to promote the startup ecosystem was approved. After the approval of the mentioned startup law, measures and incentives to promote the competitiveness of the Spanish economy have been incorporated into the Spanish legal system, including simplified procedures for the creation of new companies and tax incentives to attract entrepreneurs and highly qualified employees.

---

* José is a senior lawyer in the Banking and Finance Department at Gómez-Acebo & Pombo. His practice focuses on structured finance, capital markets, financial regulation and fintech. José works on a regular basis with local and international credit institutions, e-money institutions, payment institutions, investment funds and other financial institutions in Spain, having participated in some of the most important and complex transactions in recent years.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

Spain has adopted certain measures to implement the fifth Anti-Money Laundering EU Directive, which widens the EU's regulatory perimeter for AML/CFT controls, and brings providers of exchange services between virtual currencies and fiat currencies as well as custodian wallet providers into its scope.

The Bank of Spain (Banco de España or BdE) maintains a register of providers engaged in exchange services between virtual currencies and fiat currencies, and custodian wallet providers. This was created by means of the Second Additional Provision of Law No 10/2010 of 28 April 2010, on the prevention of money laundering and terrorist financing and the Royal Decree No 7/2021 of 27 April. Natural or legal persons, whatever their nationality, who offer or provide the above services in Spain, the natural persons who provide these services when the base, direction or management of these activities is located in Spain, and legal entities established in Spain need to be registered to carry out their activities. Nonetheless, registration does not entail approval or verification by the BdE of the activity carried out by these service providers.

The BdE and the Spanish Markets Securities Commission (Comisión Nacional del Mercado de Valores or CNMV) have issued several statements, warning consumers of the inherent risks of purchasing these types of digital assets.

On 8 February 2018, the CNMV issued a statement to clarify several issues in relation to the marketing of tokens. According to the CNMV, certain initial coin offerings (ICOs) should be treated as initial public offerings (IPOs) of transferable securities. This inevitably resulted in the application of the relevant national and European regulations, mainly enabled by the broad concept of transferable security in the Spanish Securities Market Law.

On 20 September 2018, the CNMV also published a document on the initial criteria that it was applying in relation to ICOs – which is still subject to review, taking into account both the experience accumulated and the debate that is currently taking place at an international level. In this document, the Spanish securities regulator clarifies the concept of a security token, and deems it appropriate to exclude from the definition of transferable assets those cases in which it is not reasonable to establish a correlation between the revaluation or profitability expectations of the instrument and the evaluation of the underlying business.

Additionally, the advertisement of crypto assets as a means of investment, not as a financial instrument, is subject to CNMV Circular No 1/2022, of 10 January. According to the Spanish regulation, any advertising directed at investors or potential investors in Spain which, implicitly or explicitly, offers or draws attention to such crypto assets will be subject to certain requirements and the competent authorities may request the termination or rectification of the advertising activity. Mass advertising campaigns must comply with additional rules, including mandatory prior notification to the CNMV.

After the entry into force of the EU Distributed Ledger Technology (DLT) Pilot Regime Regulation, certain matters that potentially preclude or limit the use of distributed ledger technology in the issuance, trading and settlement of crypto assets that qualify as financial instruments will be solved.

The EU DLT Pilot Regime Regulation establishes the conditions for: permission to operate a DLT market infrastructure, the DLT financial instruments that can be admitted to trading and settled on the DLT, and cooperation between the DLT market operators, competent authorities and the European Securities and Markets Authority (ESMA).

Since the approval of the EU DLT Pilot Regime Regulation did not imply a modification of book entry form requirements applicable in Spain, the Spanish government approved a new securities markets law (Law No 6/2023) which includes, among others, the rules applicable to registration, transmission and representation of DLT securities.

Crypto assets that do not qualify as financial instruments will be subject to the future EU Markets in Crypto-Assets Regulation (MiCA), which provides a new bespoke regime for all crypto assets not covered in EU financial services legislation and crypto asset service providers.

Finally, Spanish tax authorities have outlined the tax treatment of activities related to crypto assets; the Spanish Finance Ministry has also approved the form to be filled in by Spanish taxpayers who hold crypto assets – with a minimum value of €50,000 – abroad (Form 721). Please note that the disclosure obligation applies from 1 January 2024.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

The legal framework applicable to payment institutions and service providers operating in Spain mainly comprises Royal Decree-law No 19/2018 of 23 November on payment services and other urgent financial measures, and Royal Decree No 736/2019 of 20 December on the legal regime of payment services and payment institutions.

These Spanish payment regulations implemented Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015, on payment services in the internal market (PSD2) which, among others, aims to make payments more secure in Europe, to boost innovation and to adapt payment services to newly developed technologies.

Likewise, Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009, on the taking up, pursuit and prudential supervision of the business of electronic money institutions (E-money Directive) was implemented by Law No 2/2011 of 26 July on e-money, and Royal Decree No 778/2012 of 4 May on the legal regime of e-money institutions.

Payment institutions and e-money institutions ought to be authorised by the BdE, as the competent authority in Spain to carry out their activities. For this purpose, the relevant application shall be submitted to the BdE together with:

- a programme of operations;
- a business plan;
- evidence of the initial capital;
- a description of the measures taken for safeguarding payment service users' funds;

- a description of the governance arrangements and internal control mechanisms;
- several procedures; and
- information on the management bodies and the shareholders.

Please note that the BdE follows the European Banking Authority (EBA) Guidelines on the information to be provided for the authorisation of payment institutions and e-money institutions, and for the registration of account information service providers (EBA-GL-2017-09).

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

In 2016, the CNMV created an 'innovation hub' under the name of Portal Fintech on its official webpage. This innovation hub aims to: (1) provide support to developers and financial institutions on regulatory aspects of securities markets that might affect their projects; (2) create an informal space where developers and financial institutions can share their initiatives in this field; and (3) generate criteria on certain relevant fintech issues in the securities markets.

Furthermore, the newly implemented regulatory sandbox allows companies to test innovative products, services and business models in a live market environment while ensuring that appropriate safeguards are in place under the supervision of competent authorities. This tool deals with the issue posed by the most innovative financial companies: the complexity of financial regulations.

The sandbox operates under a cohort system, with two calls per year: one in March and the other one in September. The cycle of each of the cohorts involves a total of five phases.

- *Presentation of requests for access*: the Spanish Treasury shall convene a cohort by means of publishing a resolution on the same web page. Once the application period is opened, promoters have 30 business days to submit their projects.
- *Prior evaluation*: once the deadline for submitting applications has expired, the supervisory authorities will carry out a preliminary evaluation of the applications, for which they will have one month – a period that may be extended for an additional month.
- *Negotiation of the test protocol*: the list of projects temporarily admitted to the sandbox will be published. The promoters and the supervisory authorities shall agree on the conditions under which the activity will be carried out in the sandbox.
- *Test period*: it will begin once the protocol has been signed, the consent of participants in the test has been obtained and the guarantee system has been put in place.
- *Exit from the sandbox*: at the end of the testing period or during it, if necessary, promoters may request an authorisation to start the tested activity. Likewise, promoters are required to prepare a report evaluating the results of the test and the competent supervisory authority will publish a report of conclusions in this regard.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

European law has established an international regulatory framework and standard for the promotion of an open banking model. Consequently, Spanish law supports the transformation of retail banking from a vertically integrated model in which each credit institution performs all the activities comprising the value chain in an independent manner, into an open model in which credit institutions and other institutions work together and compete in each activity.

Payment initiation services (PISs) and account information services (AISs) are regulated under the Spanish legal framework within which: (1) users have the right to make use of services enabling access to account information to stimulate competition; (2) the development of new products and innovative offerings is enabled; and (3) customers may obtain high-value services.

Nonetheless, the European Commission was required to evaluate PSD2, in particular concerning charges, scope, thresholds and access to payment systems. The evaluation took place in 2022, including advice from the European Banking Authority (EBA), a general and targeted public consultation and a report from an independent consultant. Following such evaluation, the European Commission decided to propose amendments to PSD2.

The amendments will improve the functioning of EU payment markets by improving the functioning of open banking, especially as regards the performance of data interfaces, removing obstacles to open banking services and consumer control over their data access permissions. Therefore, further measures will be adopted to ensure the expansion from access to payment accounts data towards access to other types of financial data, moving from ‘open banking’ to ‘open finance’.

Sweden

Lisa Antman
Wigge, Stockholm
lisa.antman@wiggepartners.se

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

As fintech may encompass any activities related to the financial system – such as lending, payment mediation, asset management and insurance activities – fintech companies must comply with prevailing legislation like any other financial company in Sweden. Due to this, fintech business may be subject to several regulations both at national and European Union level. The regulation applicable depends on the specific fintech activity. However, to engage in fintech activity, the regulations generally require a licence from or registration with the Swedish Financial Supervisory Authority (the SFSA).

The most relevant regulations concerning fintech are listed below. Certain authorities, such as the SFSA, have issued further guidelines and supplements to the regulations mentioned below.

The most relevant laws and regulations related to lending and payment mediation business

- The Banking and Financing Business Act (2004:297) (*lag om bank-och finansieringsrörelse*) regulates banking and financing business conducted by credit institutions (ie, banks and credit market companies). The Consumer Credit Act (2010:1846) (*konsumentkreditlag*) implements the EU Consumer Credit Directive and parts of the EU Mortgage Credit Directive. The Act regulates the providing and intermediation of consumer credit, and contains mandatory consumer protection provisions related to such activities.
- The Certain Consumer Credit-related Operations Act (2014:275) (*lag om viss verksamhet med konsumentkrediter*) regulates certain professional consumer credit activities consisting of lending or credit intermediating to consumers.
- The Mortgage Business Act (2016:1024) (*lag om verksamhet med bostadskrediter*) implements the EU Mortgage Credit Directive and regulates lending, credit intermediation, and counselling activities in respect of consumer mortgages.
- The Payment Services Act (2010:751) (*lag om betaltjänster*) implements the EU Payment Services Directive (PSD2) and regulates payment services provided in Sweden and conducted within the European Economic Area.
- The Electronic Money Act (2011:755) (*lag om elektroniska pengar*) implements the EU Electronic Money Directive and regulates the issuance of electronic money as well as the business of institutions of electronic money and registered issuers.

- The Currency Exchange and Other Financial Operations Act (1996:1006) (*lag om valutaväxling och annan finansiell verksamhet*) regulates certain currency exchange activities. This involves professional trading in foreign currency and coins, management and trading in virtual currency, and certain other professional activities listed in Chapter 7, Section 1, second paragraph, points 2, 3 and 5–12 of the Banking and Financing Business Act (2004:297) (inter alia, lending and credit intermediation activities).
- The Debt Recovery Act (1974:182) (*inkassolag*) regulates debt recovery activities.

The most relevant laws and regulations related to asset management business

- The Securities Market Act (2007:528) (*lag om värdepappersmarknaden*) implements the EU Markets in Financial Instruments Directive (MiFID II) and regulates, inter alia, investment advisory business, regulated markets and portfolio management. The Securities Market Act further implements parts of the EU Investment Firm Directive (IFD) which, together with the EU Investment Firms Regulation (IFR), inter alia, stipulates capital adequacy of investment firms.
- The Alternative Investment Fund Managers Act (2013:561) (*lag om förvaltare av alternativa investeringsfonder*) implements the EU Alternative Investment Fund Managers Directive (AIFMD), and regulates the management of alternative investment funds and the supervision of entities that manage such funds.
- The Swedish UCITS Act (2004:46) (*lag om värdepappersfonder*) implements the EU Undertakings for Collective Investment in Transferable Securities Directive (UCITSD) and regulates the operations of UCITS funds.

The most relevant laws and regulations related to insurance business

- The Insurance Business Act (2010:2043) (*försäkringsrörelselag*) implements the EU Solvency II Directive and regulates insurance activities conducted by insurance companies.
- The Insurance Distribution Act (2018:1219) (*lag om försäkringsdistribution*) implements the EU Insurance Distribution Directive and regulates insurance distribution by insurance companies and insurance intermediaries.
- The Insurance Contracts Act (2005:104) (*försäkringsavtalslag*) regulates insurance contracts and the legal relationship between the insurer and the insured (or other persons covered by the insurance).
- The Foreign Insurance Contracts Act (1998:293) (*lag om utländska försäkringsgivares och tjänstepensionsinstituts verksamhet i Sverige*) regulates the insurance business of foreign insurers in Sweden.

Crowdfunding

Crowdfunding activities are regulated in the EU Crowdfunding Regulation and the Swedish supplement law to this regulation. These regulations set out requirements for the provision of crowdfunding services and the business of crowdfunding service providers. A licence from the SFSA is required to provide crowdfunding services. The SFSA is the supervisory authority of companies conducting crowdfunding business.

Other regulations and guidelines

Entities conducting fintech business may also have to comply with certain other regulations, such as the Anti-Money Laundering and Terrorism Financing Act (2017:630) (*lag om åtgärder mot penningtvätt och finansiering av terrorism*) (the AML Act), the EU General Data Protection Regulation (GDPR), and the Supervision of Credit Institutions and Investment Firms Act (2014:968) (*lag om särskild tillsyn över kreditinstitut och värdepappersbolag*) (which implements the EU Capital Requirements Directive).

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

Crypto assets are essentially unregulated in Sweden. The SFSA has warned about investment in crypto assets due to the lack of supervision and consumer protection. Besides this, there is limited guidance on how crypto assets should be handled.

Pursuant to the Currency Exchange and Other Financial Activities Act (1996:1006), a natural or legal person who intends to conduct business in Sweden that includes management and trading of virtual currencies must apply for registration with the SFSA. Management of virtual currencies encompasses the provision of services to safeguard private cryptographic keys on behalf of customers for the purpose of holding, storing and transferring virtual currencies. Trading of virtual currencies means exchanges between virtual currencies and fiat currencies, electronic money or other virtual currencies. As a result of the registration, the registered person must comply with the AML Act.

However, the EU Markets in Crypto-Asset Regulation (MiCA), which entered into force on 29 June 2023 and will apply from 30 December 2024, may change the unregulated area of crypto assets in Sweden. MiCA is expected to have a significant impact on crypto assets within the EEA market by introducing a harmonised regulatory framework for crypto assets. MiCA will, inter alia, introduce disclosure requirements for the issuance and admission to trading of crypto assets. MiCA will further introduce licence requirements for issuers and offerors of certain kinds of crypto assets.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

Pursuant to the Payment Services Act (2010:751), entities with a turnover for payment services exceeding an equivalent of €3m per month require a licence as a payment institute from the SFSA to provide payment services. There are, however, exemptions to this licence requirement. An entity with a turnover for payment services less than €3m per month may apply to the SFSA as a registered

payment service provider to provide payment services without a licence. However, providers of payment initiation services always require a licence and are not covered by the exemption. Further, account information service providers (AISP) may apply to the SFSA to be exempted from the licence requirement regardless of whether the turnover for payment services exceeds €3m per month. To be exempted, the AISP shall instead, inter alia, have liability insurance. The SFSA registers those who have been exempted from the licence requirement.

Certain entities, for instance credit institutions, do not require a separate licence as payment services are covered by the licence requirement in the Banking and Financing Business Act (2004:297). Further, entities licensed to issue electronic money under the Electronic Money Act (2011:755) (ie, institutions for electronic money and registered issuers) may, in addition to issuing electronic money, provide payment services under the Payment Services Act (2010:751).

Payment service providers are subject to certain requirements, such as information and capital requirements. The Payment Services Act (2010:751) also stipulates certain qualification requirements on the management. Payment service providers must further have a system of appropriate measures and controls for operational and security risks related to the provided payment services.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg regulatory sandboxes and accelerator programmes) and regulations regarding special support.

So that financial regulation does not prevent the development and innovation in the financial sector, the SFSA has established an innovation centre to facilitate a dialogue with companies conducting innovative business. The innovation centre is supposed to be the first point of contact for companies that are uncertain about the rules, processes and principles related to innovation. It enables companies to get information on relevant regulations and supervision related to fintech business. However, the SFSA does not engage in sandbox activities.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

The Payment Services Directive (PSD2) is implemented in Sweden primarily by amendments to the Payment Services Act (2010:751). PSD2 has broadened the scope of the Payment Services Act to cover new types of payment and account information services. It stipulates requirements for third-party operators – ie, operators other than banks – to obtain a licence from the SFSA or similar authority within the EU/EEA to provide payment initiation services and collect account information by accessing bank accounts.

Following the implementation of PSD2, the legislator has made further amendments to the Payment Services Act (2010:751). The amendments included a prohibition from having credit purchases as the default payment alternative for online consumer payments in case there are other payment alternatives offered.

Switzerland

Marco Häusermann*
Niederer Kraft Frey, Zurich
marco.haeusermann@nkf.ch

Simon Bühler†
Niederer Kraft Frey, Zurich
simon.buehler@nkf.ch

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

In Switzerland, there are few specific laws and regulations regarding fintech. This results from the technology-neutral approach of the Swiss supervisory law: ie, the regulation must be so open and flexible that it does not hinder future technological developments and can also be applied under changed conditions.

Business activities with similar characteristics fall under the same requirements (whether advanced technology is used or not) in order to level the playing field. This allows for more flexibility and higher stability of the existing legal framework.

On the other hand, this results in a number of different federal acts and ordinances that may be applicable to fintech companies, eg, the Anti-Money Laundering Act (AMLA), the Banking Act (BA), or the Financial Market Infrastructure Act (FinMIA). The most relevant aspects are summarised below.

Distributed ledger technology (DLT) trading facility

On 1 August 2021, following the principle of technology neutrality (see above), the Federal Act on the Adaptation of Federal Law to Developments in Distributed Electronic Register Technology (DLT Act) and the associated ordinance was enacted, resulting in several amendments to the already existing laws.

The DLT Act introduced a new type of licence for companies seeking to operate a DLT trading facility, which is defined as 'a commercially operated institution for multilateral trading of DLT securities whose purpose is the simultaneous exchange of bids between several participants and the conclusion of contracts based on non-discretionary rules' (Article 73a, FinMIA). In addition, a DLT trading facility must either:

- admit 'natural persons or legal entities, provided that they declare that they are participating in their own name and for their own account' as participants (Article 73c, FinMIA);

* Marco is a specialist in international and domestic banking, finance and debt capital market transactions as well as restructurings and insolvency matters.

† Simon is a member of NKF's Banking, Finance & Regulatory team. His practice focuses on banking and financial markets regulation as well as compliance (including AML) and regulatory litigation.

- hold 'DLT securities in a central custody based on uniform rules and procedures' (Article 73a, FinMIA); or
- clear and settle 'transactions in DLT securities based on uniform rules and procedures' (Article 73a, FinMIA).

DLT securities are standardised book-entry securities suitable for mass trading in the form of either: (1) ledger-based securities (*Registerwertrechte*) or (2) other uncertificated securities that are held in distributed electronic registers and use technological processes to give the creditors, but not the obligor, power of disposal over the uncertificated security.

The possibility of admitting end customers as participants and offering settlement and custody services alongside trading (which, for example, a stock exchange is not allowed to do) is a unique combination. This combination of previously incompatible services could possibly lead to innovative business models. To date, the Swiss Financial Market Supervisory Authority (FINMA) has not yet issued a licence for a DLT trading facility.

Fintech licence

In order to foster innovation, a fintech licence (sometimes also referred to as the 'banking licence light') was implemented in the Swiss legal system in Article 1b of BA. This licence allows entities to accept deposits (in certain cases also in the form of crypto-based assets) up to a threshold of CHF 100m under certain conditions. Neither can the deposits be invested, nor can there be interest paid on them. Please see Question 4.

Insurtech

Broadly speaking, all insurance companies require authorisation in the form of a licence issued by FINMA. Based on the revised Insurance Supervision Act and the pertaining ordinance which became effective on 1 January 2024, in order to safeguard the future viability of the Swiss financial centre, the Federal Government will be able to exempt innovative insurance companies in whole or in part from supervision and attach conditions to this exemption, taking into account factors such as the business model, the risks of the insurance product for the policyholders concerned, the business volume and the group of insured persons.

Crowdfunding

Providers of crowdfunding platforms and project developers must verify whether they need to obtain a banking licence from FINMA or comply with other financial markets laws before channelling funds through their accounts. In July 2020, FINMA published a crowdfunding fact sheet, pursuant to which crowdfunding platforms generally do not need to obtain a banking licence if the funds are not channelled through accounts of the platform or, if channelled through accounts of the platform, if they do not exceed CHF 1m.

However, if funds are accepted on a commercial basis and are being held for more than 60 days, they are subject to a licence. The same applies if they channel funds with an aggregated amount

exceeding CHF 1m. Also, if funds are channelled through accounts of the platform, anti-money laundering (AML) laws are likely to be applicable. See Question 4.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

Switzerland has only a few specific regulations governing crypto assets. Following the principle of technology neutrality (see Question 1), financial intermediary activities involving crypto assets fall under the same regulations as other financial services, eg the AMLA.

As a result of the newly implemented DLT Act, a fintech or banking licence is now mandatory for the collective custody of crypto assets on a commercial basis for clients (see Question 4 for exemptions to the licence requirement). Furthermore, the principle of asset segregation of crypto-based assets came into force. This provides investors with better protection, especially in the event of bankruptcy of custodians, with respect to their crypto-based assets provided they are held in readiness for the customer at all times.

Regarding cryptocurrencies, the Federal Government attaches great importance to ensuring that the same rules apply to cryptocurrencies as to fiat monetary assets. Therefore, a Swiss financial intermediary holding (or helping to transfer) cryptocurrencies is subject to the same obligations as when handling fiat money. However, the AMLA thresholds are lower for cryptocurrencies compared to fiat money. Due to the increasingly decentralised models of cryptocurrencies, a financial intermediary activity (triggering the duties under the AMLA) does not require that the financial intermediary has at any point in time the power of disposal over the cryptocurrencies. Rather, it is sufficient that the financial intermediary supports the transfer of virtual currencies to a third party and thereby maintains a permanent business relationship with its contracting party.

In December 2023, FINMA also published a guidance regarding staking which FINMA defines as 'the process of blocking native crypto assets at the staking address of a validator node in order to participate in a blockchain validation process based on a proof-of-stake consensus mechanism'. FINMA reiterates that the holding of payment tokens in a collective account with clear customer shares requires a banking licence or a fintech licence, provided that the payment tokens are held in readiness at all times. A banking licence is not required for individual custody of payment tokens held in readiness at all times. However, such custodians are subject to the AMLA as financial intermediaries and must join a self-regulatory organisation for the purposes of AML supervision.

As regards the staking of crypto assets, FINMA primarily distinguishes between staking on the institution's own account and staking carried out on behalf of the customer for the customer's account. If the crypto assets are staked on the institution's own account, they cannot be segregated in the event of bankruptcy and attract capital requirements for the financial institution. On the other hand, when the staking is carried out on behalf of the customer for the customer's account, according to FINMA, the legal position is uncertain. In these situations, the exact staking mechanism of the blockchain concerned needs to be analysed on a case-by-case basis (in particular if there is a risk of slashing and/or a delay in unstaking (lock-up/exist period). The qualification of whether crypto assets are held in readiness for the customer at all times is important for financial institutions as to whether the crypto assets held by FINMA-supervised institutions will be segregated

in bankruptcy, as depending thereon capital adequacy requirements may apply. For non-FINMA supervised market participants, FINMA clarifies that it generally does not intend to require a banking/fintech licence if they engage in custodial direct staking commissioned by customers for their own account provided that the staked payment tokens continue to be held in individual custody: ie, there is a separate and assignable blockchain address for each customer (at the levels of the original custody address, staking address and withdrawal address) and the provider holds the withdrawal keys itself. However, in such case, the market participant will be nevertheless subject to AMLA regulations and become a member of a self-regulatory organisation for AMLA supervision.

Also, in the case of crypto assets, a main question is whether the coins/tokens qualify as 'securities' (*Effekten*) and/or as 'financial instruments' (*Finanzinstrumente*) under Swiss law. The legal nature of coins/tokens is controversial. However, FINMA has provided some guidance in respect of whether digital ledger coins/tokens qualify as a 'security' (though subject to a caveat in its guidance that it will correct its practice if a court reaches a different conclusion). In principle, FINMA distinguishes between three types of tokens: payment tokens, utility tokens and investment tokens.

- Payment tokens (such as cryptocurrencies) are accepted as a means of payment for the purchase of goods or services or are intended to serve the transfer of money and value. According to FINMA, pure payment tokens do not qualify as 'securities', but their issuance generally is subject to anti-money laundering laws.
- Utility tokens provide access to a digital usage or service that is provided on or using a blockchain infrastructure. In order to qualify as utility tokens, the digital usage or service needs to be fully operational at the time of the token issuance (otherwise, it has more the character of an investment token; see below). According to FINMA, pure utility tokens do not qualify as 'securities'.
- The investment token category includes tokens that represent assets. Such tokens may represent a debt claim against the issuer or a membership right in the corporate law sense. According to the economic function, the token thus represents a share, a bond or a derivative financial instrument. According to FINMA, investment tokens generally do qualify as 'securities'.

Hybrid tokens are also possible. For example, a token can qualify as a utility token, a payment token or an investment token at the same time. In this case, we would expect that FINMA would qualify such hybrid tokens (if they contain an element of a 'security') as a 'securities' token, which usually entails stricter regulation.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

Payment service providers

All providers that operate payment systems, defined as 'an entity that clears and settles payment obligations based on uniform rules and procedures' (Article 81, FinMIA), are subject to a licence if (1) the payment system is deemed to be of systemic relevance or if (2) supervision is required for the protection of financial market participants.

However, payment systems operated by a licensed bank (Article 4, Paragraph 2, FinMIA) or by or on behalf of the Swiss National Bank (SNB) (such as the Swiss Interbank Clearing (SIC) payment systems for CHF and EUR) are not subject to a licensing requirement. Systemically important payment systems are subject to supervision and reporting obligations to the SNB (Article 83, FinMIA).

Furthermore, SNB has wide discretion to subject foreign payment systems of systemic relevance to Switzerland to its supervision.

As a result of the high thresholds and exceptions stated above, there are currently no FINMA-licensed payment systems, and only two payment systems of systemic relevance under the supervision of the SNB in Switzerland, namely the SIC and the foreign payment system Continuous Linked Settlement (CLS), which is jointly supervised by all participating central banks under a cooperative oversight agreement. Nevertheless, all payment systems that allow third parties to transfer values, and thus qualify as financial intermediaries, are subject to the AMLA duties.

Digital wallet providers

There are two types of wallets: non-custodian wallets and custodian wallets.

The providers of non-custodian wallets do not have access to their clients' private keys. Thus, other than providing the software, they are not directly involved in the transfer of assets. As a result, the providers of non-custodian wallets do not qualify as financial intermediaries and are not subject to the AMLA. It is to be noted that providers of non-custodial wallets that also support the transfer of virtual currencies to a third party in any form are subject to the AMLA duties if the providers are in an ongoing business relationship with the client.

Custodian wallet providers, on the other hand, keep and manage their clients' private keys safe. They have also the direct power of disposal over third-party assets, meaning they can provide a payment transaction service. The professional service for payment transactions is subject to the AMLA. In addition, questions also arise under banking law. According to FINMA, a banking licence may generally not be required under strict conditions if the crypto assets are held separately per client on a blockchain and can be allocated to the individual client at any time.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

There are two main regulatory alleviations implemented in Swiss law regarding fintech companies.

Sandbox

Implemented in the Banking Ordinance (BO) in August 2017, the so-called sandbox allows fintech companies to accept deposits up to a maximum of CHF 1m without the requirement of a specific licence, provided that (1) the assets are not used for so-called interest rate differential business and

(2) the depositors are informed, before they make a deposit, that the company is not supervised by FINMA and that the deposit is not covered by deposit insurance (Article 6, Paragraph 2, BO).

Article 5 of BO stipulates inter alia that, if settlement of the funds received by precious metal dealers, asset managers or similar companies takes place within 60 days, those funds do not qualify as deposits. This allows certain crowdfunding companies to be exempt from the licence requirement. In contrast to the fintech licence (see below), the deposits can be invested. This solution allows fintech companies to test their business strategy without having to meet the entry barrier of a banking or fintech licence.

Fintech licence

Financial service providers can also obtain the fintech licence. With this licence, the financial service providers are able to accept deposits from the public, if (1) the amount of the deposits (in certain cases also in the form of crypto-based assets) does not exceed CHF 100m (aggregated) and (2) the deposits are neither invested nor interest-bearing (Article 1b, Paragraph 1, BA). In special cases FINMA can issue the fintech licence at its discretion to a company that accepts deposits exceeding the threshold of CHF 100m, or publicly recommends itself to do so, if the company neither invests nor pays interest on the deposits and ensures the protection of clients by taking special precautions (Article 1b, Paragraph 5, BA). The fintech licence is not an ordinary banking licence, meaning that these financial service providers do not have the same regulatory status as an 'ordinary' bank. On the other hand, the companies are subject to less strict requirements when obtaining and maintaining the licence.

Since 2016, financial intermediaries have been allowed to use video and online identification for customers in the process of opening a bank account. Furthermore, on 1 June 2021, the possibility of scanning chips embedded in biometric identity documents in the online identification process was implemented. These measures considering the newest technological developments could help financial intermediary startups to reduce their costs, especially when purely offering online services.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

In Switzerland (contrary to the EU), there is currently no legislation specifically regulating open banking. Accordingly, the general regulations for financial services have to be adhered to: eg, regarding banking secrecy (Article 47, BA). For the time being, Switzerland is refraining from obliging regulated financial institutions to open interfaces. However, various players, such as the Swiss Bankers Association, have launched initiatives to coordinate and facilitate frameworks and standardise technical interfaces while other financial institutions voluntarily offer application programming interface (API) services.

United Kingdom

Caroline Phillips*
Slaughter and May, London
caroline.phillips@slaughterandmay.com

Nick Bonsall†
Slaughter and May, London
nick.bonsall@slaughterandmay.com

Tim Fosh**
Slaughter and May, London
timothy.fosh@slaughterandmay.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

There continues to be no single overarching regulatory regime specific to fintech companies in the United Kingdom. The test for whether a particular fintech company or service will be subject to regulation remains whether its business involves it carrying on one of a number of 'specified activities' which, subject to a range of tests, exemptions and exclusions, would require authorisation for a firm to conduct by way of business in the UK.

The key development in 2022/2023 in this respect has been the Financial Services and Markets Bill 2023 (FSMA 2023), which has both (1) made substantial changes to the regulation of a number of specified activities which fintechs often perform; and (2) anticipates further structural reform to the UK financial services regime, whilst not providing definitive dates for these further changes to be made.

In addition to FSMA 2023, there have been a number of other minor changes and proposals announced which might impact fintechs.

Payment services

FSMA 2023 provides that the Payment Services Regulations 2017 (PSRs) and Electronic Money Regulations 2011 (EMRs) will be repealed but does not state when this will take place. The UK government's intention is that the provisions in the PSRs and EMRs will be transferred into primary legislation or into the rulebooks of the Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) as appropriate. A detailed consultation process on the way this will be done will take place prior to this transfer.

Specific shorter-term changes to payment services regulation are described in Question 3.

---

* Caroline is a financing partner at Slaughter and May with a broad international practice covering banking, capital markets, securitisation, derivatives and structured finance in which she advises issuers, borrowers and counterparties of all types.

† Nick is a partner in the Financial Regulation group at Slaughter and May with a broad financial institutions practice, including extensive experience advising insurers, banks and asset managers on a range of stand-alone advisory and transactional projects.

** Tim is a senior counsel in the Financial Regulation group at Slaughter and May with a practice spanning transactional and non-transactional work for both financial and (traditionally) non-financial institutions.

Lending money and taking deposits

There have been no major changes to the regulation of banking activities as they are performed by fintechs specifically. However, banking regulation more generally is currently subject to considerable change, particularly as a result of the implementation of the Basel 3.1 standards.

Open banking

FSMA 2023 has not made any substantial changes to the regulation of open banking in the UK. However, there is continuing momentum on this front from regulators and government alike, as discussed in more detail in Question 5.

Buy now pay later

Again, there have not been any shifts in the regulation of buy-now-pay-later ('BNPL') services in 2022/2023. However, the previous government had consulted on new legislation which would bring substantial numbers of BNPL agreements within the 'regulatory perimeter'. The new Labour government (in power since July 2024) indicated in its manifesto that it will prioritise regulating the BNPL sector, meaning that the implementation of these proposals is likely to occur relatively soon.

Under these proposals, third-party lenders who offer BNPL services to consumers are likely to find themselves subject to consumer credit regulation in future (albeit not in its entirety – in particular the usual pre-contractual requirements will be disapplied) while providers of goods and services who offer BNPL services to their consumers will likely not fall within the scope of regulation.

Detailed proposals are yet to be announced and are likely to remain forthcoming in the short-to-medium term. Before BNPL firms become subject to full regulation, they will be able to rely upon a 'temporary permissions regime' which will give them deemed authorisation while the FCA considers their full application.

Crypto assets

See Question 2.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

The main change which has taken effect regarding crypto regulation in 2022/2023 has been the extension of the financial promotion regime to include a number of types of crypto asset. Previously, crypto assets had not been subject to the prohibition in UK law against promoting investment activity in respect of specified investments, unless the person making the invitation or inducement is authorised or the promotion has been approved by an authorised person.

Since August 2023, this has now changed so that 'qualifying crypto assets' (defined as crypto assets which are both fungible and transferable) are now within scope of UK financial promotion regulation. This means that firms seeking to market crypto assets will need to (1) be registered with

the FCA as a crypto asset firm; (2) structure their marketing so as to fall within an exemption to the prohibition against marketing by unauthorised persons; or (3) rely upon an authorised person to approve the relevant marketing which has become more complex since February 2024 and the introduction of a specific permission that authorised persons are required to apply for if they wish to approve promotions of unauthorised persons).

In addition, marketing materials which qualify as financial promotions will now need to be clear, fair and not misleading (in addition to a number of other requirements such as including a cooling-off period for consumers in certain circumstances). The FCA has recently increased enforcement action against illegal or non-compliant promotions of other investments (ie, non-crypto assets, which were already within the financial promotion regime), and is likely to be equally vigilant in its regulation of crypto assets promotions.

The FCA has also set out new regulatory expectations in relation to the compliance of cryptoasset firms with the 'Travel Rule', the global recommendation by the Financial Action Task Force (FATF) requiring greater transparency for crypto asset transfers. Firms will need to take all reasonable steps and exercise all due diligence to comply with the Rule, and fully comply with it when transferring crypto assets to any other jurisdiction which has implemented the Rule.

FSMA 2023 also provides extensive optionality for the UK government to increase regulation of crypto assets in other ways in the future. Most notably it has amended the definition of 'investment' to include crypto assets (meaning that existing regulated activities can be extended to include those in respect of crypto assets) and has explicitly empowered the Treasury to regulate payments and systems relating to 'digital settlement assets'.

In November 2023 the FCA published a discussion paper setting out its high-level proposals for the regulation of stablecoin issuers (including rules regarding conduct of business, prudential requirements and the application of the new Consumer Duty to issuers). The deadline for stakeholders to respond to the FCA's paper was February 2024, and the FCA continues to consider next steps.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

There have been no major changes to the scope of payments regulation as a result of FSMA 2023, though it is clear that significant shifts in how this regulation works are forthcoming (see Question 1).

One important development was the introduction of an obligation on the Payment Systems Regulator (PSR) – the regulatory body responsible for supervising payment systems – to ensure that payment service providers are required to reimburse consumers where fraudulent payments are executed over the Faster Payments Scheme (with a similar requirement likely to soon be imposed on payments through the CHAPS system as well).

Fraudulent payments, particularly 'authorised push payment' frauds, have also been considered by the British courts – in July 2023 the UK Supreme Court ruled in the case of *Philipp v Barclays Bank* that there was no common law duty (often called a *Quincecare* duty) for payment service providers to

refrain from executing payment instructions where that bank has reasonable grounds to believe that the instructions have been given as part of an attempt to defraud the customer.

The government also consulted on payment service regulation reform as part of its Future Payments Review, looking to optimise customer journeys while also ensuring that the UK remains competitive as a venue for payment institutions to do business. The recommendations coming out of this review were published in November 2023; the main recommendation was that the UK government develop and adopt a national payments strategy, whilst other more concrete recommendations related to items such as improvements to strong customer authentication, the integration of minimum dispute resolution into open banking and a review of the PSR's new authorised push payment fraud rules discussed above.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

FSMA 2023 has provided for the creation of a number of new financial market infrastructure (FMI) sandboxes by the Treasury, intended to test the efficiency or effectiveness of the carrying on of FMI activities in a particular way, and to assess whether or how relevant enactments should apply in relation to FMI activities carried on in that way.

The first such sandbox created has been the Digital Securities Sandbox. As part of this scheme, firms will be able to operate FMIs which use 'innovative digital asset technology, performing the activities of a central securities depository (specifically notary, settlement and maintenance), and operating a trading venue, under a legislative and regulatory framework that has been temporarily modified to accommodate digital asset technology'.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

At the end of 2022, the Treasury, Competition and Markets Authority (CMA), FCA and PSR published a joint statement on open banking reaffirming their commitment to developing open banking and continuing the work of the Joint Regulatory Oversight Committee.

The Committee has set out a 'roadmap' in which it outlines the ways in which it proposes to enable open banking to continue to grow and evolve; in 2023 they have focused upon developing an understanding of how financial crime might impact open banking services, and in 2024 have built upon this through publishing a new paper setting out proposals for a new industry body to supervise open banking, as well as by improving data sharing to prevent fraud and financial crime, and supporting the development of commercial and liability frameworks.

Middle East

Iran

Amir Mirtaheri*
Sabeti & Khatami, Tehran
amir.mirtaheri@sabeti-khatami.com

Nika Baghestani†
Sabeti & Khatami, Tehran
nika.baghestani@sabeti-khatami.com

Niloofar Massihi‡
Sabeti & Khatami, Tehran
niloofar.massihi@sabeti-khatami.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

There is no overarching fintech law in Iran and the diverse activities often classified as fintech are only partially and recently regulated as the regulators navigate new financial technologies introduced by industry players.

The Central Bank of Iran (CBI) has issued policy papers and regulations related to digital payments, digital banks, digital asset exchanges and digital custody (wallets). It has also introduced microfinancing regulations which bear on digital lending activities. The Exchange and Securities High Council (Securities Council) and the Securities and Exchange Organization (SEO), the capital market regulators, have introduced regulations on digital capital raising (crowdfunding) and certain asset management technologies (algorithmic trading). Central Insurance of Iran (CII), the insurance regulator, has introduced some regulations relevant to insurtech.[1] All these regulatory frameworks are discussed below.

To date, there is no specific regulation on digital savings mechanisms such as digital funds. A host of other fintech services such as financial management and business intelligence technologies, digital accounting, KYC, credit rating/scoring, due diligence and risk analytics remain either unregulated or subject to general subject-matter regulations.

Digital payments

CBI regulation of digital payments has created a three-layer structure consisting of (1) a central payment network called Shaparak connecting CBI, banks and payment service providers (PSPs), (2) PSPs and (3) payment facilitators, which are intermediaries between PSPs and sellers of goods and services.

* Amir is a senior associate at Sabeti & Khatami and advises on corporate and financial law, usually in matters with a cross-border element. Amir has extensive corporate and M&A experience in the e-commerce and fintech sectors.

† Nika is an associate at the firm and advises clients on corporate, contract and investment matters. She is experienced in advising VCs and e-commerce and technology startups in relation to investment and M&A transactions.

‡ Niloofar is a senior associate at Sabeti & Khatami and advises clients on corporate, contract and capital market matters. She is experienced in negotiating complex mergers and structuring financial instruments in the tech sector.

1 Insurance and technology.

CBI's Regulation on Establishment, Operation and Monitoring of Payment Service Providers (PSP Regulations), approved in 2011, is discussed in Question 3.

CBI's latest regulation on payment facilitators was issued in 2018. The regulation sets out:

- payment facilitators' corporate and management requirements;
- the qualification process (including required contractual arrangements with a PSP and with Shaparak);
- the scope of permitted activities (limited to providing payment services to sellers); and
- capital adequacy, know your customer (KYC), record-keeping, reporting, anti-money laundering (AML) and counter-terrorist financing (CTF) rules and settlement processes.

PSPs have supervisory responsibilities vis-à-vis payment facilitators with whom they enter into payment agreements.

CBI has a specific regulation on card-not-present (CNP) payments dating back to 2017 and covering matters such as risk management (including via transaction limits), transaction authentication, and record-keeping, incident reporting and outsourcing rules.

In 2022, the CBI began a trial implementation of digital checks, with three banks initially joining the programme. This was based on the recognition of such checks as valid instruments of payment under the 2018 amendments to the Check Act. Currently, half a dozen banks are issuing digital checks to their customers on a trial basis, although the momentum is likely to grow as Parliament is deliberating on a proposed law to abolish paper checks in three years. The shift to digital checks is intended to address common problems associated with physical checks such as loss, forgery, signature issues and other discrepancies.

Digital banks

During the past decade, digital banking has thrived in Iran in part because of the digital banking mandate in the Fourth Development Plan Law, 2004 and the subsequent Digital Banking Regulations approved by the Council of Ministers on 13 March 2008.

The latter Regulations, which cover mobile and online banking as well as necessary hardware infrastructure such as point-of-sale and ATM networks, created a mandate for CBI, other government entities and banks to facilitate rapid expansion of secure digital banking. The Regulations also required CBI to introduce further regulations of various digital banking services. Except for the case of virtual banking discussed below, no such regulation has been publicly announced, although CBI seems to have been in close coordination with banks in relation to development of their digital services per CBI news announcements.

CBI did introduce its regulations on fully digital banks (virtual banks) in 2011. These regulations set out virtual banks' establishment requirements (such as CBI licensing process and single ownership limits), required operational plans and management qualifications, permitted activities, and record-keeping, data security and reporting rules.

Digital custody

Two pieces of regulation deal with digital wallets:

- Directive No H54251T/107837 of the Council of Ministers dated 6 November 2018 (Fintech Directive); and
- CBI's 2020 Digital Wallet Operators Regulation (Wallet Regulation).

Details of these are discussed in Question 3.

Digital asset exchanges

CBI has regulations on trading crypto assets discussed in Question 2.

Digital lending

There is no regulation specifically dealing with digital lending activities, but CBI has recently issued the Implementation Directive on Micro-lending, and a few banks have introduced microfinancing via their digital platforms based on their internal credit scoring systems.

In addition, an official platform was recently launched (Setareh Samat) where borrowers can pledge their shares in public companies as security in support of their loan applications to banks. The platform is intended to be used for pledging other types of securities and financial instruments in the future, such as gold certificates.

There is a considerable demand in the market for microfinancing and buy now pay later schemes, and many e-commerce companies are exploring digital lending arrangements for their customers. It would be of no surprise if CBI introduces specific regulations in this matter in the near future.

Digital capital raising

The primary regulation here is the 2018 Crowdfunding Directive by the Securities Council. Crowdfunding operators must obtain a licence from the special evaluation committee established under the Directive.

Once a project is approved by a licensed operator in accordance with the Directive, and the necessary contractual arrangements are entered into between the operator and the fund applicant, an exchange ticker is assigned by Farabourse, one of the two securities exchanges in Iran, following which public fundraising may commence.

There are limits on the size of the fund to be raised for a single project and on the aggregate at any given time of ongoing fundraising targets by a single operator. Fund applicants are required to provide at least 10 per cent of their project's capital needs in equity.

Asset management technologies

There is no regulation of asset management technologies except for SEO's 2020 Regulation of Algorithmic Trading, which could be used as part of a fintech approach to asset management. The regulation sets out the technical requirements for permissible machine trading such as frequency limit, permitted time windows for order submission, logging requirements, record-keeping rules and capability to immediately cancel orders or terminate algorithms when required by law. High frequency trading is prohibited.

Insurtech

In the two sets of regulations issued in 2019, CII addressed online insurance activities such as brokerage services, marketing, sales and payments, and set out requirements such as an electronic commerce licence from the Ministry of Industry and minimum hardware and software capabilities. More recently, CII and Iran's Vice Presidency for Science and Technology have entered into an agreement to support development of insurtech. As a result, more regulatory activities in this matter may be enacted in the future.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

The focus of crypto regulation has been on mining, which witnessed a boom during 2020 and 2021 thanks to heavily subsidised electricity prices. Having started from an outright ban in early 2021, the government moved to allow crypto mining and adopted new regulations.

Under the most recent crypto mining regulations approved in late 2022 and in 2023 by the Council of Ministers, miners can use specific energy sources to meet their needs. Examples are setting up renewable energy plants, using energy saving certificates, investment in gas-to-electricity power plants or purchasing electricity at unsubsidised rates. The Ministry of Energy has introduced detailed regulations on electricity tariffs applicable to mining facilities.

In most cases, miners must also obtain approval from the Ministry of Energy or the Ministry of Petroleum (depending on the source of their electricity), the Environmental Protection Organisation and the National Standard Organisation before they can obtain an operation license from the Ministry of Industry. Furthermore, mining centres are divided into two categories – 'large-scale' and 'regular' – although the details of what constitutes each category and the regulatory consequences are yet to be announced by the Ministry of Industry. Mining activities will be subject to ceilings to be determined by the CBI.

Still, some previous restrictions continue to apply: mining facilities must not be in the vicinity of large population centres and they may not operate during peak hours of electricity consumption.

Outside mining, CBI has maintained a fairly sceptical attitude in regulating the use and trading of crypto assets. In early 2019, it issued interim regulations on cryptocurrencies (Crypto Regulations), which prohibited the use of most crypto assets (including global cryptocurrencies, tokens based on tangible or intangible assets and tokens based on fiat currencies other than rial

central bank digital currency (CBDC)) as means of payment. Only CBI-regulated banks may issue fiat-based tokens (other than rial CBDC); and issuance of gold and metal-based tokens requires CBI's permission and bank guarantees. The regulations also dealt with ICOs.

The Crypto Regulations are fairly aggressive towards crypto exchanges. The trading of most crypto assets (such as global cryptocurrencies and gold, metal and hard currency-based tokens) may only take place in CBI-licensed crypto exchanges. While traditional licensed exchange houses may apply for a crypto exchange licence, it is unclear whether other exchange platforms are able to obtain such licences. Furthermore, CBI determines the list of cryptocurrencies that may be traded in licensed exchanges. AML and KYC rules apply, and customers and transactions' information must be recorded and reported to CBI.

The Crypto Regulations also indicated the CBI's plans to introduce its rial CBDC, known as digital rial. Digital rial and tokens based on it may be used as means of payment. According to the then-CBI governor, the CBI started a 'pre-pilot' phase of digital rial in late 2022 via limited circulation of the currency by select banks and commercial retailers, but there has been no report of further developments on this since then.

The only legitimate use of global cryptocurrencies CBI has thus recognised is for licensed miners to use their mined cryptocurrencies to finance import of goods and services into the country using the Ministry of Industry's national trade portal.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

Payment service providers

The PSP Regulations set out a long list of requirements to establish a PSP including founders' qualifications, shareholders restrictions and minimum capital requirements, CBI's licensing and Shaparak's technical approval processes, required internal controls, and audit, reporting and AML rules.

Digital wallets

The Fintech Directive designates CBI as regulator of digital wallets. CBI's Wallet Regulation sets out the general framework for open wallets by setting out:

- the requirements for wallet service providers (such as minimum capital);
- capital adequacy, KYC, transaction monitoring and recordkeeping rules;
- required internal controls;
- permitted transactions and turnover caps for commercial and personal wallets;
- responsibilities of wallet service providers; and
- the corresponding roles of national payment platforms, PSPs and credit institutions.

Wallet and transaction information must be recorded in a national database.

CBI has reportedly issued regulations on micropayments from wallets and transaction monitoring guidelines for service providers, but these are not publicly available.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

The government has, at the highest level, supported an open, competitive and innovative fintech landscape. In the Fintech Directive, the Council of Ministers required CBI to take anti-monopoly measures in the digital payment sector, banks and PSPs to offer service to licensed fintech companies and government entities to facilitate receipt of small government dues via fintech intermediaries. The Directive also prohibited CBI from imposing business restrictions on fintech companies beyond its strict role as the regulator of the financial sector.

To foster innovation, the Fintech Directive also required CBI to set up a regulatory sandbox, which was launched in June 2022 to monitor novel solutions, assess risks and help formulate regulatory responses. CBI officials have also expressed interest in the development of supervisory and regulatory technologies (RegTech) to expedite much-needed banking reform.

An agreement between CII and the Vice Presidency for Science and Technology, reported in early September 2022, includes creation of a regulatory sandbox for assessment of innovations in the insurance industry as one of the measures in support of Insurtech.

As far as we are concerned, fintech accelerator programmes exist but none of them are directly affiliated with the government. Larger accelerators are sponsored by banks, financial institutions, major fintech companies and technology universities. Banks have shown particular interest in the recent years in supporting fintech startups and in acquiring fintech targets, mostly in digital payments, digital banking and wallets.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

There are currently no open banking regulations in Iran. However, the CBI, in recognition of its significance, created an open banking committee within its digital banking task force nearly two years ago. The committee is responsible for identifying supervisory and operation procedures for open banking and has reportedly produced an internal CBI document on the overall architecture of open banking in Iran. It is reasonable to anticipate some regulatory creation in this matter in the near future – although any regulation must be reconciled with CBI's strict customer data privacy, security and confidentiality regulations for banks such as those stipulated in CBI's Directives No 7075 of 7 January 1996, and H444 of 25 September 2008. Significant expansion of entities under CBI's supervision following widespread open banking activities and the resources it will entail may be another reason for CBI's slow pace in this matter.

There are open banking platforms with the capacity to connect banks' APIs to fintech companies but no substantial open banking activities have been reported, perhaps in part due to the regulatory vacuum.

United Arab Emirates

Nadim Bardawil*
BSA Ahmad Bin Hezeem & Associates, Dubai
nadim.bardawil@bsabh.com

Marina El Hachem†
BSA Ahmad Bin Hezeem & Associates, Dubai
marina.elhachem@bsabh.com

Sam Moore‡
BSA Ahmad Bin Hezeem & Associates, Dubai
sam.moore@bsabh.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

The United Arab Emirates (UAE) continues to hold its position as the leader in fintech in the Middle East. This position is maintained with the help of supportive governmental policies and, most importantly, by the implementation of attractive programs, both onshore and in free zones. The UAE consists of onshore and financial free zone jurisdictions, to which different legal frameworks apply.

There are currently two financial free zones in the UAE: the Dubai International Financial Centre (DIFC) and the Abu Dhabi Global Market (ADGM).

Contrary to other jurisdictions, the UAE does not have a single regulator responsible for the supervision of fintech activities. In fact, fintech companies often choose where they would like to do business based on the regulatory body supervising their activity. The main regulatory bodies that exist in the UAE are listed below, along with the relevant laws.

Onshore UAE

The main financial regulators in onshore UAE are:

- the UAE Central Bank (CBUAE), which regulates banks, finance companies, payment service providers and insurance companies; and
- the Securities and Commodities Authority (SCA), which regulates markets, listed companies and securities brokers.

They are primarily tasked with supervising and regulating financial activities conducted in onshore UAE.

---

* Nadim is a partner and heads the FinTech and TMT practice groups as part of the firm's broader technology practice. He advises on complex technology-related agreements, e-commerce matters and fintech ventures. Nadim is involved with several early-stage startups and regularly contributes to public forums related to fintech, including the DIFC FinTech Hive.

† Marina is an associate in the TMT department and specialises in corporate, fintech and capital markets related matters. Marina routinely advises local and international clients on cryptocurrencies, data privacy and matters relating to the tech sphere.

‡ Sam is a paralegal in the TMT department and assists the team with various tech and corporate matters.

DIFC

The Dubai Financial Services Authority (DFSA) is the principal regulatory body of the DIFC. The DFSA supervises regulated companies and monitors their compliance with applicable laws and rules. The Regulatory Law, DIFC Law No 1 of 2004 grants the DFSA its powers as a financial services regulator.

ADGM

The ADGM's financial regulator is the Financial Services Regulatory Authority (FSRA) which has regulatory and supervision oversight of the financial services provided within its jurisdiction.

The FSRA was one of the first jurisdictions to introduce (in 2018) a comprehensive and bespoke regulatory framework for the regulation of crypto asset activities. Since then, the ADGM has continued to update its legal framework to keep up with the cryptocurrency ecosystem.

Several laws have been enacted with the aim to either supplement existing legislation or create new legislation to address disruptive technology in financial services. Some of these include large-value payment systems regulations, security tokens and of course cryptocurrency regulations.

Central Bank Circular No 9/2020 on Large-Value Payment Systems Regulations

This Regulation focuses on large-value payment systems (LVPSs) which are financial infrastructure systems that support the financial and wholesale activities in the UAE. The regulation covers the licensing requirements in relation to LVPSs as well as the obligations and ongoing requirements in relation to a designated LVPS. The Regulation applies to:

- LVPSs that are operated in the UAE; or
- LVPSs that accept the clearing or settlement of transfer orders denominated in the AED currency both in the UAE or outside the UAE.

The regulation does not apply to LVPS incorporated in financial free zones, unless when expressly provided for.

The Stored Value Facilities regulation

The stored value facilities (SVF) regulation, issued in September 2020, repeals and replaces the regulatory framework for stored value and electronic payment systems.

An SVF is defined as a facility whereby a customer can pay a sum of money to the SVF issuer in exchange for the storage of that money on the facility. This regulation applies to companies wishing to undertake a SVF activity, with certain exceptions.

This regulation is highly focused on technology and risk management, and includes extensive obligations around cyber security and technology governance that businesses will need to consider when setting up a SVF activity in the UAE.

Regulation of security tokens

The DFSA has launched its regulatory framework for investment tokens based on its Consultation Paper No 138 – Regulation of Security Tokens, published in March 2021. Investment token is defined to include:

- a security (which includes, for example, a share, debenture or warrant) or derivative (an option or future) in the form of a cryptographically secured digital representation of rights and obligations that is issued, transferred and stored using distributed ledger technology (DLT) or other similar technology; or
- a cryptographically secured digital representation of rights and obligations that is issued, transferred and stored using DLT or other similar technology and:
    - confers rights and obligations that are substantially similar in nature to those conferred by a security or derivative; or
    - has a substantially similar purpose or effect to a security or derivative.

Key cryptocurrencies (ie, Bitcoin, ETH) are not subject to this regulatory framework, given that they are not securities, nor are they considered substantially similar in nature or purpose to a security or derivative.

Companies who wish to undertake financial services relating to investment tokens in or from the DIFC (ie, issuing, trading, holding, dealing in, advising on and managing portfolios) must meet certain licensing and technological requirements set by the DFSA.

The DFSA Rulebook General Module

The DFSA is the regulatory authority for the DIFC financial free zone. DFSA's objective is to contribute to the stability of the UAE financial system by examining and supervising the financial activities conducted in or from the DIFC.

The DFSA Rulebook sets out the DFSA's requirements for authorised companies, including banks, brokers and dealers, asset managers, corporate financiers, wealth managers, insurers and insurance intermediaries.

Depending on the type of financial services business that is conducted in the DIFC, financial institutions will need to obtain the appropriate DFSA regulatory approval and be authorised to undertake the specified regulated activities.

If financial services wish to conduct any of these financial businesses in the DIFC, they must comply with all DFSA rules and regulations.

The FSRA regulatory framework for the authorisation and supervision of fintech

The FSRA manages any potential risks to the marketplace and oversees all financial activities within the ADGM international financial centre. By promoting a supportive and well-regulated environment,

the FSRA plays a vital role in attracting businesses to the ADGM, helping it grow into a leading international financial centre.

The FSRA introduced a regulatory framework in 2021 for the authorisation and supervision of fintech companies providing third-party services to customers of financial institutions.

This regulatory framework enables the FSRA to grant licences to fintech companies providing third-party financial technology services to customers of authorised financial institutions in the ADGM. The FSRA will also be able to impose requirements on these companies and supervise their activities. This regulatory framework promotes innovation in the financial services sector while ensuring that customers are protected from risks. The introduction of the regulatory framework has encouraged more fintech companies to enter the ADGM market and provide innovative new services to customers.

Regulatory and insurance technology

In the wake of the Covid-19 pandemic, financial institutions were forced to move to remote working models. These were difficult to monitor, especially in terms of regulatory compliance. To deal with the pandemic and mitigate risks incurred, the UAE continued to push for the emergence of regulatory technology (RegTech), whereby artificial intelligence (AI) was used to help companies meet their due diligence requirements.

Regulations Lab (RegLab) was launched in January 2019 in partnership with Dubai Future Foundation, pursuant to a federal law issued in 2018 authorising the UAE Cabinet to grant temporary licences for the testing and vetting of innovations that use future technologies and its applications such as AI. RegLab was designed to proactively anticipate and develop future legislation governing the use and applications of emerging technologies in the UAE in ways that maximise the benefits and minimise the risks. It aims to create a reliable and transparent legislative environment, introduce new or develop existing legislation and regulate advanced technological products.

RegLab works closely with lawmakers from federal and local government authorities, as well as the private sector and business leaders to support the UAE's role as a global incubator of innovations and creative projects.

Insurance Technology (insurtech) is now ingrained in the region after having gained popularity at a slow but steady pace in the UAE. Most insurtech startups are focused on (1) offering comparison features to users allowing them to select the insurance package that best suits their needs; (2) digitising the process of subscribing to an insurance policy; and/or (3) streamlining processes between insurance companies using blockchain technology. As the industry continues to develop, we are beginning to see greater utilisation of data and technology to create a tailored experience for each user, where issues can be addressed in real time.

We continue to see traditional insurance companies collaborating with insurtechs to improve their efficiency, indicating the potential and benefits of the insurtech industry and the willingness of traditional insurance companies to adopt new technologies, viewing insurtech largely as an enabler instead of a competitor.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

Onshore UAE

The SCA issued Decision No 23 of 2020 concerning the Crypto Assets Activities Regulation (CAAR), which aims to regulate and license key aspects of dealing in crypto assets – including the issuance and promotion thereof, provision of crypto asset custody services, operating exchanges, and fundraising platforms.

The CAAR applies to most forms of crypto assets which are listed and available for trading on a recognised market, whether securities or otherwise. The CAAR is not intended to include items regulated by the CBUAE such as currencies, virtual currencies, digital currencies, stored-value units, payment tokens and payment units.

Generally, there are two main requirements to provide cryptocurrency assets or related services in the UAE:

- the service provider must be incorporated onshore within the UAE or any of the UAE's financial free zones; and
- the service provider must be licensed by the SCA.

With the introduction of crypto asset-specific rules such as (1) minimum disclosure standards that ensure risks are fully identified to investors; (2) additional regulatory requirements for crypto exchanges; and (3) additional AML protections that target the increased risk caused by cryptocurrency, the CAAR provides customers with protection that targets the industry and builds on global standards.

DIFC

Having previously excluded crypto assets from the scope of application of issued regulations regarding security tokens and investment tokens, the DFSA has recently enacted rules regarding the regulation of crypto tokens on 1 November 2022, influenced by the increase in the use of cryptocurrency as a means for financial transactions. Under the new legislation, crypto tokens are defined as a 'token that is used, or is intended to be used, as a medium of exchange or for payment or investment purposes but excludes an investment token, or any other type of investment, or an excluded token'. Although generally aligned with the widely recognised Financial Action Task Force definition, this regulation adopts a broader definition of 'token', changing 'used' to 'used or intended to be used', including crypto that may not otherwise be covered by the regulation.

Crypto tokens currently recognised by the DFSA are as follows:

- Bitcoin;
- Ethereum; and
- Litecoin.

ADGM

The FSRA has released additional guidance on 28 September 2022 on the regulatory treatment of various newly emerged digital assets in conjunction with its framework and original guidance issued in 2017. The Framework makes it evident that:

- Crypto asset activities may only be allowed in connection with crypto assets that are categorised as accepted crypto assets – ie, those crypto assets that fulfil criteria prescribed by the FSRA – and any person dealing with such accepted crypto assets including intermediaries (such as brokers/dealers, asset managers, crypto asset exchanges and crypto asset custodians) involved in dealing, managing or arranging accepted crypto assets would require a financial service provider to operate in and from the ADGM. To become a financial service provider, all applicable FSRA and Financial Services and Market Regulations must have been, and must continue to be, complied with.
- There are six key principles that the FSRA framework targets:

    1. robust and transparent risk-based regulations;
    2. high standards for authorisation;
    3. preventing money laundering and other financial crime;
    4. risk-sensitive supervision;
    5. commitment to enforce on regulatory breaches; and
    6. international cooperation through the support of a number of bilateral and multilateral agreements to support the exchange of information between regulators.

The ADGM issued the Distributed Ledger Technology Foundations Regulations in October 2023, aiming to create a tailored legislative framework specifically designed for decentralised autonomous organisations (DAOs). The proposed regulations are poised to revolutionise the legal structures for DAOs and fuel the growth of the crypto industry in the UAE. The new regime has been introduced in line with the ADGM's strategy to foster initiatives in the broader blockchain and digital asset realm.

It is an innovative, purpose-built regime that addresses the unique legal requirements of blockchain foundations, DAOs and the broader crypto industry.

Dubai World Trade Centre

The Virtual Assets Law No 4/2022 (VAL) established a framework for the regulation of virtual assets in Dubai and created a regulatory authority for virtual assets called the Virtual Assets Regulatory Authority (VARA). On 19 September 2023, the Virtual Assets and Related Activities Regulation was issued, creating a comprehensive regulatory framework, setting out the powers of VARA and placing various controls on virtual assets. The main points from the regulation are:

- the regulations provide for VARA's accepted virtual asset activities, including requirements that all VASPs must comply with as well as activity-specific requirements; and

- like other industry-leading jurisdictions, entities wishing to carry out virtual asset activities must be granted a license by VARA to do so. Licensing conditions are communicated to the entity by VARA; VARA maintains the sole and absolute discretion to grant the licence and incorporate in the licence any limitations or stipulations that it deems appropriate.

VARA has unveiled the guidelines governing the marketing and promotion of digital assets. These guidelines are said to ensure 'factual accuracy, explicitly demonstrate any promotional intent and in no way mislead on the guaranteed nature of their returns'. These guidelines apply to all entities promoting services in the emirate of Dubai, whether they are under the supervision of VARA or not.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

Onshore UAE

The sources of payments law in onshore UAE principally consist of four regulations, which have been enacted by CBUAE as follows:

- the Stored Value Facilities Regulation, issued in November 2020;
- the Large Value Payment Regulation, issued in January 2021;
- the Retail Payment Systems Regulation, issued in January 2021; and
- the Retail Payment Services and Card Schemes Regulation, issued in July 2021.

DIFC

The sources of payments law in DIFC are found in the DFSA Rulebook, specifically the DFSA Rulebook Conduct of Business Module or COB. The DFSA issued a new financial services category in April 2020, categorised as money services under Category 3D; this covers payment service providers.

ADGM

The FSRA regulates financial services conducted in or from the ADGM. The sources of payments law in the ADGM are found in the FSRA Rulebook, which added a money services activity in October 2020 under a Category 3C licence.

New law or regulation foreseen in the future

The CBUAE, along with the SCA, DFSA and FSRA, released a consultation paper titled *Guidelines for Financial Institutions adopting Enabling Technologies* in 2021. The Guidelines laid down certain key principles for financial institutions to apply when using enabling technologies, such as application programming interfaces (APIs), cloud computing, biometrics, big data analytics, AI and DLT. The Guidelines were published to invite consultation from stakeholders. However, concrete guidelines on integrating enabling technologies into financial services are still to be issued by the CBUAE.

The CBUAE also launched its Financial Infrastructure Transformation Programme (FIT Programme) on 12 February 2023, which aims to accelerate the digital transformation of the financial services sector. The FIT Programme outlines nine key initiatives, with full integration of these initiatives to be expected by 2026. While these initiatives are not laws or regulations in themselves, we can expect to see supporting guidelines and regulations to provide clarity and direction as to their implementation and how they are to be controlled. Key initiatives are:

- *Card domestic scheme*: a unified, secured and efficient card payment platform to foster the growth of e-commerce and digital transactions;
- *eKYC*: to facilitate non-face-to-face customer onboarding and ongoing customer due diligence;
- *Central bank digital currency*: to address the problems of inefficiency associated with cross-border payments; and
- *Open finance*: driving innovation and competition through interconnectivity and interoperability.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

Various initiatives have been taken to encourage innovation, especially in the financial sector. Most notably, regulators have put in place sandbox regimes to allow innovators to test their products under more lenient regulatory requirements.

Onshore UAE

In the past few years, many government authorities have shown an increasing interest in fintech. In fact, many initiatives to encourage the emergence of fintech in the UAE have been introduced. Notably, the SCA has put in place a pilot regulatory environment (sandbox) to encourage innovation in the fintech industry and allow entrepreneurs to test their products in more relaxed regulatory environments.

Furthermore, CBUAE launched a fintech office in the second half of 2020 to support startups and build a mature fintech ecosystem in the UAE.

DIFC

The DIFC launched an accelerator programme, named the Fintech Hive, to encourage cutting-edge fintech solutions for leading financial institutions. Pursuant to this programme, the DIFC established an innovation testing licence which permits qualifying fintech companies to develop and test innovative concepts for a period of six to 12 months without being subject to all regulatory requirements that normally apply to regulated companies. If the outcomes detailed in the regulatory test plan are fulfilled, and the participating company can satisfy DFSA requirements, it may migrate

to full authorisation. If such conditions are not met, the company must cease to carry on any and all activities requiring regulation in the DIFC.

ADGM

The ADGM launched an accelerator programme named the Regulatory Laboratory to encourage cutting-edge fintech solutions for leading financial institutions. Pursuant to this programme, the ADGM established a special type of financial services permission (ie, a licence) which allows qualifying fintech companies to develop and test innovative concepts for up to two years without being subject to all regulatory requirements that normally apply to regulated companies.

If participating companies are capable of meeting ADGM requirements at the expiry of the licence, they may be transferred to the regular authorisation and supervision review. If such companies cannot meet these requirements, they must cease to carry on activities requiring regulation in the ADGM.

In addition to launching an accelerator programme, the ADGM added legislation in the Financial Services and Markets Regulations specifically addressing the emergence of new technologies, namely crypto assets.

The CBUAE and ADGM have together signed a fintech cooperation agreement to develop fintech initiatives. This agreement will improve their collaboration along with a co-sandbox programme. Additionally, the DIFC and the CBUAE have also signed a cooperation agreement in the field of fintech with the implementation of a co-sandbox programme.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

Onshore UAE

No regulations expressly targeting open banking have been issued. Several regulations can notably be relied on to conclude the UAE's position on open banking. For example, the Retail Payment Services and Card Schemes Regulation regulates and mandates the licensing of account information services (AIS) and payment initiation services (PIS).

DIFC

The DFSA recognises money service businesses as a category of activities that require its authorisation and licensing. Money service businesses are further categorised into two groups: (1) arranging and advising on money services; and (2) providing money services.

Entities involved in arranging and advising on money services include AISs and PISs that enable them to provide open banking services. In April 2022, the DFSA granted its first AIS and PIS licence to Tarabut Gateway to provide open banking services in and from the DIFC.

ADGM

Like the DFSA, the FSRA issues licences to entities involved in money service businesses. By obtaining a Category 3C licence, companies can engage in money service business activities, including arranging and advising on money services.

North America

Canada

Nicolas Faucher*
Fasken, Montreal
nfaucher@fasken.com

Felicia Yifan Jin†
Fasken, Montreal
fjin@fasken.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

There is currently no single legal framework in place governing fintech entities in Canada. Rather, the nature of products and services being offered by each fintech entity determines which laws and regulations apply. These are a combination of both federal and provincial laws. Canada's fintech industry covers a broad range of products and services, the most common being related to payments, lending, insurance, digital currencies, and capital markets.

Federal

Use of bank words

The Bank Act restricts fintech entities' ability to use the words 'banks', 'banker' and 'banking' to indicate or describe a business in Canada. While some exceptions apply, they are generally not broad enough to cover known fintech activities.

Payment services

Payments Canada is the government entity overseeing Canada's payment infrastructure. Fintech entities wishing to have access to such infrastructure must be members of Payments Canada, as required by the Canadian Payments Act. Only certain entities are eligible as such.[1] Please see Question 3 for further details.

---

* Nicolas is a partner, co-leader of the Financial Services Group and co-president of the Corporate/Commercial Group at Fasken. He specialises in legal issues related to financial institutions, financial services, technology and professional services companies.

† Felicia is an associate within the Corporate and Commercial Law Practice Group at Fasken. She assists financial institutions with the regulations applicable in Canada and Québec and practises in the area of private capital and risk capital, as well as mergers and acquisitions.

1 The Bank of Canada; every bank; every authorised foreign bank; every cooperative credit association, loan company or trust company that is designated as a bridge institution under the Canada Deposit Insurance Corporation Act; a central cooperative credit society, a trust company, a loan company and any other person, other than a local that is a member of a central or a cooperative credit association, that accepts deposits transferable by order; a province or an agent or mandatary of a province, if it accepts deposits transferable by order; a life insurance company; a securities dealer; a cooperative credit association; the trustee of a qualified trust; and a qualified corporation, on behalf of its money market mutual fund.

Money services businesses, payment services providers and digital currencies

Fintech entities offering services of: foreign exchange dealing, remitting, or transmitting funds (including payment services providers); issuing or redeeming money orders, traveller's cheques, or anything similar; dealing in virtual currency; and crowdfunding platforms must register as money services businesses (MSB) under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA). The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) works to ensure compliance with PCMLTFA. Please see Question 3.

Fintech companies can also be subject to generally applicable federal legislation. This includes the Competition Act, the Personal Information Protection and Electronic Documents Act and the Canadian Anti-Spam Law.

Provincial

A fintech entity will also most likely also be subject to various provincial laws, including privacy laws and consumer protection laws. As previously mentioned, this is entirely dependent on the type of products and services being offered by the entity.

Deposits

Certain provinces require fintech entities that accept deposits to register as provincial deposit-taking institutions, trusts or loan companies. This implies that each registrant qualifies as such, meaning that they meet all conditions of entry (eg, sufficiency of capital, compliance framework, governance, ownership, etc). Under such registration, it is often required that such entities subscribe to a provincial deposit insurance organisation.

Money services businesses

Fintech entities operating as money services businesses in the province of Québec must also register with the Minister of Revenue of Québec and Revenu Québec under the Money-Services Businesses Act.

On 11 May 2023, British Columbia's Money Services Businesses Act (MSBA) received Royal Assent, the object of which is to establish a money services businesses registration regime that will be administered by the British Columbia Financial Services Authority (BCFSA). While the MSBA is currently not in force, in accordance with the 2024/25 Regulatory Roadmap published in April 2024, the BCFSA will support the Government of British Columbia and develop requirements that will form the regulatory framework governing the regulation of money services businesses in British Columbia.

Lending services

Generally, lending activities require registration only in the case of high-interest loans or payday loans, although certain provinces require registration for all lending activities. All consumer protection laws will impose conditions on lending activities offered to consumers, including disclosure obligations and

limitations on advertisement. In addition, fintech entities wanting to engage in peer-to-peer lending activities can be subject to certain securities regulations.

Crowdfunding

Crowdfunding rules have slowly been developing across a number of jurisdictions in Canada. The rules are intended to make it easier for startups, including fintechs, to finance their activities. Specifically, they allow for retail investors to engage in the raising of capital for these small businesses.

Additionally, in June of 2021, the Canadian Securities Administrators (CSA) adopted *National Instrument 45-110: Start-up Crowdfunding Registration and Prospectus Exemptions*, in an effort to establish a more uniform national regime for crowdfunding. This instrument increased not only the individual investment limit but also the limit on the maximum capital allowed to be raised within a 12-month period.

In line with the CSA, provincial securities regulatory authorities have also created prospectus and dealer registration exemptions. These exemptions allow startups and early-stage companies to offer securities to investors without having to file a prospectus, enabling them to raise capital more efficiently. Certain provinces, including Manitoba, New Brunswick, Nova Scotia, Ontario and Quebec, enable non-accredited investors to participate in such funding through their exemptions. In addition to the exemption, British Columbia, Manitoba, New Brunswick, Nova Scotia, Quebec and Saskatchewan also offer what is known as the Start-Up Exemption. This differentiates itself from the first exemption as it has a lower maximum capital and has less prescriptive provisions.

Insurance

Insurance fintech entities are subject to the same laws and regulations as regular insurance companies, insurance brokerages and insurance agencies. In Canada, insurance is regulated by both the federal and provincial governments. Such laws and regulations govern both the offering and the distribution of insurance products.

Capital markets (securities)

Fintech entities participating in the securities market are regulated at the provincial level by their respective provincial securities commissioners. In this respect, there have been recent amendments to the self-regulatory organisations established to supervise the specific areas of the Canadian securities market. Effective as of 1 January 2023, the new self-regulatory organisation of Canada was established, otherwise known as the Canadian Investment Regulatory Organization (CIRO). The creation of this organization stems from the amalgamation of the Investment Industry Regulatory Organization of Canada (IIROC) and the Mutual Fund Dealers Association of Canada (MFDA).

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

'Dealers in virtual currencies', now identified as MSBs, are subject to reporting and compliance obligations under the PCMLTFA. Moreover, crypto assets could be subject to provincial securities

legislation, dependent on whether the assets fall under the definition of 'security' found within the respective legislation. This determination is conducted on a case-by-case basis. Generally, a crypto asset will qualify as a 'security' under the law as it is frequently considered to be an 'investment contract' or a defined security instrument. If, and when, a crypto asset does fall under the mentioned definition, its valid and authorised distribution will be subject to prospectus and registration requirements.

The CSA has indicated that, where initial coin offerings (ICO) and initial token offerings (ITO) are considered to be the entirety of the offering or arrangement of the business, such coins and tokens should be considered securities. It has also noted that, where a cryptocurrency exchange or a crypto trading platform is involved and is offering securities in cryptocurrency, the CSA must determine whether the exchange constitutes a marketplace. If so, the marketplace would be required to comply with the rules governing exchanges and other trading systems.

Furthermore, the CSA continues to issue new rules and guidance for fintech businesses dealing with cryptocurrencies. Examples of this include:

- Staff Notice 21-333 Crypto Asset Trading Platforms: Terms and Conditions for Trading Value-Referenced Crypto Assets with Clients;
- Staff Notice 21-332 Crypto Asset Trading Platforms: Pre-Registration Undertakings Changes to Enhance Canadian Investor Protection;
- Staff Notice 46-307 Cryptocurrency Offerings;
- Staff Notice 21-327 Guidance on the Application of Securities Legislation to Entities Facilitating the Trading of Crypto Assets; and
- Staff Notice 21-329 Guidance for Crypto-Asset Trading Platforms: Compliance with Regulatory Requirements.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

Payment service providers

Since June 2021, the Bank of Canada has taken on the role of regulator for 'any retail payment activity that is performed by a payment service provider' (PSP), who either has a place of business in Canada or who is located outside of Canada but is directing its activities to a Canadian end user.

According to the Retail Payment Activities Act (RPAA), a PSP 'may include a variety of entities that perform electronic payment functions, such as payment processors, digital wallets, money transfer services and other payment technology companies'. Obligations for PSPs include operational risk management, end-user (payor or payee) funds safeguarding, registration requirements, and incident reporting requirements. From 1 November 2024 until 15 November 2024, any PSP who falls under this definition must register and provide the prescribed information with the Bank of Canada. This includes any MSB engaged in retail payment activities. As of September 2025, the Bank of Canada will begin enforcing the obligations under the RPAA in accordance with finalised guidelines, which are to be published by the end of 2024.

Digital wallets

While there has been no definitive position of the regulators on this matter other than that highlighted in Question 1, entities offering digital wallets should review their activities under the laws and regulations applicable to deposits and under the RPAA. Closed-loop wallets, gift cards and prepaid cards are subject to specific consumer protection laws.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

Federal

While there is no fintech-specific programme being offered by the federal government, there exist several incentive schemes which encourage investments in small and medium-sized entities. This includes those in the fintech industry. Some examples of these programmes include The Scientific Research and Experimental Development Program, the Industrial Research Assistance Program (IRAP) (which will be integrated into the Canada Innovation Corporation as of 2026), the Women Entrepreneurship Knowledge Hub, and the Black Entrepreneurship Program. Additionally, the Government of Canada has allocated up to CA$298m to the Digital Technology Cluster, where the objective is to accelerate the development and adoption of digital technologies that help Canadians stay healthy, address climate change, drive economic productivity and build digital skills. The CSA has also established the CSA Financial Innovation Hub (its predecessor was the CSA Regulatory Sandbox), an initiative aimed at supporting fintech businesses and other innovative business models in testing novel ideas or technology solutions based on themes pre-determined by the CSA. Through the FinHub, the CSA takes a proactive approach to considering new technologies and innovative business models, including assessing the scope and nature of regulatory implications and evaluating what may be required to modernise the securities regulatory framework for such innovation.

Provincial

Certain provinces have established more fintech-specific initiatives. As an example, the Ontario Securities Commission (OSC) created the OSC Launchpad, a team whose purpose is to help fintech companies navigate securities law requirements. In British Columbia, the British Columbia Securities Commission has initiated a Fintech & Innovation Team that is dedicated to supporting the innovation and adoption of new technologies in the financial services sector.

For more information, see the crowdfunding section in Question 1.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

The Federal Government is currently developing its open banking framework, more recently designated as its consumer-driven banking framework, to allow consumers and small businesses to securely transfer their financial data through an application programming interface (API) to approved service providers of their choice.

In this regard, the Federal Government intends to introduce in spring 2024 the first of two pieces of legislation to implement the Framework, starting with key elements such as governance, scope, and criteria and processes for the technical standard. Remaining elements of the Framework would be legislated in the autumn of 2024. The legislation will expand the mandate of the Financial Consumer Agency of Canada (FCAC) to include oversight of consumer-driven banking and establish foundational Framework elements related to scope, system participation, safeguards in respect of integrity and national security, and common rules covering privacy, liability, and security. The Framework will also include the principles and process for the selection of a single technical standard for data sharing that will ensure the standard is fair, open and accessible.

United States

Arturo Banegas Masiá*
Akerman, New York
arturo.banegasmasia@akerman.com

Glorimer Rodriguez†
Akerman, Miami
glorimer.rodriguez@akerman.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

The complex landscape of fintech regulation in the United States is shaped by a dual regulatory system (operating at both the federal and state level) that distinguishes it from other regulatory frameworks across the globe. The interplay of federal and state regulations that apply to fintech are implemented and enforced by an extensive network of federal and state agencies, each with a distinct array of responsibilities and authorities. Nonetheless, there is often overlap between federal and state regulations, and their respective enforcement agencies. At the same time, there are pockets of fintech-related issues that are regulated at the state level and not at the federal level. Thus, while federal agencies and regulations may often displace or pre-empt its state-level counterparts, the industry is necessarily subject to both levels of authority.

Key regulators

At the federal level, fintech companies may need to adhere to regulations of several regulatory bodies including:

- the Financial Crimes Enforcement Network (FinCEN), which oversees anti-money laundering measures and enforces the Bank Secrecy Act (BSA);
- the Consumer Financial Protection Bureau (CFPB), which may conduct examinations of certain non-bank business that are deemed to pose a risk to consumers;
- the Board of Governors of the Federal Reserve System (FRB), which oversees the operations of all depository institution holding companies and regulates all state-chartered banks that are members of the federal reserve system;
- the Federal Deposit Insurance Corporation (FDIC), which insures consumer deposits and supervises state-chartered banks which are not members of the Fed;
- the Office of the Comptroller of the Currency (OCC), which supervises national bank charters;

* Arturo is a partner at Akerman. He advises in corporate and transactional deals, with a particular focus on technology transactions and product development strategies in technology, ICT and financial industries, including counselling entrepreneurs, investors, startup and emerging companies in the fintech industry to fund, structure and set up MSBs in the US and globally, and cross-border deals with Latin America and southern European countries.

† Glorimer is an Associate at Akerman. She dedicates her practice to corporate and transactional matters, with a focus on mergers and acquisitions, capital markets, cross-border deals with Latin America and providing counsel to businesses on a wide array of corporate matters.

- the Securities and Exchange Commission (SEC), which regulates securities, broker dealers, investment advisers, funds, and digital asset exchanges; and
- the Federal Trade Commission (FTC), which safeguards consumers from unfair or deceptive practices.

This list is by no means exhaustive: fintech businesses may fall under the purview of several other regulatory entities depending on the type of business and their particular activities.

At the state level, most states have regulatory authorities that require and oversee licensing for fintech business; specifically, money services business and non-bank lenders are commonly targeted by state regulators.

Key regulations

State licensing requirements

Money services business (such as digital wallets) are required to obtain money transmission in every US state, except Montana (this is more thoroughly discussed in Question 3). The requirements to obtain licensing are nuanced from state to state, with some taking a more stringent approach than others. The state-by-state licensing process is long and cumbersome, prompting certain state regulators to focus their efforts to streamline the process and encourage uniformity across states. Similarly, fintech businesses who offer credit and lending products are required to obtain lender licences in most states, in addition to complying with federal regulatory requirements.

Anti-money laundering

The Anti-Money Laundering Act, which amended the Bank Secrecy Act, signalled an aggressive regulatory step in investigating and preventing potential terrorist funding or other money laundering schemes. It requires financial institutions (which now includes money services businesses) to conduct 'know your client' and 'know your business' checks, submit reports of suspicious transactions to FinCEN, and even grants FinCEN and the DOJ authority to subpoena non-US banks to request records. Further, the Corporate Transparency Act, effective 1 January 2024, requires reporting companies to provide reports on the ultimate beneficial owner to FinCEN.

Credit laws

Fintech businesses offering credit products may be regulated by the Truth In Lending Act (TILA), Fair Credit Opportunity Act (FCRA), and the Equal Credit Opportunity Act (ECOA). Among other things, these regulations require specific disclosures of important credit terms, notices of adverse actions, and impose restrictions on how consumer credit data may be used.

Data privacy

At the federal level, the Gramm-Leach-Bliley Act (GLBA) regulates collection, usage and disclosure of financial information and applies to businesses that are 'significantly engaged

in financial activities'. It generally requires disclosures on information sharing practices and procedures to safeguard sensitive data. Further, there has been recent increase in state-level data privacy regulation: 15 states have currently enacted data privacy legislation. The California Consumer Privacy Act of 2018 (CCPA) as amended by the California Privacy Rights Act of 2020 (CPRA), which is analogous to the European GDPR, paved the way for state-level data privacy legislation. Several states have since followed California's lead and enacted their own data privacy legislation: the Connecticut Data Privacy Act (CTDPA), the Utah Consumer Privacy Act (UCPA), the Virginia Consumer Data Protection Act (VCDPA), the New York SHIELD Act, the Delaware Personal Data Privacy Act, the Tennessee Information Protection Act, and the Texas Data Privacy and Security Act are all state-level consumer data privacy laws enacted in the past four to five years. More states seem to be following this trend, as 14 other states have introduced data privacy bills in the past year.

Consumer protection

In April 2022, the CFPB asserted its authority to examine and regulate fintech businesses under a segment of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010. On November 2023, the CFPB proposed a rule that would subject large non-bank entities offering financial services (such as digital wallets and payment apps) to the same supervisory examination process as large banks and other financial institutions currently supervised by the CFPB. Under the proposed rule, the CFPB would be able to supervise compliance with applicable federal consumer financial protection laws, which includes applicable protections against unfair, deceptive and abusive acts and practices, rights of consumers transferring money, and privacy rights. The period for public comments on the proposed rule ended on 8 January 2024, and the final rule has yet to be released.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

US regulation regarding cryptocurrency continues to be ambiguous in terms of defining the legal character ascribed to cryptocurrencies. Regulatory authorities at the federal level offer differing labels and regulatory treatment to cryptocurrency. Under the 'Howey Test' (a legal framework that the US Supreme Court developed in 1946 to determine if a transaction is an investment contract and should be regulated) certain cryptocurrencies may be considered 'investment contracts', and therefore securities regulated by the SEC. The SEC takes the position that the sale and offering of cryptocurrencies that satisfy the Howey Test must therefore be registered with the SEC or be exempt from registration under the Securities Act of 1933. The treatment of certain cryptocurrencies as securities also means that their owners would be subject to periodic reporting requirements with the SEC. In practice, however, very few offerings have in fact registered with the SEC. Under the Howey Test, a digital asset constitutes an 'investment contract' where its sale involves (1) an investment of money; (2) in a common enterprise; (3) with the reasonable expectation of profits; (4) due to the managerial efforts of others. However, SEC guidance has explained that the Howey Test requires purchasers to rely on the efforts of an 'active participant' to develop profits. Thus, offerings that lack a centralised managerial effort would not be considered securities, an issue that causes much ambiguity.

Simultaneously, the CFTC supervises the trading of cryptocurrency derivatives, considering cryptocurrencies to be commodities subject to the Commodity Exchange Act. However, the CFTC only has authority over derivative markets, not spot markets. Therefore, cryptocurrency regulation does not neatly fall under the CFTC's purview either. The uncertainty and ambiguity of the current regulatory framework has caused a push towards regulations and clarification when it comes to cryptocurrency.

At the state level, states have generally applied existing regulations to cryptocurrencies (such as money services businesses (MSB) licensing requirements, further explained in Question 3) depending on their features and activities. However, a few states have enacted their own cryptocurrency regulations: Wyoming enacted 13 laws in 2019 designed to enable cryptocurrency businesses in the state. Among other things, the Wyoming framework recognises protectable property rights for owners of digital assets and creates a method that would allow state banks to be treated as 'qualified custodians' of cryptocurrency assets.

Similarly, Montana enacted a law which would prevent local governments in the state from enacting rules which would prohibit cryptocurrency mining. Most notably, New York has created its own licensing framework specific to virtual currency businesses, known as the BitLicense.

New developments

ETFs

On 10 January 2024, the SEC approved the launch of the first exchange-traded fund (ETF) which tracks Bitcoin. The approval was an important development in the cryptocurrency market, allowing investors to access Bitcoin through regulated investment vehicles without directly owning it. Following the decision, several BTC ETFs launched at the same time, fiercely competing for market share. The approval followed a series of rejections by the SEC in previous years, which appeared to indicate a shift in regulatory stance towards crypto assets. Nonetheless, the approval order included a reminder that significant regulatory hurdles remain when it comes to Bitcoin ETFs. Among others, sponsors will be required to provide extensive disclosures about the investment products, and they will be closely monitored and investigated when necessary to ensure enforcement of rules regarding fraud and manipulation.

Stablecoins

There is currently no comprehensive federal regulatory framework specifically designed to regulate stablecoins. However, federal and state law is applicable depending on the type of activity. For example, federal anti-money laundering regulations, and state MSB licensing requirements (discussed more in depth in Question 3) may be applicable depending on the activity and features of the particular stablecoin.

There has been a recent market push demanding stablecoin regulation. In July 2023, the Clarity for Payment Stablecoins Act proposed a series of requirements to issue stablecoins, including the requirement that the issuer hold at least one dollar of permitted reserves for every dollar worth of stablecoins outstanding/issued (limiting permitted reserves to 'safe assets'). The proposed legislation

would also specify that payment stablecoins fall outside of the securities and commodities categories and are thus exempt from oversight by the SEC and CFTC. The bill was ordered to be reported (amended) soon after, and there have been rumblings that a new bill will be proposed soon. US Senator Cynthia Lummis has expressed that she is drafting stablecoin regulations along with Senator Kirsten Gillibrand and that an announcement is imminent, after receiving technical feedback from The New York Department of Financial Services, the Federal Reserve, the Treasury Department and the National Economic Council.

Certain states have also begun taking steps to regulate stablecoins. For example, in May 2023 Wyoming enacted the Stable Token Act, which laid out the steps for Wyoming to issue the US's first government-issued stablecoin. The Act creates a Stable Token Commission tasked with developing a plan for the issuance. As of December 2023, the Commission's executive director expressed that the response from vendors interested in helping develop the Wyoming stablecoin was substantial, and he looks forward to issuing formal requests for proposal.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets

Federal regulations

Money transmitting businesses (ie, those businesses that issue, transmit, and/or accept payment instruments such as wire transfers, money orders, and stored value cards) have fallen under heavy federal scrutiny due to the potential for such businesses to be conduits for terrorist funding and other money laundering schemes. The USA Patriot Act strengthened federal anti-money laundering (AML) laws and modified the Bank Secrecy Act (BSA) to make it more difficult for money launderers to operate, and easier for law enforcement and regulatory agencies to police money laundering operations.

Thus, money services businesses (MSBs) are subject to certain requirements under the BSA, which generally include an obligation to maintain an AML programme, as well as registration, reporting and record-keeping requirements. Specifically, MSBs must: (1) register with FinCEN, and renew every two years; (2) undergo an initial risk assessment and adopt a written AML policy based on those risks; (3) appoint a qualified compliance officer with a sufficient budget and qualifications adequate to the business's risks; (4) train employees in the operationalisation and implementation of the compliance programme; and (5) undergo regular independent testing and review of the business' compliance programme.

MSBs must also report to FinCEN personal information of their customers as well as transactional data. In certain situations, MSBs must outright deny service to certain customers, and even continue servicing customers while permitting government agencies to monitor each of the transactions. Suspicious transactions must be reported to FinCEN. In the cases of international or otherwise 'high risk' clients, the business must take even more stringent identification measures. Further, reporting suspicious activities affords safe harbour protections to the money transmitter for a particular transaction. If FinCEN investigates a transaction in which a money transmitter is involved and it did not report as suspicious, the money transmitter may be subject to substantial civil and criminal liabilities.

State regulations

Money transmitting businesses are also regulated at the state level. Every US state (except Montana) now regulates money transmitters in addition to the federal requirement that all such businesses register with FinCEN. Whereas FinCEN's federal regulators see themselves as money laundering preventers, state regulators see themselves as consumer protectors. The goal of the application process is to ensure the safety, soundness and solvency of the business. States differ in their approaches to the regulation of money transmitters, with some states requiring higher security deposits than others, and some taking a more active role than others in enforcing the registration and licensing requirements that they impose upon such businesses.

The common features of most state money transmitter laws are:

- initial registration fees;
- minimum capitalisation requirements (varying between $50,000 and $1m);
- background checks on all principals in business;
- some form of security (bond or its equivalent in securities);
- regular reporting requirements;
- annual renewal fees;
- audits; and
- the requirement for a full-time AML compliance officer.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

US regulatory agencies have recently been increasing their efforts towards developing regulations that foster fintech and digital asset innovation. For example, the OCC created an Office of Financial Technology aimed at developing regulations to foster and support responsible fintech innovation. Additionally, the CFPB created an Office of Innovation focused on promoting competition in the fintech sector by identifying stumbling blocks for new market entrants.

Nonetheless, at the federal level, the US lacks widely available special programmes to support fintechs. However, several states (including Arizona, Florida, Hawaii, Nevada, North Carolina, Utah, West Virginia, and Wyoming) have enacted regulatory sandbox programmes aimed at fostering innovation within the fintech sector. These programmes ease certain regulatory requirements (such as licensing requirements) while maintaining a level of oversight, allowing market participants to test certain fintech products in a controlled environment and on a limited scale.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

The US has previously recognised personal financial data rights in the Consumer Financial Protection Act. While the US had not yet implemented said rights, in October 2023, the CFPB released a long-awaited proposed rule which would implement the right to open banking and consumer financial data. The proposed rule would require financial institutions (upon a consumer's request) to provide timely access to covered financial data in an electronic form that is usable by consumers and authorised third parties. The period for public comments on the proposed rule ended on 29 December 2023; the final rule has yet to be released.

South America

Argentina

Carlos María Melhem
Allende & Brea, Buenos Aires
cmelhem@allende.com

Esteban Gómez Moretto
Allende & Brea, Buenos Aires
egomez@allende.com

Luciana González
Allende & Brea, Buenos Aires
lgonzalez@allende.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

In Argentina, there is not one single piece of regulation or law specific for fintech. Argentina does not have a fintech law. Nevertheless, there are different, separated regulations that indirectly relate to technology applied to financial innovation, the most relevant of which are summarised below.

3.0 transfers (T3.0) – *Transferencias 3.0*

In 2020, the Argentine Central Bank (the 'Central Bank') passed regulations creating a new standardised payments interface that allows the matching of payments through an open and interoperable digital ecosystem within the Argentine National Payment System ('T3.0 Regulations'). These regulations provide that all banks and payment service providers that offer virtual payment accounts (PSPCPs) are required to comply with the T3.0 Regulations. The T3.0 Regulations incorporate an automatic and irrevocable accreditation payment system, which is available 24 hours a day, seven days a week. The T3.0 transfer system entered into operation on 7 December 2020, in relation to the use of debit cards and the provision of QR Codes for the initiation of such payments, except for prepaid cards, for which the use of T3.0 was not allowed until 31 May 2021. The T3.0 real-time payment system comprises mainly the following participants: (1) a payer, (2) a receiver; (3) one or more financial institutions, banks and/or PSPCPs; and (4) an administrator. As regards to the latter, the entities authorised by the Central Bank to function as administrators of T3.0 so far are: Compensadora Electrónica SA, Interbanking SA, Newpay SAU and Red Link SA.

In this respect, it is worth mentioning that the T.3.0 Regulations contemplate three types of immediate transfers: (1) push immediate transfers; (2) pull immediate transfers; and (3) payments with transfer (PCT, for its Spanish acronym). Push immediate transfers are defined as the remittance of funds that are debited from the sender's customer account and credited to the receiver's customer account instantaneously. Pull immediate transfers are defined as requests for funds that, with prior authorisation or consent, allow the debit of the receiving customer's account and the immediate credit of funds to the requesting customer's account. These movements of funds occur directly from

one account to another, without third party involvement. Finally, PCTs are defined as immediate transfers used to purchase a good and/or service with the participation of a payment acceptor.

Payment service providers

Central Bank regulations contemplate nine[1] types of payment service providers (PSPs):

- PSPCPs;
- administrators;
- payment acceptors;
- payment service providers who perform payment initiation activities (PSIs, for its Spanish acronym);
- ATM networks;
- electronic fund transfer networks;
- acquirers;
- payment aggregators; and
- extra-bank tax and/or service collection companies.

Except for PSPs that act as administrators, PSPs must be registered with the Registry of Payment Service Providers of the Central Bank. Please see our comments on Question 3 below.

Digital wallets

Central Bank regulations define 'digital wallet service' as the service offered by a financial entity, bank or PSP through an application in a mobile device or web browser that allows, among other transactions, to make payments with transfer (PCT) and/or with other payment instruments, such as debit, credit, purchase or prepaid cards (digital wallets). Central Bank regulations provide that digital wallets, which allow the initiation of payments with QR codes, must be registered with the Registry of Interoperable Mobile Wallets before the Central Bank. Please see our comments on Question 3 below.

Crowdfunding

The Entrepreneurial Support Act No 27,349 and Resolution 717/2017, amended by Resolution 942/2022 of the Argentine Securities and Exchange Commission (CNV, for its acronym in Spanish) provides a crowdfunding regulatory framework for equity crowdfunding in Argentina. This framework establishes certain requirements, as summarised below:

1 The main PSPs acting in the Argentine market are the following: (1) PSPCPs: Uala, Moni and Prex; (2) administrators: COELSA, Interbanking and Newpay; (3) payment acceptors Openpay, Pago Virtual del Sur and Mercado Pago; (4) PSIs: MODO, Movytech and TDK Labs; (5) ATM networks: Banelco, Octagon and Red Link; (6) electronic fund transfer networks: Red Link and Newpay; (7) acquirers: Getnet, Payway and Global Processing; (8) payment aggregators: Mercado Pago, Dlocal and PayU; (9) extra-bank tax and/or service collection companies: Rapipago and La Pagaduría.

- crowdfunding platforms must be registered as corporations with the relevant public registry and be authorised by the CNV;
- the corporate purpose of the crowdfunding platforms must be to connect, within a professional framework and exclusively through web platforms, investors with entrepreneurs for the financing of projects;
- crowdfunding platforms must hold a minimum net worth of 65,350 units of purchasing value (*Unidad de Valor Adquisitivo* or UVA);[2]
- crowdfunding platforms are required to collect the information about the proposed projects, and are accountable to the investors for the due diligence in obtaining and verifying such information;
- the project issuances may not exceed 1.5 million UVAs in total in a 12-month period;
- entrepreneurs must comply with an annual and quarterly reporting regime with CNV; and
- investors are limited to a maximum investment of 10 per cent of the subscription or 150 UVAs per project, whichever is lower.

Crowdlending

The Central Bank regulates companies that provide credit services through technological platforms by connecting one or more credit providers with potential borrowers in order to carry out loan transactions in Argentine pesos (credit service providers platforms). Credit service providers platforms must be registered with the registry of private-to-private credit service providers through platforms enabled by the Central Bank. The Central Bank regulations establish certain requirements, as summarised below:

- credit service providers platforms shall neither be liable for the credit risk of the transactions made through their platforms nor guarantee the obligations entered into between the parties;
- credit service providers platforms shall neither commit to repay the credits to the investors nor acquire such credits;
- credit service providers platforms must provide all the information to identify the potential borrowers;
- funds transfers may be carried out through banks or payment accounts;
- credits granted through credit service providers platforms must be kept apart from the credit service providers platforms' net worth; and
- credit service providers platforms must have a specific manual showing the process through which the investments are carried out.

In addition, credit service providers platforms may provide credit analysis, administration and collection management services, provided that the investors retain the final decision regarding the granting of the loans.

2 Currently, one UVA = AR$1,067.33.

QR codes

Central Bank issued new regulations regarding QR codes in the frame of T3.0 payment schemes. In this respect, the T3.0 Regulations specifically contemplate payment through QR codes to promote the interoperability so that all users (ie, clients or merchants) can make payments from the same QR code to any other user (ie, clients or merchants), regardless of who initiates or accepts the payment. In addition, the T3.0 Regulations provide that:

- the QR codes that the acquirers and payment acceptors make available to their clients must comply with certain requirements and shall meet the standards defined by the Central Bank; and
- any digital wallet that allows the initiation of payments with interoperable QR codes must adapt their systems to allow the capture of QR codes associated with any request for payment, without discrimination. Hence, the 'administrators' of T3.0 under no circumstance may enable an acquirer and/or payment acceptor to receive transfer payments initiated with QR codes if they have not verified that such QR codes can be read by all digital wallets.

In May 2023, through Communiqué A 7769, the Central Bank established that any printed image, device or terminal that is provided or made available by an acquirer or payment aggregator, that allows credit card payments to be accepted by reading a QR code, shall: (1) allow the acceptance of PCTs on the same QR code displayed, when the acquirer or aggregator is also a payment acceptor; and (2) allow any digital wallet registered in the Registry of Interoperable Digital Wallets to make payments with the associated credit cards.

Additionally, in May 2024, through Communiqué A 8032, the Central Bank established that any digital wallet that allows credit card payments through QR codes shall be able to read any QR code provided by any acquirer or payment aggregator. Moreover, the Central Bank established that the rules regarding interoperability for credit card payments through QR Codes shall also apply to payments with prepaid cards.

In summary, the interoperability of QR codes for payments with transfers, credit and prepaid cards ensures that QR codes displayed by merchants can accept payments from any digital wallet registered in the Registry of Interoperable Digital Wallets, regardless of the QR code's brand.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

Until March 2024, there were no specific regulations in Argentina relating to crypto assets or cryptocurrencies. Nevertheless, under general applicable law, cryptocurrencies were classified as intangible assets rather than as currency or securities, in accordance with Section 16 of the Argentine Civil and Commercial Code, since they have a patrimonial value.

The first specific reference to crypto in a regulation was UIF Resolution No 300/2014, whereby the Argentine Information Unit (the Argentine anti-money laundering authority, or UIF for its Spanish acronym) established that AML obliged/accountable persons or entities for AML regulations must perform enhanced due diligence for clients that use digital assets for their transactions.

Also, from a tax perspective, under the Income Tax Act amendment passed in 2017, profits obtained by the sale of cryptocurrencies were established to be taxable events subject to a 15 per cent tax in Argentina.

Furthermore, in 2019, the Central Bank has issued certain regulations pertaining to cryptocurrencies and crypto assets. For example, through Communiqué A 6823, the Central Bank established the prohibition to access the official foreign exchange market to purchase foreign currency for transactions with credit, debit and prepaid cards for the 'acquisition of crypto assets in their different modalities' with foreign crypto exchanges. In addition, in 2021, the Central Bank and the CNV issued a jointed communication stating that: 'crypto assets, which are intended to be used as payment instruments or for investment purposes, are not issued or backed by a Central Bank or governmental authority and do not qualify as legal tender or negotiable instruments'.

In the same communication, the Central Bank and CNV defined crypto assets as 'a digital representation of value or rights that are transferred and stored electronically using Distributed Ledger Technology (DLT) or other similar technology. While these technologies could help promote greater financial efficiency and innovation, crypto assets are not legal tender'.

In 2022 the Central Bank issued Communiqué A 7506, which provides that banks and financial institutions are not allowed to carry out or facilitate to their clients any kind of transactions with digital assets including crypto assets (eg, NFTs). Later, in 2023, by means of Communiqué A 7759, the Central Bank extended same prohibition to PSPCPs.

In March 2024, an amendment to the Anti-Money Laundering Act No 25.246 ('AML Act') was passed to provide:

- a definition of virtual assets, defining them as 'any digital representation of value that can be traded and/or transferred digitally and used for payments or investments. Which, under no circumstances shall be understood to be an Argentine legal tender currency nor currencies issued by other countries or jurisdictions (fiat currency)';
- a definition of virtual assets service providers (VASPs), defining them as 'any human or legal entity that, as a business, performs one or more of the following activities or transactions for or on behalf of another human or legal entity:
    - exchange between virtual assets and legal tender (fiat currencies);
    - trading between one or more virtual assets;
    - transfer of virtual assets;
    - custody and/or management of virtual assets or instruments that enable control over virtual assets; and
    - participation in and provision of financial services related to an issuer's offering and/or selling of a virtual asset' (the 'Regulated Activities').
- the creation of the Virtual Asset Service Provider Registry (the VASP Registry) under CNV's scope, where VASPs, whether locals or foreign, must be registered in order to be able to operate in Argentina; and
- the incorporation of VASPs as obliged/accountable persons or entities for AML regulations.

Furthermore, the CNV through Resolution No 944/2024 ('CNV Resolution') specified that VASPs will be deemed to be performing activities in Argentina, and therefore subject to registration at the VASP Registry, when any one of the conditions listed below are met:

1. the domain name used by the VASP is '.ar';
2. there are any commercial agreements to receive funds at a national level or assets from Argentine residents to fund operations (ramp services);
3. the services are clearly targeted to Argentine residents;
4. the marketing is aimed at Argentina; or
5. the VASP's turnover in Argentina exceeds 20 per cent of the total VASP's turnover.

In addition, the CNV Resolution provides that individuals and legal entities domiciled, constituted, or residing in domains, jurisdictions, territories, or associated states included in the list of non-cooperative jurisdictions for tax transparency purposes, and considered as non-cooperative or high-risk by the Financial Action Task Force (FATF), cannot be registered in the VASP Registry.

On the other hand, the UIF issued Resolution No 49/2024 ('UIF Resolution') establishing minimum requirements for the identification, evaluation, monitoring, management and risk mitigation of money laundering/financing terrorism (ML/FT) that VASPs must comply with. To this end, the UIF Resolution established that the sole registration of VASPs in the VASP Registry triggers the obligation to be registered as an obliged/accountable entity with the UIF and to develop an AML prevention system, within 30 days as from the VASP registration with the CNV is granted.

Once registered with the UIF, among other requirements, the obliged/accountable entity must (1) have in place a Money Laundering Prevention Manual and a Code of Conduct; (2) submit systematic monthly and annual reports with the UIF; and (3) appoint AML compliance officers, who must be members of the board of directors of the VASP, noting that for foreign VASPs there is no requirements for the AML compliance officer to be an Argentine resident.

Finally, the CNV Resolution is the CNV's first step towards regulating VASPs which clearly took the approach of 'light' registration. It is likely that the CNV, in line with the approach of other jurisdictions, will issue in the coming months a new set of regulations contemplating, among others, the following:

- the need for VASPs to obtain a licence from the CNV to be able to operate in Argentina;
- a minimum capital requirement for VASPs to request a CNV licence;
- a duty for VASPs to have clear fund segregation;
- IT requirements;
- whether VASPs will require a local presence in Argentina; and
- whether cryptocurrencies are considered as securities.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

The regulatory and supervisory authority that oversees the regulation of payment services in Argentina is the Central Bank, pursuant to Section 4(g) and Section 14(j) of the Central Bank's Charter (Act No 24,144).

In addition, the Argentine National Payment System operates within a regulatory framework consisting of:

- the Central Bank's Charter;
- the Financial Entities Law;
- the Credit Card Act;
- the Executive Decree on Bills of Exchange; and
- the rules set by the Central Bank for the financial market infrastructures, the national payment system, the electronic payment system (EPS), real time payments and the clearing houses, among others.

The national payment system is a set of instruments, processes and methods to transfer funds whose purpose is to ensure the circulation of funds among the participants of the financial and banking systems. In Argentina, the national payment system is implemented through the electronic payment system operated by the Central Bank as a real-time gross settlement (RTGS) payment system that provides settlement from all participants (ie, banks and clearing houses).

The regulations on the national payment system provide that all intervening parties must operate through the Central Bank and the electronic payment system, requiring that they all hold accounts with the Central Bank and that every transaction involving debits and credits from financial entities, or any other legal entity that is part of the electronic payment system, must have the Central Bank's prior validation.

Thus, the Central Bank is the governmental entity that regulates, controls, and provides the legal framework for PSPs and digital wallets. Such regulations provide that there are nine types of PSPs:

1. PSPCPs;
2. administrators;
3. payment acceptors;
4. payment service providers who perform payment initiation activities (PSIs, for its Spanish acronym);
5. ATM networks;
6. electronic fund transfer networks;
7. acquirers;
8. payment aggregators; and
9. extra-bank tax and/or service collection companies.

PSPCPs are defined by the regulations as the ones who offer virtual payment accounts. If the PSPCPs were to perform digital wallet services in addition to offering virtual payment accounts, they must adapt their operational and commercial description accordingly and update their registration as a PSP with the Registry of Payment Service Providers of the Central Bank.

On the other hand, PSIs are defined by the regulations as those who offer digital wallets services through a mobile app or a web browser, which allows: (1) immediate payments; and/or (2) credit, debit and/or prepaid card transactions. If the PSIs were to offer digital wallet services, they must be registered in the Registry of Payment Service Providers with the Central Bank as a PSP.

Additionally, as from March 2024, as mentioned in Question 2, the amendment to the AML Act included PSPs as AML-obliged/accountable entities with the UIF. Consequently, all PSPs must also register with the UIF. This registration obliges PSPs to implement an AML system and file periodic reports with the UIF regarding their clients' transactions to prevent ML/FT.

Regarding digital wallets, please see our comments to Question 1 above, regarding the definition of digital wallet service and the Registry of Interoperable Digital Wallets. In addition, please find below a list of the requirements for registration with the Interoperable Digital Wallets Registry:

- be registered as a PSPCP or PSI;
- comply with the information regime with the Central Bank; and
- file with the Central Bank the following:
    - certification issued by the each of the administrators of the Transferencias 3.0 payment scheme authorised by the Central Bank, stating that the service to be provided has successfully completed the integration with each of the acceptors adhered to its payment scheme, and that it is ready to be used by the general public to make payments by transfer through the reading of the QR codes generated by each and every one of those acceptors;
    - personal information of the person in charge of the technology and information systems matters;
    - personal information of the person in charge of the information security and asset protection matters;
    - locations of processing centres; and
    - a list of suppliers providing information technology systems and information security services.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

In Argentina, there are no special programmes supporting the fintech ecosystem or fintech startups, such as regulatory sandboxes and accelerator programmes.

Nevertheless, in the recent years (since 2016 to date), the Central Bank has organised 'financial innovation tables' as a dialogue forum between public and private stakeholders to develop initiatives related to financial inclusion and technology applied to financial services. The main points discussed may be summarised as follows: (1) payment infrastructure; (2) technology applied to payment schemes; (3) alternative credit and savings channels; and (4) blockchain technology. In addition, after the development of the T3.0 Regulations, the Central Bank has promoted special meetings among many payment industry players in Argentina to discuss this new payment scheme, particularly in relation to tax matters.

Moreover, the Central Bank has developed a 'Financial Innovation Programme' for all professionals, entrepreneurs and students who are specialists in the financial innovation field. The main purpose of the programme was to develop a wide range of projects related to: (1) digitalisation; (2) digital payments; (3) alternative scoring; (4) data and end user protection regulations; and (5) financial opportunities, among others. This programme was aimed to foster financial inclusion through a collaborative work between public and private stakeholders.

Additionally, in Argentina, there are governmental incentives for startups and fintech businesses (ie, small and medium-sized businesses), such as tax incentives, related to investment and development in technology. In 2019, the Knowledge Economy Promotion Act No 27.506 was enacted to promote economic activities related to the use of knowledge and the digitalisation of information, supported by advances in science and technology, to obtain goods, provide services and/or improve processes. The main benefits are the following: (1) reduction in the amount of income tax, (2) reduction in social security contributions, and (3) exemption of certain subjects from withholdings and collections for exports contemplated by VAT.

Finally, it is worth mentioning that in Jul 2024, the so-called Bases and Starting Points for the Freedom of Argentines Act No 27742 was passed, which among others contemplates an incentive scheme for large investments (*régimen de incentivos para grandes inversiones*) applicable to, among others, technology industry projects, which investments (1) exceed the US$200m; (2) qualify as a unique project vehicle (VPN, for its Spanish acronym); and (3) are long-term investments. The purpose of the incentive scheme for large investments is to encourage new investments in Argentina by promoting benefits such as (1) customs benefits; (2) tax exemptions; and (3) exemptions to enter and liquidate foreign currency from exports of goods and/or services.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

Currently, in Argentina there are no specific regulations for open banking. Argentina does not have an open banking law like the European model developed in recent years. Nevertheless, there are several companies in Argentina which have launched their businesses incorporating some of the principal characteristics from the European model, in anticipation of the development of the open banking system.[3]

3 'One of the pioneers in laying the first foundations to move towards a more open and collaborative ecosystem is BIND (Banco Industrial). This bank, together with Poincenot Technology Studio, launched open APIs into the market, which is one of the fundamental pillars of Open Banking [...] Another example of open banking in Argentina is the Digital Wallet MODO.' Jose Marcos, 'First Steps Towards Open Banking Excellence' (Open Banking Excellence, 9 September 2021), www.openbankingexcellence.org/blog/first-steps-towards-open-banking-in-argentina.

Bolivia

Teddy Mercado*
Moreno Baldivieso, La Paz
tmercado@emba.com.bo

Mirko Olmos†
Moreno Baldivieso, Santa Cruz de la Sierra
molmos@emba.com.bo

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

Bolivia does not currently have laws or regulations in place specifically for fintech or financial innovation.

However, there are currently two bills in the Legislative Assembly under consideration. The first one, presented on 13 June 2023 by the ruling party, is a Bill for a Crypto Assets and Financial Technology Regulation Law. The second bill, presented on 31 August 2023 by the opposition, is a Crypto Assets Integral Adoption Law. Both initiatives aim to legalise and regulate the use of cryptoassets in Bolivia, which is currently prohibited.

In general, the financial system in Bolivia is supervised and regulated by the Financial System Supervisory Authority (FSSA), while the payment system is regulated by the Bolivian Central Bank (BCB).

Bolivian law distinguishes three types of financial institutions: (1) state-owned or majority state-owned financial institutions (ie, public banks), (2) private financial intermediation institutions (ie, private banks), and (3) complementary financial services companies (ie, mobile payment companies, currency exchange companies, electronic card management companies, among others).

While Bolivian law prohibits the incorporation of financial entities not authorised by law or admitted by the regulator, in practice fintech companies from determined verticals often apply rules of the Civil Code and the Commercial Code for the provision of their services without requesting regulatory approval. Additionally, they must comply with the General Law on the Rights of Users and Consumers, which forbids misleading or abusive advertising and any information or omission about the products offered is prohibited among other things.

On 21 September 2022, BCB issued a new Payment Services, Electronic Payment Instruments, Clearing and Settlement Regulation, approved by Board Resolution No 079/2022 (2022 BCB Payment Services Regulation). Under this regulation, BCB included provisions to improve the

* Teddy is a Partner of Moreno Baldivieso and is co-head of the banking and financial practice. He promoted the creation of the Fintech & Technology department in Moreno Baldivieso and currently leads this practice. He advises local and international companies on corporate structures, M&A, banking and financial services, fintech products, regulatory and contractual matters in Bolivia.

† Mirko is an associate of Moreno Baldivieso's banking and financial practice and fintech and technology law. He promoted the creation and co-led the development of the fintech and technology practice at Moreno Baldivieso. He advises local and international companies with commercial and regulatory matters, including mobile and digital wallets, digital payment systems and processors, paytech companies, lending platforms, challenger banks, online gambling and betting companies and tech conglomerates.

use of QR codes by regulated entities, requiring them to enable this method of payment within determined times.

Additionally, in September 2022, the Preliminary Draft Law on Support for Entrepreneurship and the Digital Economy was presented by the Agency for e-Government and Information and Communication Technologies (AGETIC). As of the date hereof, this draft has not been discussed by the Bolivian Senate, however, there is a positive outlook from the corresponding authorities. The main issues addressed by this Draft Law are:

- creating the Entrepreneurship Development Fund, a public entity with the purpose of promoting and incentivising startups in Bolivia;
- regulating investments in the private sector on startups by allowing the creation of venture capital institutions;
- regulating digital platforms and crowdfunding;
- allowing startups to request non-objection authorisations to the applicable regulators;
- allowing the creation of regulatory sandboxes;
- creating a new type of company, simplified joint stock companies, which allow a single shareholder with limited liability; and
- defining the tax treatment of capital contributions to startups.

It is not possible to confirm when this law will be approved, nor its final content.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

Since 2014, BCB has demonstrably been against the use of currencies not regulated by 'states, countries or economic zones' in the Bolivian payment system. This stance has become even clearer since the end of 2020, with Board Resolution No 144/2020, which prohibited:

- financial entities processing payment orders for the purchase and sale of crypto assets;
- linking or associating electronic payment instruments (EPI) (ie, debit or credit cards) regulated by BCB to crypto assets; and
- using authorised EPIs to buy crypto assets through electronic payment channels.

Furthermore, in May 2020, BCB issued a press release where it reiterated Board Resolution 144/2020 and recommended against the use of crypto assets. On 4 October 2022, FSSA modified the Regulation for the Issuance and Management of Electronic Payment Instruments, reaffirming the BCB prohibition on all regulated entities.

Currently, there are two bills under discussion in the legislative assembly, which aim to legalise and regulate the use of cryptoassets in Bolivia.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

The Bolivian Payment System is regulated by BCB and supervised by FSSA. In practice, BCB issues regulations related to payment activities and instruments, while FSSA issues specific regulations and supervises its compliance within the framework of the regulations issued by BCB.

The 2022 BCB Payment Services Regulation includes the following regulated entities as payment services companies:

- electronic card administrators;
- money remittance and remittance companies;
- mobile payment services companies; and
- money exchange companies.

FSSA is in charge of approving the incorporation and licensing of these companies. Additionally, they must comply with FSSA regulations to provide services, and with applicable specific anti-money laundering, combatting the financing of terrorism and financing of the proliferation of weapons of mass destruction (AML/CFT/WMD) rules approved by the Financial Investigations Unit.

Only one type of digital wallet is allowed in Bolivia: mobile payment services companies. They are regulated by FSSA and must comply with the parameters established by law and specific regulation. These companies are only allowed to perform the following activities:

- operating mobile payment services;
- issuing mobile wallets and operating payment accounts;
- electronically executing payment orders and queries with mobile devices through mobile phone operators; and
- others related to payment services, subject to authorisation by FSSA.

In the 2022 BCB Payment Services Regulation, BCB included the definition of a payment gateway administrator (PGA) as a legal entity that provides payment channels between affiliated merchants or establishments and financial intermediation institutions (FIE) (eg, banks) or payment service providers (eg, mobile wallets) (PSP). Its function is to register and transmit payment orders exclusively with electronic payment instruments (which are approved by the Central Bank). It defines two roles:

- *Aggregator*: allows the receipt of outgoing payments. They receive, group and transfer payments within a given period of time; and
- *Facilitator*: routes and facilitates the processing of online transactions. Resources are transferred directly to accounts.

BCB chose to assign FIEs and PSPs liable to users for damages caused by a PGA with which they have a contractual relationship. It also included the minimum content that the agreements between EIFs/PSPs and PGAs must have.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

Bolivia does not currently have any special programmes supporting the fintech ecosystem. There are private accelerator programmes that support startups in general. However, they are not specifically for fintech startups. Please refer to Question 1 to see current initiatives from the Bolivian Government to promote these programmes with the Preliminary Draft Law on Support for Entrepreneurship and the Digital Economy.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

Bolivia has no specific open banking regulation. There have been initiatives from the regulators for interconnection and interoperability from the regulators, which could lead to the establishment of open banking.

In 2021, the BCB issued its annual payments system surveillance report which establishes that the next stage of payment system development in Bolivia will promote the emergence of innovative business models for which schemes such as open banking will be necessary. Thus, open banking is already on the regulators' radar. It is yet to be seen whether they will issue specific regulation on this matter.

The following provisions from the Financial Services Law may have an indirect effect on open banking:

- financial consumers have the right to confidentiality, with the exceptions provided by law;
- transactions carried out within the framework of the services provided by financial institutions may be carried out by electronic means, which must necessarily comply with the security measures that guarantee integrity, confidentiality, authentication and non-repudiation; and
- financial operations carried out by natural or legal persons, Bolivian or foreign, with financial institutions shall enjoy the right of reserve and confidentiality. Any information referring to these operations shall be provided to the owner, to whom they authorise or to whoever legally represents them. Thus, potential conflicts with privacy and data protection of financial consumers should be considered. Bolivia does not yet have a personal data protection law.

In practice, some banks in Bolivia have decided to include open banking initiatives by providing access to their APIs, allowing companies to develop software.

Brazil

Bruno Balduccini
Pinheiro Neto, Sao Paulo
bbalduccini@pn.com.br.

Nicolás Alonso
Pinheiro Neto, Sao Paulo
nalonso@pn.com.br

Micaela Boruchowicz
Pinheiro Neto, Sao Paulo
mboruchowicz@pn.com.br

Alexia R. Campedelli
Pinheiro Neto, Sao Paulo
acampedelli@pn.com.br

1. Fintech regulatory framework: please provide a description of the most relevant laws and regulations on fintech and financial innovation in your country. Please also refer to any new law or regulation foreseen in the near future or any bill on fintech and financial innovation in your jurisdiction.

Brazil has a cutting-edge regulatory framework applicable, among others, to digital lending (fintechs), payments and acquiring services, foreign exchange and remittances, insurance, asset management and crypto. In recent years, the Brazilian Congress, the Central Bank and other relevant regulators have built a modern regulatory framework aiming to foster competition and promote entry and adoption of new technologies in those sectors.

It is worth mentioning that the term 'fintech' is widely and indistinctively used in the Brazilian market to describe both payment institutions (which include e-money issuers, credit card issuers, acquirers and payment initiation service providers) and digital lending entities (which include direct credit companies and peer-to-peer lending companies). Even though the regulatory requirements are somehow similar, payment institutions and digital lending fintechs have different regulatory frameworks.

The main regulatory frameworks applicable both to payment institutions and digital lending fintechs are as follows.

Payment institutions

Law 12.865 of 9 October 2013, National Monetary Council – CMN Resolution No 80 of 2021, CMN Resolution No 81 of 2021, and Central Bank – BCB Resolution No 96 of 2021 (as amended). Payment institutions are legal entities that have as their principal or ancillary activity, the provision of payment services to end-customers. Payment institutions are classified based on the services provided, as follows:

1. **Issuers of electronic currency (eg, issuers of pre-paid instruments):** Entitled to offer and manage prepaid accounts and allow its clients to make payment transactions with the electronic currency deposited into such accounts.[1]

2. **Issuers of post-payment instruments (eg, issuers of credit cards):** Entitled to offer and manage registered post-paid payment accounts to its clients and allow such clients to make payment transactions with such accounts. These entities cannot lend (such as revolving loans) to its clients.

3. **Acquirers:** Institutions that (1) enable recipients (merchants) to accept payment instruments issued by a payment institution or by a financial institution; and (2) participates in the process of settlement of payment transactions as a creditor before the issuer, in accordance with the rules applicable to payment arrangements.

4. **Payment transaction initiators:** Entitled to offer payment transaction initiation services but not authorised to offer and manage any payment accounts and may not receive or hold at any time the funds transferred within the provision of the service.

E-currency issuers and payment transaction initiators require prior authorisation from the Central Bank to start operations. Issuers of post-payment instruments and acquirers may start operating without Central Bank´s prior approval and once they hit specific volume thresholds can continue to operate but must request authorisation from the Central Bank. Regulated payment institutions (eg, after Central Bank approval is obtained) should comply with certain regulatory requirements including, but not limited to, (1) minimum capital requirements, (2) prudential requirements, (3) reporting and risk administration system requirements, (4) data protection laws, (5) bank secrecy regulations, (6) consumer protection laws, etc.

Digital lending fintechs

Law 4.595 of 31 December 1964, and CMN Resolution No 4.656 of 26 April 2018, as amended by CMN Resolution No 5.050 of 25 November 2022, with effect as of 1 January 2023. Such digital lending fintechs are considered 'financial institutions' and as such can lend money to third parties and follow a simplified and lighter regulatory regime. This is particularly important to the Brazilian market because, different from other jurisdictions in Latin America, the activity of granting loans even with its own capital is a regulated activity[2] that requires prior authorisation from the Central Bank.

The digital lending fintechs are classified as follows:

1. **Direct credit companies – SCDs:** Financial institutions entitled to grant loans and financing to borrowers exclusively by means of electronic platforms and by using their own capital. SCDs are not entitled by law to offer deposit-taking products and, thus, are not entitled to perform financial intermediation to leverage lending activity with its deposit-taking activity. Besides granting digital loans, SCDs are also entitled to offer the following services: (1) perform credit

1 Clients' funds contained in such accounts are bankruptcy remote and cannot be used by the payment institution to funds its operation. In addition, clients' funds, while not being used, must be either deposited at the Central Bank or used to purchase government bonds.

2 Lending without a proper licence (as a financial institution) constitutes a crime. Not all financial institutions are allowed to lend money. Commercial banks, multipurpose banks with specific licences, credit, investment, financing entities, SCDs and SEPs are types of financial institutions that are authorised to lend.

rights acquisition operations; (2) credit analysis services for third parties; (3) collection of credit rights services; (4) act as an insurance representative in the offering of insurance products related to the services mentioned above; (5) issuance of electronic currency (eg, issuer of pre-paid cards); and (6) post-paid payment instruments (eg, credit cards).

2. **Person-to-person loan companies – SEPs:** Financial institutions that have as purpose offering a digital platform that creates a lending marketplace between companies, securitisation vehicles and individuals as lenders and companies and individuals as borrowers. Besides that, SEPs are also entitled to (1) credit analysis services for third parties; (2) collection of credit rights services; (3) act as an insurance representative in the offering of insurance products related to the services mentioned above; and (4) issuance of electronic currency (eg, issuer of pre-paid cards). SEPs are not entitled to fund directly the loans offered within their platforms and are not entitled to retain the funds disbursed by the lenders within their platforms.

As mentioned, both SCDs and SEPs require prior authorisation from the Central Bank to start operations, and should also comply with several regulatory requirements including, but not limited to:

- minimum capital requirements;
- prudential requirements;
- reporting and risk administration system requirements;
- data protection laws;
- bank secrecy regulations; and
- consumer protection laws.

In essence, an SCD is a lighter bank subject to lesser financial regulatory requirements.

2. Regulations on crypto assets: please provide a summary of the legal framework of crypto assets in your country and how crypto assets are regulated in your jurisdiction.

Like other Latin American countries, as of November 2022, Brazil had no specific legal framework applicable to the crypto assets industry. However, on 22 December 2022 Law No 14.478 was published (Law No 14.478/22) aiming to regulate the crypto assets market in Brazil. Although published, such Law came into force only 180 days after its publication, on 20 June 2023. Law No 14.478/22 is aligned with global regulatory standards, including the recommendations of the Financial Action Task Force in connection with virtual assets. It also focuses on combatting crypto-related crimes, and removes crypto assets from the regulatory and supervisory scope of attributions of the Brazilian Securities and Exchange Commission (Comissão de Valores Mobiliários or CVM), and creates instruments to reduce the ecological footprint of the mining process through tax incentives.

Therefore, since it came into force, (1) the 'digital assets service providers' (which is the name that the bill grants to those entities involved in a crypto transaction, or VASPs) wishing to operate in Brazil require a regulator's prior authorisation, and (2) the digital assets service providers that were already

operating before the new law was enacted have, at least, six months to adapt themselves to the new applicable regulations and may continue to operate until the relevant authorisation is granted; and (3) such digital assets service providers must comply with certain minimum regulatory requirements such as risk management, operational and capital requirements, etc.

Pursuant to the approved text of Law No 14.478/22, 'digital assets service provider' is defined as a legal entity that performs, on behalf of third parties, at least one of the following digital assets services:

- trade between digital assets and national or foreign currency;
- trade between one or more digital assets;
- transfer of digital assets;
- custody or management of digital assets or instruments that confer control over digital assets; or
- participation in financial services and provision of services relating to the offering by an issuer or sale of digital assets.

Recently, on 14 June 2023, Decree No 11.563 (Decree 11.563/23) was published, regulating Law No 14.478/22 and appointing the Central Bank as the authority responsible for regulating and supervising the entities that may be classified as VASPs within the scope of said Law. Decree 11.563/23 gives the Central Bank power to: (1) regulate the provision of virtual asset services, subject to the guidelines of Law No 14.478/22; (2) regulate, authorise and supervise VASPs; and (3) deliberate on the other scenarios established by Law No 14.478/22, except for the operation of the National Registry of Politically Exposed Persons (CNPEP) created by the aforementioned law. Moreover, Decree 11.563/23 also reinforces that it in no way alters the powers of the CVM.

Decree 11.563/23 came into force on 20 June 2023, the same date as Law 14.478/22. In view of the principle-based nature of Law 14.478/22, the regulation issued by the Central Bank will be a determining factor in ensuring that the new legal framework brings greater judicial safety to the Brazilian market and greater protection for its investors.

Until Law No 14.478/22 came into force, the following applied to the crypto assets industry in Brazil:

1. no prior licence or prior authorisation is required to operate a crypto exchange in Brazil or to offer crypto assets in the Brazilian market provided that such crypto assets do not fall within the legal definition of a security (in Portuguese, a *valor mobiliario*). Conversely, if the crypto asset falls within the definition of a security, then the following would need to be complied with: (a) the issuer needs to be previously registered before CVM and the offering needs to be listed and authorised by the CVM; and (b) the offering and distribution needs to be performed by a regulated entity such as a broker. This did not change with Law No 14.478/22, as securities are excluded from the virtual assets concept. Therefore, everything that involves assets that could potentially be characterised as securities must observe CVM's rules;
2. any acquisition or sale of crypto assets between a Brazilian individual or entity and an offshore individual or entity required a foreign exchange transaction to be entered into with a local financial institution authorised to operate in foreign exchange. In practice, the remittance of

funds abroad to purchase a crypto asset needed to be performed with the intermediation of a regulated financial institution. This did not change when Law No 14.478/22 came into force;

3. in general, according to the CVM´s opinions and communiques, depending on the economic essence of the rights granted to their holders and the function assumed thereby, certain crypto assets and tokens may be deemed securities; and

4. crypto exchanges need to comply with the general anti-money laundering regime applicable to any non-regulated entity.

Now Law No 14.478/22 is effective and the regulatory authority has been designated, the new regulation for VASPs will follow and shall set a period (not shorter than six months) for those entities to adapt to the new rules. Such new regulation, to be issued by the Central Bank, will yet establish the rules for the licence to be required from VASPs.

Therefore, while the general guidelines, definitions, and principles applicable to VASPs are already known, at this moment there are no formal licensing options available for VASPs in Brazil.

3. Payment service providers and digital wallets: please describe how payment service providers and/or digital wallets are regulated in your country. Please mention any foreseen law or regulation in this respect.

Please refer to our answer in Question 1.

4. Special support to fintechs: does your jurisdiction provide any special programme supporting the fintech ecosystem, in particular fintech startups (eg, regulatory sandboxes, accelerator programmes). Are such programmes supported by the regulator in your country?

Yes, the Central Bank created and implemented a regulatory sandbox to support and foster the entrance of new innovative players to the Brazilian market. Like other Latin American jurisdictions, the regulatory sandbox is a controlled environment in which companies are authorised by the Central Bank to test, for a limited period, an innovative project related with the financial or payment markets. The purpose of the sandbox is to stimulate innovation and diversity of business models, and foster competition within the Brazilian financial system (SFN) and the Brazilian payment system (SPB).

The Central Bank also created the Financial and Technological Innovation Laboratory (LIFT), which is a joint initiative of the Central Bank and National Federation of Associations of Central Bank Servers (Fenasbac). The main purpose of LIFT is to foster innovation by encouraging the creation of prototypes of technological solutions for the financial system. This means that LIFT is truly an ecosystem aimed and owed to innovation.

Finally, other regulators such as the CVM and the Superintendency of Private Insurance have their own regulatory sandboxes with similar purposes and regulations, aiming to foster innovation in their relevant industries.

5. Open banking: please advise whether in your jurisdiction there are regulations on open banking. If the response is no, please provide any reference to regulations that may directly or indirectly affect open banking. Please include any foreseen laws and regulations on open banking.

Yes, Brazil has a specific legal framework and a highly developed open finance system. According to the current regulatory framework contained in Joint Resolution No 1 of 2020, issued by the Central Bank and the CMN, and several normative instructions issued by the Central Bank, the Brazilian open finance system is defined as the system that allows customers of financial products and services to share their information between different financial institutions duly authorised by the Central Bank to receive a better financial product or service through the integration of platforms and infrastructure of information systems, enhancing transparency among the institutions and their customers.

Recently, the Central Bank decided to change the name of the system from 'open banking' to 'open finance', with the purpose of allowing the sharing of financial information not only related with traditional financial products (savings accounts and loans), but also information related with any financial product such as foreign exchange, acquiring, investment, insurance, etc. In general terms, this new environment aims to integrate the financial system to the different digital innovations and to reduce the informational asymmetry among financial service providers.

The Brazilian open finance system follows the following principles.

1. As described above, only regulated entities may participate in the open finance system to guarantee the privacy, due storage, encrypted sharing and correct processing of confidential personal and transactional data which is subject to bank secrecy obligations. Despite of the foregoing, the current regulatory framework applicable to the open finance system provides for mandatory and voluntary participants, which will depend on the significance and size of the financial institution in the Brazilian market.

2. The open finance system did not modify or alter the Brazilian General Data Protection Law, which needs to be strictly complied with among the participants.

3. The main purpose of the open finance system is to foster competition and provide transparency to the users.

4. Users are the owners of their data and, thus, the open finance system is based on the principle that data sharing is only legally and practicably possible upon user's express consent.

5. The Central Banks regulated the minimum governance and technical standards to be mandatorily adopted among participants in order to be plugged in to the open finance system.

Alongside the implementation of the open finance system, the Central Bank is updating and improving the regulation to enhance the system's efficiency, which is in line with Agenda BC#, which focuses on tackling structural issues of the National Financial System by fostering technological innovation.

In this sense, on 23 February 2023, the Central Bank issued BCB Resolution No 294 and BCB Resolution No 295, updating the technical requirements and operational procedures for open finance implementation and waiving the mandatory participation of account-holding institutions in specific situations, with effect from 1 April 2023.

Lastly, and most recently, on 29 August 2023, the Central Bank issued BCB Normative Instruction No 409, publishing the latest version of the Open Finance Customer Experience Manual, which must be followed by participating institutions.

Chile

Matías Langevin Correa
HD Legal, Santiago
mlangevin@hdgroup.cl

Javiera Ruiz-Tagle Lyon
HD Legal, Santiago
ruiztagle@hdgroup.cl

Fernanda Aillach Núñez
HD Legal, Santiago
faillach@hdgroup.cl

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

Currently, the most relevant laws and regulations on fintech and financial innovation in Chile comprise Law No 21,521, which promotes competition and financial inclusion through innovation and technology (the 'Fintech Law' or 'Law') and its secondary regulation issued by the Financial Market Commission (CMF).

The Fintech Law

The main objective pursued by this Law is to establish a general framework to encourage the provision of financial services using technological means by the service providers governed by it. Among the many innovations contained in the Law, the following aspects must be highlighted.

- The legal recognition and regulation of virtual financial assets or cryptoassets, which the Law defines as 'digital representation of units of value, goods or services, other than money, whether in local or foreign currency, which can be transferred, stored or exchanged digitally'.
- The regulation of parametric insurance, ie, insurance that, upon the occurrence of a predefined event covered by the policy, obligates the insurer to pay the claim, releasing the insured party from having to justify the existence or amount of the damage, and even if there was no actual loss.
- Contracts for difference (CFDs) are now expressly regulated as financial instruments.[1]
- The Fintech Law incorporates new reporting agents to the Financial Analysis Unit (UAF) pursuant to Law No 19,913 (anti-money laundering and countering the financing of terrorism): entities registered in the Registry of Financial Service Providers and in the Registry of Payment Initiation Service Providers regulated in the open finance system, which provides crowdfunding platforms, alternative trading systems, custody of financial instruments, brokering of such instruments and initiation of payments.

1 Before the Law, as was the case for crypto assets, CFDs were not considered securities by the CMF and, therefore, were outside its scope of regulation and oversight.

- New payment methods: digital, electronic or computerised representations, registered through systems that use distributed ledger or other similar technologies (such as blockchain), of units whose value is directly determinable and backed by money (such as stablecoins). These digital, electronic or computerised representations may be the object of payment orders regulated in the Organic Law of the Central Bank of Chile.
- New foreign currencies: the abovementioned digital, electronic or computerised representations are now also included in the concept of foreign currency.

The Law is divided into two main subjects: (1) regulated fintech services and (2) an open finance system.

Financial services

Regarding regulated financial services, the Fintech Law regulates the commercialisation of the following technology-based financial services.

- *Crowdfunding platforms*: Physical or virtual places through which those who have investment projects or financing needs divulge, communicate, offer or promote those projects or needs, or the characteristics thereof, and contact or obtain contact information of those who have available resources or the intention of participating in or satisfying those projects or needs; in order to facilitate the materialisation of the financing operation.
- *Alternative trading systems (ATS)*: Physical or virtual places that allow their participants to quote, offer or trade financial instruments, or publicly offered securities, and that is not authorised to act as a stock exchange or commodities exchange pursuant to applicable laws (includes operations in crypto assets, derivatives and CFDs).
- *Credit advisory*: Provision of evaluation services or recommendations to third parties regarding the capacity or probability of payment by a person or entity, or concerning their identity, for the purpose of obtaining, modifying or renegotiating a loan or financing agreement.
- *Investment advisory*: Provision of evaluation services or recommendations to third parties regarding the convenience of making certain investments or transactions in publicly traded securities, financial instruments or investment projects.
- *Custody of financial instruments*: Safekeeping, on their own behalf but also on the account of third parties, or on behalf of third parties, of financial instruments, money or foreign currencies arising from cash flows or from the selling of financial instruments held in custody, or that have been delivered by them for the acquisition of financial instruments or to guarantee transactions with such instruments.
- *Order routing and brokerage of financial instruments*: Service for channelling orders received from third parties for the purchase or sale of publicly offered securities or financial instruments to ATS, securities intermediaries or commodity exchange brokers.

The Fintech Law establishes the obligation of registration in the Registry of Financial Service Providers (the 'Registry'), to any person who decides to professionally engage in the provision of

the financial services regulated by it. After the registration, the Law establishes that the proper authorisation from the CMF must be obtained prior to initiating the provision of the financial services regulated therein.

Notwithstanding the above, some entities already supervised by the CMF may provide the financial services regulated in this Law without the need to register in the Registry.

Open finance

The Fintech Law establishes basic rules and principles to regulate an open finance system which allows the exchange of information between different information service providers regarding financial customers who have expressly consented to it, and other types of data set forth in the Law, through remote and automated access interfaces that allow for interconnection and direct communication between participating institutions ('Participating Institutions').

The Participating Institutions are the following:

- information providers;
- information-based services providers;
- account providers; and
- payment initiation services providers.

These institutions must adopt the necessary measures to allow the consultation, access, delivery and exchange of information regarding the types of data, products and financial services related to financial clients who have contracted such products or services, or carried out transactions with them, in an expeditious and secure manner, under the conditions established by the CMF by means of a General Rule.

The delivery and exchange of information shall be carried out through one or more remote and automated access interfaces (APIs) maintained by the Participating Institutions, whose minimum standards are determined by the CMF by means of a General Rule.

Other relevant rules established in the Fintech Law

The Fintech Law also regulates the following matters related to financial service providers.

It establishes that such providers must adopt policies, procedures and controls aimed at preventing the offering of products that do not meet the needs, expectations and risk profile that customers have previously communicated to them regarding the products and services they wish to acquire. Therefore, they should offer their financial products and services according to the customer's profile.

Moreover, banks offering current account services must establish public, objective and non-discriminatory conditions to offer and provide access to such services to financial providers regulated by this law, to issuers and operators of payment cards and to other financial institutions supervised by the CMF.

Secondary regulation

The Fintech Law delegated to CMF the issuance of the secondary regulation of activities governed by said Law.

In this regard, on 12 January 2024, the CMF issued General Rule No 502 (NCG No 502) which regulates the registration, authorisation and obligations of financial services providers, and which came into effect on 3 February 2024. NCG No 502 consolidates in a single regulatory framework the instructions and requirements for financial service providers.

The main aspects regulated by NCG No 502 concerning financial service providers include:

- registration in the Registry;
- authorisation for the provision of financial services;
- disclosure obligations and information delivery to clients and the public;
- corporate governance and risk management;
- minimum capital and guarantees for certain financial service providers;
- operational capacity; and
- inherent activities.

On 4 July 2024, the CMF issued General Rule No 514 (NCG No 514) which regulates the open finance system. The main aspects regulated by NCG No 514 regarding the open finance system include:

- perimeter;
- operation;
- security and safeguards;
- information;
- sanctions; and
- terms to implement it.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

The Fintech Law expressly defines virtual financial assets or crypto assets, stating that they are 'digital representations of units of value, goods, or services, with the exception of money, whether in national currency or foreign currency, that can be transferred, stored, or exchanged digitally'.

Likewise, for the purposes of the Fintech Law, it considers crypto assets (as defined) to be a financial instrument when they are represented through a title, contract, document, or incorporeal asset.

In this context, the Fintech Law regulates financial services providers, who may engage in certain lines of business involving crypto assets, namely: (1) custody; (2) intermediation; (3) order routing; (4) investment advice; and (5) alternative trading systems.

On the other hand, the Fintech Law introduced amendments to various regulatory frameworks where stablecoins are referenced as: (1) a means of payment, (2) currencies, and (3) subject to payment orders.

As for relevant tax implications, the Chilean Internal Revenue Service (*Servicio de Impuestos Internos*) has issued several rulings on the taxation applicable to crypto asset transactions. In its General Notice No 963 of 2018, relating to the taxation arising from the purchase and sale of cryptocurrencies (specifically, Bitcoin), both at the income tax level and at the VAT level, it concluded that the income gains are taxable pursuant to general-application income taxes. With regards to VAT, the sale of Bitcoins or other virtual or digital assets is not subject to this tax, as it concerns intangible goods.

On a different case, analysed in General Notice No 1371-2019, the Chilean Tax Authority considered that the intermediation of digital assets is classified in No 4 of article 20 of the Income Tax Law, and that the commission received by the intermediary is subject to VAT.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

Payment service providers

The Central Bank of Chile's Compendium of Financial Regulations (*Compendio de Normas Financieras*), in Chapter III.J.2 concerning the operation of payment cards (credit, debit, and prepaid cards), regulates payment processing service providers (PSPs).

In this context, Chapter III.J.2 establishes that such companies will be exempt from said regulation when they only render the following services to payment cards issuers and/or operators:

- the authorisation and registration of transactions made by cardholders or card users;
- the procedures for affiliation of entities to the system, not including the provision of services regulated as part of the operation of cards;
- the provision of point-of-sale terminals, or electronic or computerised channels or applications that allow the authorisation, capture, aggregation and communication of payment transactions, so that they may be subsequently processed by an operator for settlement and/or payment purposes; and
- other activities related to the operation of cards, provided that they do not involve the settlement and/or payment of benefits due to affiliated entities for the use of such instruments.

On the other hand, the aforementioned chapter states that PSPs may exceptionally provide services that include the settlement and/or payment of amounts due to affiliated entities for transactions made with payment cards, without being subject to the requirements and obligations imposed on payment card operators, provided that two conditions stated in the aforementioned regulations are met:

- that the PSP enters into a contract or agreement with an issuer or acquirer, in which it is expressly stated that any of the latter has assumed or shall assume the corresponding payment responsibility before the affiliated entities, notwithstanding that the respective PSP shall make the settlements and/or payments that may be applicable;[2] and
- the settlement and/or payments made by a sub-acquirer, over the preceding 12 months, on behalf of one or more issuers or acquirers with whom it maintains a current contract or agreement for this purpose, must be less than 50 per cent of the 1 per cent of the total payment amount to affiliated entities made by all acquirers governed by this regulation during the same period (sub-acquiring threshold).

If a PSP engaging in sub-acquiring activities reaches or exceeds, for two consecutive quarters, 50 per cent of the sub-acquiring threshold with respect to one or more issuers or operators, it must establish itself as a sub-acquiring acquirer and comply with the following requirements:

- it must enter into a contract or agreement with an issuer or another acquirer, explicitly stating that the issuer or acquirer has assumed or will assume the corresponding payment responsibility to affiliated entities, which must also be documented in the relevant affiliation contract;
- this contract or agreement must specify the type of payment cards involved;
- it must demonstrate having paid-up capital and reserves equal to or greater than the equivalent of 1,000 UF (*Unidades de Fomento*);
- their bylaws must exclusively refer to the activity of acquiring payment cards under the sub-acquiring modality and any complementary activities authorised by the CMF through General Rules; and
- it cannot enter into a contractual relationship with another sub-acquiring acquirer for the purpose of receiving sub-acquiring services.

Then, the PSP must apply for registration in the Card Acquirers Registry managed by the CMF, following the instructions issued by that entity.

Lastly, if the settlement and/or payments made by a sub-acquiring acquirer, on behalf of one or more issuers or acquirers with whom it maintains a current contract or agreement for that purpose, exceed, for two consecutive quarters, the 1 per cent of the total payment amount to affiliated entities made by all acquirers governed by this regulation over the preceding 12 months, it must comply, within the timeframe and under the terms and conditions established by the CMF, with the minimum capital and liquidity reserve requirements stipulated in Chapter III.J.2 for the acquirers, as well as make any necessary statutory and operational adjustments.

Digital wallets

With regards to digital wallets, Law No 20,950 authorises the issuance and operation of prepaid means of payments by non-banking entities.

Pursuant to this law, in Chile there is a similar figure to the digital wallets that is used for similar purposes and consists of the prepaid funds accounts (*Cuentas de Provisión de Fondos* or CPF), which are

2 This exception shall not apply to sub-acquiring acquirers engaged in cross-border acquiring.

specifically regulated in Chapter III.J.1.3 of the Central Bank of Chile's Compendium of Financial Regulations, regarding the issuance of prepaid payment cards.

This chapter sets forth that the sole purpose of these accounts is to receive funds destined to be used for prepaid payment cards as a means of payment and for other purposes permitted by law.

Consequently, several applications (apps) that provide digital accounts associated to prepaid payment cards have appeared in recent years, which allow individuals to deposit funds in such accounts in order to use them via their associated prepaid payment cards to acquire goods or services or fulfil other payment obligations.

Furthermore, the chapter states that issuers may establish payment schemes using the cards they issue to facilitate fund transfers between their own cardholders or CPF. These operations may be initiated by the cardholder or by a third party specially authorised by the cardholder, and will be executed through corresponding debits and credits within CPF, without needing to comply with the rules and affiliation schemes applicable to affiliated entities. The aforementioned schemes do not preclude the respective cards from being used for other purposes inherent to this payment method.

Finally, with the enactment of the Fintech Law, the commercialisation of the custody of financial instruments (such as crypto assets) is now regulated as a fintech service in Chile. In this respect, Article 2 of the Fintech Law defines financial instruments as any security, contract, document or incorporeal good, designed, used or structured for the purpose of generating monetary income, or representing an outstanding debt or a virtual financial asset (also called 'crypto assets' in the Law). Accordingly, fintech services concerning the custody of virtual financial assets or crypto assets is currently regulated in Chile.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

In Chile there is currently no regulatory sandbox programme, innovation hub or accelerator programme promoted by any regulatory entity that promotes innovations in the fintech ecosystem.

However, we can mention several state initiatives that aim to promote different types of enterprises such as, for example, the entrepreneurship programmes of the Corporation for the Promotion of Production (CORFO); a public business accelerator called Start-up Chile, which promotes technological ventures under the umbrella of CORFO and the Chilean Government, among other initiatives which coach and provide financing to entrepreneurs in various fields, including the fintech area, so that they can start, develop, and scale their business ideas and plans.

Also, concerning the Fintech environment, the Association of Fintech Companies of Chile (FinteChile), a private association, aims to represent and promote the growth of the Fintech industry in Chile. For this purpose, it has four key pillars:

- active participation in the design of public policies and regulation;
- development and attraction of talent to the industry;

- attraction of greater quantity and quality of investment to the industry; and
- massification of the use of fintech services.

One of the most recent manifestations of its active participation in regulation can be found in the Framework Agreement for data capture entered into with the banking entities part of the Association of Banks and Financial Institutions of Chile A.G. (*Asociación de Bancos e Instituciones Financieras* or ABIF) and BancoEstado, for the purpose of establishing standards of responsibility and mechanisms for capturing customer data from the institutions that adhere to the Framework Agreement in a controlled manner via web scraping (extraction of information from websites) while other capture mechanisms are established and, without prejudice, to future regulations that may be issued in this regard.

Lastly, in 2023 the CMF established a Financial Innovation Centre whose objective is to create a bridge between the CMF and the private sector, enabling a communication channel between the regulator and the fintechs under supervision. Among its main tasks are guiding companies interested in conducting fintech activities in Chile and receiving/responding to their enquiries.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

As previously mentioned, the Fintech Law regulates an open finance system which allows the exchange of information between different institutions, regarding financial customers who have expressly consented to it and other types of data set forth in the Law, through APIs that enable an interconnection and direct communication between the participating institutions, allowing the provision of new financial services.

Also regarding the open finance system, NCG No 514 regulates the:

- perimeter;
- operation;
- security and safeguards;
- information;
- sanctions; and
- terms to implement it.

Finally, as mentioned in the previous question, there is currently a Framework Agreement for data capture via web scraping between the banking companies' members of ABIF and Banco Estado, and the companies associated with FinteChile. This agreement regulates the standards of responsibility and the mechanisms for capturing data from the clients of the institutions to adhere to certain legal and best practice standards. This Framework Agreement must be complemented by bilateral contracts entered into by the interested parties, which specify the conditions under which the data capture would operate.

Colombia

Natalia Escobar
Posse Herrera Ruiz, Bogotá
natalia.escobar@phrlegal.com

Julián Aguirre
Posse Herrera Ruiz, Bogotá
julian.aguirre@phrlegal.com

Introduction

Deepening access to financial services through the application of information technologies is the public policy goal that has guided the development of fintech activities in Colombia in its different spheres, including digital payments, digital loans, asset management, personal finance and crowdfunding.

To this end, Colombia has adopted a functional equivalence between digital and analogue finance, and the principle of technological neutrality to facilitate the creation of channels associated with electronic payments, credit origination, disbursement, and digital management of savings and investment, promoting competition among relevant agents.

During the last two decades, the Colombian government has established public policy goals and issued rules covering the rendering of payment, deposit and lending services by financial institutions and non-regulated entities while striving to maintain financial stability, access to credit and a level playing field for financial consumers and their protection.

Currently, and as a reflection of a challenging macroeconomic environment, the discussion on the legal segmentation between regulated financial institutions (financial institutions in a broad sense) and non-regulated entities that compete in the financial services market (mainly loans, payments and asset management) has become livelier, specifically due to: (1) the funding costs of lending activities and their relationship with the regulatory burden on financial institutions, which derives from the constitutional standard that all activities related to the management, use and investment of resources collected from the public must be subject to prior state licensing; and (2) the pressure of the financial risk management models that restricts the capacity of financial institutions to deepen their credit offer to segments that become more expensive due to their higher levels of credit risk.

On the other hand, Colombia has segmented the payments and wire transfer market, allowing non-regulated agents to participate in several steps of the value chain of such demand, including the acquiring activity itself. However, in practice, financial institutions are still predominant in this process, mainly due to the restriction for those who do not have this status to directly manage deposit accounts for the clearing and settlement of payment transactions within low-value payment systems.

Regarding asset management, the Colombian market continues to be mainly intermediated and shallow. Although the use of information technologies has permeated this market, its primary manifestation has been more on the side of distribution and scaling of self-management mechanisms

for clients than in an increase of market players offering more services. This circumstance is replicated within the insurance market.

Regarding open data strategies applied to financial services, Colombia has recently adopted and is in the process of implementing an open economy model that seeks to encourage the flow of personal data in the economy. The regulatory requirements have focused on privacy protection and computer security in the storage, transfer and transmission of personal data, and the standardisation of technologies and protocols for this purpose. To date, a regulatory project on the latter aspects is in progress.

Finally, Colombia has decided to adopt an agnostic approach to digital assets, seeking to manage the legal effects of their negotiation and possession based on the country's traditional rules of ownership in force. There is no recognition in Colombia of digital assets as a legal tender. However, the regulation has recognised the potential risks involved in this market, especially in terms of money laundering, financing of terrorism, and proliferation of weapons of mass destruction, which has resulted in a phenomenon of 'de-banking' that restricts the supply of financial services associated with the flow of resources to and from the environment of digital assets. Although no comprehensive or unique regulation has been issued for digital assets, the regulatory projects underway follow the international trend of focusing their command-and-control efforts on digital asset service providers.

It is worth mentioning that this regulatory effort is guided by key public policies set forth by the National Council for Economic and Social Policy (CONPES) and the National Policy Plan (*Plan Nacional de Desarrollo*), in the following initiatives:

- The Bank of Opportunities of 2006, a policy to promote access to credit and other financial services aimed at seeking social equity by creating the necessary conditions to facilitate access of the excluded or underserved population to the formal financial system.
- The National Policy for Digital Transformation and Artificial Intelligence of 2019, that guides regulatory changes required to enhance the efficiency and competitiveness of the low-value payment ecosystem.
- The National Policy for Inclusion and Economic and Financial Education of 2020, that seeks to foster digital interactions of citizens with the government and with financial institutions, including laying the groundwork for tools such as 'digital citizenship' and open finance.
- The National Policy Plan of 2023 – the Ministry of Finance and Public Credit, in coordination with other state agencies, will promote the development of instruments and programmes to foster the financial and credit inclusion of the popular economy, minimal producers in the agricultural sector and micro-businesses, the promotion of green finance, innovation, and entrepreneurship. These instruments and programmes will include initiatives that accelerate the modernisation of the financial system, including the promotion of fintech companies regulated by the Financial Superintendency of Colombia (SFC) and the institutional strengthening of the entities that make up the cooperative economic system.
- The National Policy Plan of 2023: with the purpose of promoting competition and innovation for financial and credit inclusion, state agencies that make up the branches of public power and all private legal entities must give access to and provide all information that may be used to facilitate

access to financial products and services, without prejudice to the exceptions to their access and safeguards of confidentiality of the information, provided for in the regulations in force. The government will regulate this initiative by setting forth the rules to safeguard the adequate operation of the scheme, the recipients, and conditions of access to the information, the security, operational and technological standards, and other aspects required to comply to facilitate access to financial products and services. Notwithstanding this article's provisions, personal data processing will be governed by the conditions of Statutory Laws 1712 of 2014, 1266 of 2008, 1581 of 2012, 2157 of 2021, or those that modify or replace them, as well as their regulatory standards.

- The National Policy Plan of 2023: the financial consumer will have the right to request the transfer of financial products from one financial institution to another one, together with the general and transactional information associated to them. For such purpose, the financial consumer must inform the new (recipient) institution its desire of transferring one or more financial products, and the latter must initiate the portability assessment to approve or disapprove such request. If exercising the right to financial portability is approved, it should not generate any type of penalty or additional charge to the consumer. Financial institutions oversee that consumers are able to exercise this right. The government, by means of the Ministry of Finance and Public Credit, will regulate this matter.

1. Fintech regulatory framework: please provide a description of the most relevant laws and regulations on fintech and financial innovation in your country. Please also refer to any new law or regulation foreseen in the near future or any bill on fintech and financial innovation in your jurisdiction.

Colombia has not adopted a specific regulatory framework for fintech. However, there are laws and regulations currently in place, such as the National Policy Plan of 2023, that direct state agencies to implement and enable innovation technology in the financial services industry, which may be classified into four groups, further developed below: (1) e-commerce, (2) personal data, (3) digitalisation of financial products, and (4) regulatory financial innovation tools.

E-commerce, digital contracting and technological infrastructure for providing financial services.

1. *Decree 410 of 1971 (Code of Commerce)*. Provides merchants the possibility of executing agreements by any unequivocal means.

2. *Law 527 of 1999 (E-commerce)*. Defines and regulates the access and use of data messages, electronic commerce (including financial services and products), digital signatures, and certification entities. Sets forth the 'functional equivalency principle' applicable to signatures, written documents and original compositions. Recognises the validity and enforceability of data messages.

3. *Law 1735 of 2014*. Electronic payment and deposit companies (s*ociedades especializadas en depósitos y pagos electrónicos* or SEDPEs) are financial institutions that may (a) receive deposits through simplified savings accounts; (b) make payments and transfers and act as acquirers;

(c) take loans locally or internationally to finance their operation; (d) send and receive money transfers. A SEDPE may not provide loans. This law also enables financial institutions and financial services operators to access personal and biometrical identification data held by the government when required to gain adequate access to financial services (ie, for know your customer (KYC) procedures).

4. *Ley 1273 of 2009*. Amends the Criminal Code to include criminal offences against data and information systems' confidentiality, integrity and availability. These enhanced protections served as an enabling factor for the development of technological innovations, including fintech.

5. *External Circular 029 of 2014*. Issued by the SFC, this reissues the Basic Legal Circular (BLC), a compilation of mandatory regulations issued by the SFC to govern the products, services and institutions that comprise the Colombian financial system. Two chapters are noteworthy for this document:

    a) *SFC's BLC, Part I, Title II, Chapter I*. Instructs financial institutions and other regulated entities on digital transaction security, quality requirements, and standards for customer service through electronic channels.

    b) *SFC's BLC, Part I, Title IV, Chapter V*. Instructs financial institutions and other regulated entities on the minimum requirements for information- and cyber-security risk management.

6. *Decree 1074 of 2015*. Codifies several decrees regarding the commercial, industrial, and tourism sectors, including e-commerce and electronic signatures regulations.

7. *Decree 620 of 2020*. Provides guidelines to foster the access of Colombian citizens to private and public digital services, including financial services.

8. *Decree 338 of 2022*. Strengthens the governance of digital security.

Personal data and consumer protection

1. *Statutory Law 1266 of 2008*. Provides a protection scheme for the right of habeas data and regulates the treatment of personal financial and credit data, as well as personal data sharing within the country and on a cross-border basis.

2. *Law 1581 of 2012*. Provides a general protection for personal data.

3. *Decree 1074 of 2015*. Codifies several decrees regarding the commercial, industrial and tourism sectors, including authorised financing activities developed by non-regulated entities, such as private lenders and factoring. Several fintech business models are based on these activities.

4. *External Circular 10 of 2001*. Issued by the Superintendency of Industry and Commerce (SIC) and also referred to as the Unique External Circular (UEC), this consolidates all mandatory regulations issued by the SIC. It is important to highlight two sections:

    a) *SIC's UEC, Title V*. Provides instructions on data protection and data processing activities applicable to all economic sectors in Colombia.

b) *SIC's UEC, Title VIII.* Provides instructions regarding lending activities by non-regulated entities, including buy now pay later business schemes.

5. *Law 1328 of 2009.* Provides the financial consumer protection scheme that applies to products and services offered by financial institutions to any type of consumer.

6. *Law 1480 of 2011.* Provides a general consumer protection scheme, including rules on e-commerce platforms, electronic payments reversion, and online shopping withdrawal rights.

Digitalisation of financial products

1. *Decree 661 of 2018 (compiled on the Decree 2555 of 2010).*[1] Authorises financial institutions to use technological tools to provide advisory and product recommendations using technical means (eg, robo-advisers).

2. *Decree 1357 of 2018 (compiled on the Decree 2555 of 2010).* Governs collaborative financing (crowdfunding) instruments (both equity and debt) based on electronic infrastructures, which may include interfaces, platforms, internet sites or other electronic communication means, to match contributors and recipients to finance a business initiative.

3. *Decree 222 of 2020 (compiled on the Decree 2555 of 2010).* Regulates simplified savings accounts, electronic savings accounts, and low-amount credit facilities by enabling digital opening, onboarding, and disbursement processes. This decree also allows financial institutions and other regulated entities to enter into agreements with non-regulated agents (ie, correspondents) and broaden the means for providing services to their clients through the correspondent's physical and digital infrastructure.

4. *Decree 1692 of 2020 (compiled on the Decree 2555 of 2010).* Governs low-value payment ecosystems, including acquiring and payment services providers' activities, such as processing, aggregation and access technologies.

5. *Decree 1297 of 2022 (compiled on the Decree 2555 of 2010).* Regulates payment initiation services, open banking, financial services ecosystems (embedded and third-party prompted), open financial architecture and technology infrastructure services provided by financial entities to third parties.

6. *Decree 2443 of 2018 (compiled on the Decree 2555 of 2010).* Enables some financial institutions to invest directly in financial technology innovation companies (FTIC), provided that the FTIC does not conduct any other core activities and refrains from holding equity in other entities. Colombian law and regulations strictly limit local financial institutions' equity investment capacity.

1 Decree 2555 of 2010 codified several decrees governing the finance sector, including financial, securities markets and insurance activities, and the financial institutions and other regulated entities that offer related products and services.

Regulatory financial innovation tools

1. *Law 1955 of 2019, National Development Plan, article 166.* Authorises the SFC to issue temporary financial services licences (up to two years) in a controlled environment (known as a sandbox) to innovative technological developments related to activities reserved for financial institutions and other regulated entities. It also authorises all SFC-supervised institutions to develop and test creative technological activities under similar time conditions.

2. *Decree 1234 of 2020 (compiled on the Decree 2555 of 2010).* Provides the objectives, requirements, and stages of operation of the SFC's controlled financial innovation environment (ie, sandbox) as a tool to promote innovation in financial services and facilitate the identification of new financial developments by government authorities.

3. *External Circular 16 of 2021 (compiled in the SFC's BLC).* Provides further instructions regarding access to the SFC's sandbox.

2. Regulations on crypto assets: please provide a summary of the legal framework of crypto assets in your country and how crypto assets are regulated in your jurisdiction.

Colombia has yet to issue comprehensive regulations on crypto assets. Some initiatives have focused on warning the public about the risks of investing, offering, or facilitating operations over digital assets, including crypto, and reminding financial institutions that they are not authorised to participate in such activities. Furthermore, specific anti-money laundering (AML) provisions have been implemented to address the higher AML-risk profile of crypto assets.

In this vein, the SFC has issued Circular Letters 29 of 2014, 78 of 2016, and 52 of 2017, addressed to the public and financial institutions and other supervised entities, stating that Colombian financial institutions are not allowed to provide custody, invest, intermediate or operate with these instruments, nor can they use their platforms to conduct operations of cash-in or cash-out outside the controlled financial innovation environment. Financial institutions are not authorised to advise on or manage operations with crypto assets. No private or governmental guarantee or deposit insurance scheme is available to invest such assets.

Furthermore, the Board of Directors of the Colombian Central Bank (Banco de la República), the SFC, the Superintendency of Companies, the Financial Regulation Unit, the National Tax and Customs Authority, the Information, the Financial Analysis Unit (UIAF) and the Colombian Accounting Board (as an observing member), have concluded that, under Colombian law and regulation, crypto assets:

1. may not be considered as legal tender: only the currency issued by Banco de la República is legal tender in Colombia.[2] As a result, it is not mandatory to receive crypto assets as a means of payment;

2. if issued abroad, crypto assets may not be considered foreign currency because they are not recognised by any international financial authority or backed by any central bank;

2 *Banco de la República* is planning to issue a digital currency.

3. are not considered securities under Colombian securities law and regulations. Therefore, they may not be referred to or advertised as such; and

4. may not be considered financial assets or investment assets in accounting terms.

Following these conclusions, in Colombia, crypto assets are treated as intangible assets that the public may acquire and sell. Its use is further limited by regulations preventing the massive solicitation of funds from the public and unauthorised cross-border offering of foreign financial services in Colombia.

Moreover, UIAF's Resolution 314 of 2021 mandates that all individuals and entities performing services related to digital assets must file reports and information about their operations, including suspicious transaction reports. Services related to digital assets include, but are not limited to, cash-in or cash-out operations, exchange, transfer, or custody performed on a proprietary basis or as a third-party agent.

Finally, the SFC published a draft regulation for public consultation in July 2022 following the conclusion of a pilot project on the SFC's sandbox on cash in/cash out transactions on virtual/crypto assets exchanges operated by fintech companies in alliance with financial institutions. The draft regulation was not further considered by the SFC, but covered the following issues.

1. Financial institutions must consider the main elements when evaluating a virtual assets service provider (VASP) as a client.

2. Consumer protection measures when financial institutions enter alliances with VASP.

3. Clarifies that the following financial institutions may enter operations involving VASP or virtual/crypto assets:

    - Managing companies of investment funds and private equity funds may include investments in foreign investment funds in the fund's portfolio with virtual/crypto assets as underlying assets.
    - Trust companies may enter trust agreements over virtual/crypto assets, directly or indirectly.
    - Colombian financial institutions may act as distributors or sub-distributors of foreign funds invested directly or indirectly invested in virtual/crypto assets.
    - Offices that represent foreign financial or securities market institutions and local correspondents of foreign securities brokers may promote and advertise financial products structured with virtual/crypto assets.

3. Payment service providers and digital wallets: Please describe how payment service providers and/or digital wallets are regulated in your country. Please mention any foreseen law or regulation in this respect.

Payment service providers

Colombia has regulated the payment services industry under the legal definition of a low-value payment system (LVPS). A payment system is an organised set of policies, rules, agreements,

payment instruments, entities and technological components – such as equipment, software and communication systems – which allow the transfer of funds between system participants by receiving, processing, transmitting, clearing and settlement of payment orders or fund transfers.

To operate, an LVPS requires (1) a low-value payment system managing company (LVPSMC); and (2) at least three or more SFC-supervised institutions and certain cooperatives (subject to requirements) to act as participants.

Access to the LVPS is considered part of the acquiring activity and, as such, may include:

1. connecting merchants to the LVPS;
2. providing merchants with access technologies that enable the use of means of payment (eg, debit and credit cards, QR codes, contactless instrument of payments, cash transfers, etc);
3. process payment orders or transfer of funds initiated through access technologies;
4. aggregating merchants before LVPS; and
5. receiving the proceeds of the sales made by a merchant through the access technologies supplied to it, as well as managing the adjustments that may arise from a process of disputes, returns, claims, or chargebacks and notifying the user of the confirmation or rejection of the payment or transfer order.

The activities referred to in (1), (2), (3) and (4) above may be carried out by the acquirer directly or through the acquirer's contractors called payment service providers (PSPs). Acquiring activity may be carried out by the following types of entities (known in this capacity as 'acquirers'): credit establishments (including banks), SEDPEs and by commercial companies not supervised by the SFC, subject to specific quantitative and qualitative requirements, including inscription in the Unregulated Acquirer Registrar kept by the SFC.

In this vein, PSPs in Colombia are mostly technology service providers for acquirers. Colombian regulations recognise the following types of PSP:

1. *Aggregator*. Acquirer payment service provider that connects merchants to the LVPS. It provides access technologies that allow the use of payment instruments and collects on their behalf the proceeds resulting from the order payment or transfer of funds in the merchant's favour;
2. *Access Technology Supplier*. Provider of payment services of the acquirer that supplies the merchant with access technologies that allow the use of payment instruments in in-person and digital environments;
3. *Acquirer Processor*. Payment service provider of the acquirer that routes orders for payment or transfer of funds to the managing entity of the LVPS; and
4. *Issuer Processor*. Provider of payment services of the issuing entity of a payment means that it transmits the authorisation of a payment order or transfer of funds to the entity administrator of the LVPS.

Digital wallets

Colombian regulations have yet to define digital wallets. However, the market understands digital wallets as instruments or mechanisms that, in association with a deposit account in a financial institution, allow the holder to pay a monetary obligation, transfer funds, or withdraw funds physically or virtually.

Digital wallets are structured in Colombia using 'low mount deposits', a type of digital simplified deposit account available to the public, subject to specific requirements, including a cap of around US$500 on the aggregated value of transactions per month and a US$2,000 maximum account balance threshold.

While receiving funds from the general public is restricted to financial institutions with deposit-taking licences, 'low amount deposits' have enabled partnerships between fintechs and financial institutions to offer banking as a service (BaaS) products. However, in Colombia, it is not possible to provide digital wallets in which a fintech aggregates depositors before the financial institution.

4. Special support to fintechs: does your jurisdiction provide any particular programme supporting the fintech ecosystem, particularly fintech startups (eg regulatory sandboxes, accelerator programmes)? Are such programmes supported by the regulator in your country?

Special programme supporting the fintech ecosystem

The Ministry of Communications and Information Technologies developed the program 'Apps. co' to provide monetary and in-kind financial aid to promote digital transformation digital technologies and strengthen digital innovation.

Sandboxes

As mentioned in Question 1, the SFC hosts a regulatory sandbox known as the Arenera and a controlled financial innovation environment.

The Arenera provides a regulatory framework to conduct tests of technological innovations applied to financial services, the stock market, or insurance services in a controlled and supervised environment. In this space, innovative companies can test new business models, applications, processes or products that have components of innovation in technology that aim to provide a benefit for the financial consumer, facilitate financial inclusion or develop the financial services markets.

The Controlled Financial Innovation Environment is a capacity-building public innovation tool that allows the Colombian government to adjust the regulatory framework to the new market dynamics and promote safe and sustained financial innovation. In this space, innovative companies that intend to implement disruptive technological developments to carry out activities reserved for regulated entities may request a temporary operation certificate, valid for up to two years. Once the temporary certificate lapses, the participant may opt to obtain a full license or to wind down its operation under close oversight by the SFC.

5. Open banking: please advise whether in your jurisdiction there are regulations on open banking. If the response is no, please provide any reference to regulations that may directly or indirectly affect open banking. Please include any foreseen laws and regulations on open banking.

Decree 1297 of 2022, also known as the Open Finance regulation, authorised financial institutions to act as data processors and to commercialise the use, storage, and transmission of their clients' data subject to compliance with Colombia's data protection law and regulations. It also regulated payment initiation activities, setting ground rules for LVPSAC neutrality, such as removing barriers to access by payment initiators and managing conflicts of interest, and a mandate for the SFC to develop applicable security requirements. It also regulated digital ecosystems, including offering third-party services through the financial institutions' distribution channels and offering financial institutions products and services through the technological platforms of third-party providers.

Colombia opted for a regulated standard for developing open financial architecture, and the SFC has a mandate to issue technical standards regarding this scheme. These technical standards were finally issued in February 2024 and are compiled in the External Circular 004/24 of the SFC.

Ecuador

Jesús M. Beltrán
Bustamante Fabara, Quito
jbeltran@bustamantefabara.com

Patricio Santos
Bustamante Fabara, Quito
psantos@bustamentefabara.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

Ecuador recently adopted a legal framework that regulates the provision of technology-based financial services within the country's borders, which is made up of laws, regulations and secondary legislation.

The Fintech Law

At the end of 2022, the Organic Law for the Development, Regulation and Control of Technological Financial Services[1] (the 'Fintech Law'), became effective in the Republic of Ecuador. Its purpose is to regulate 'fintech activities' and to promote innovation, development, adoption and use of new technologies in financial products and services (including financial, securities and insurance markets) to improve financial inclusion, productivity and provide protection to consumers.

The Fintech Law defines Fintech Activities as those related to the development, provision, use or offer of: (1) technological facilities to channel payments; (2) technological financial services; (3) specialised electronic deposit and payment companies; (4) technological services for the securities market; and (5) technological insurance services.

In order to exercise fintech activities in Ecuador, a company must meet certain requirements prescribed by the Fintech Law, such as being duly incorporated or domiciled as a fintech company in Ecuador, having the proper authorisations granted by the regulatory authorities (such as the Superintendence of Banks and the Central Bank of Ecuador) and having as its exclusive business purpose the performance of fintech activities.

Fintech companies are subject to regulations issued by the Financial Policy and Regulation Board (the 'Financial Board') and the Monetary Policy and Regulation Board (the 'Monetary Board'), according to the activities under the purview of each of these regulators. They are also subject to the supervision of the Central Bank of Ecuador (the 'Central Bank'), the Superintendence of Companies, Securities and Insurance ('Superintendence of Companies'), and the Superintendence of Banks ('Superintendence of Banks') or the Superintendence of Popular and Solidarity Economy (SEPS), depending on the type

1 *Ley Orgánica para el Desarrollo, Regulación y Control de los Servicios Financieros Tecnológicos (Ley Fintech)*, published in Supplement of Official Registry No 215. 22 December 2022.

of entity to which the fintech company provides services (if it is a bank, it would fall under the former; if it is a credit cooperative, under the latter).

Among the main features of the Fintech Law is the introduction into the private financial sector of two new categories of entities, namely technological financial services companies and specialised deposit and electronic payments companies, which will be discussed in greater detail in Question 3.

Regulations under the Fintech Law

Ecuador's President, by Executive Decree No 903, issued the implementing regulations to the Fintech Law,[2] which address the approval and supervision of fintech companies, cybersecurity, prevention of money laundering, and charges the Monetary Board and the Financial Board with regulatory authority over fintech companies.

Rules regulating currency, methods and payment systems in Ecuador and the fintech activities of its participants

The Monetary Board, in Resolution No 2023-014-M, issued regulations[3] on methods of payment validly accepted in Ecuador, the National Payments System and regulatory testing environments.

The methods of payment are classified into: (1) physical methods of payment (banknotes, coins, cheques); (2) electronic methods of payment (electronic transfers and credit, debit and prepaid cards); and (3) electronic wallets (online service that allows the channelling of money in real time, using electronic methods of payment, facilitates payments and transfers, and allows sending and receiving financial orders), which is addressed more fully in Question 3.

The National Payments System is made up of the Central Payment System and Auxiliary Payment Systems, each with its own policies, rules, instruments, procedures and services for making funds transfers.

Regulatory testing environments (known as sandboxes) are arrangements by which entities wishing to implement new business models related to technology-based payment systems, structures and services may obtain a temporary operating authorisation for such purposes, subject to prior authorisation from the Central Bank.

Rule regulating technological financial services entities

Through Resolution No F-2023-076, the Financial Board issued regulations[4] governing new types of entities under the rubric 'technological financial services entities'. These entities include (1) 'digital credit granting entities', (2) 'neobanks' and (3) entities that provide personal finance and financial advice through electronic platforms or other digital means.

---

2 *Reglamento a la Ley Orgánica para el Desarrollo, Regulación y Control de los Servicios Financieros Tecnológicos (Ley Fintech)*, published in Supplement of Official Registry No 436, 14 November 2023.

3 *Norma que regula la Moneda, los Medios y Sistemas de Pago en Ecuador y las Actividades Fintech de sus Partícipes*, published in Official Registry No 378, 21 August 2023.

4 *Norma que regula las Entidades de Servicios Financieros Tecnológicos*, published in Second Supplement of Official Registry No 402, 22 September 2023.

The regulation establishes the conditions for the provision of services under its scope, such as minimum capital requirements, the operations such entities may undertake, requirements for the establishment of provisions, risk management, etc. The regulation further provides that these entities must comply with money laundering regulations and have a compliance officer.

This regulation addresses in particular digital credit granting entities (using the acronym 'ECDCs') – the only technological financial service entities that currently operate in the Ecuadorian market – which it defines as technological financial services entities that offer credit products exclusively through electronic platforms, automated processes, and largely by the use of digital technologies. These entities are authorised to undertake publicity of credit products, evaluation of the customer's risk profile, and approval and disbursement of loans, but may not capture resources from the public for intermediation purposes. Neobanks, by contrast, may undertake the full scope of banking activities contemplated under Ecuadorian law, including the capture of deposits from the public.

In addition, the Financial Board issued Resolution No F-2024-0109, which regulates specialised electronic deposits and payments companies,[5] setting forth requirements for their incorporation and authorisation to operate.

Crowdfunding

The Organic Law of Entrepreneurship and Innovation[6] (LOEI) regulates collaborative fund platforms or crowdfunding. The LOEI classifies collaborative fund platforms into five categories in accordance with their purpose: (1) donation, (2) reward, (3) pre-purchase, (4) equity investment and (5) reimbursable financing.

The LOEI provides that, in order to develop activities through crowdfunding platforms, the following requirements must be met:

- the activity must be carried out by a legal entity that is under the supervision of the Superintendence of Companies;
- the legal entity's business purpose must only be acting as an intermediary, through internet platforms, between promoters (who require capital for a given project) and investors (who are interested in contributing their resources to the achievement of such projects);
- the entity must have a URL for the crowdfunding platform's website and institutional e-mail address for electronic notifications; and
- the use of the platform must be subject to terms and conditions and a data privacy policy, both of which must be available on the platform's website.

According to LOEI, crowdfunding platforms should adopt procedures that allow projects to be classified based on an objective analysis of the information provided by the promoters. Thus, these procedures should consider relevant project information related to their sector, purpose and/or location, among others, using homogeneous and non-discriminatory analysis criteria.

5 *Norma que regula a las Sociedades Especializadas de Depósitos y Pagos Electrónicos*, 10 May 2024.

6 *Ley Orgánica de Emprendimiento e Innovación*, published in Supplement of Official Registry No 151. 28 February 2020.

In addition, the LOEI requires that all fundraising for crowdfunding projects be executed through institutions of the financial system, and imposes a limit of 1,000 Unified Basic Wages (UBW, approximately US$460,000 in 2024) on the funds that may be raised through a crowdfunding platform for any given project.

2. Regulations on crypto assets: a summary of the legal framework of crypto assets and how they are regulated.

There is currently no specific law or regulation in force in Ecuador governing the operation of cryptocurrencies or crypto assets.

The Organic Monetary and Financial Code[7] (the 'Monetary and Financial Code') establishes the United States dollar as the legal currency of Ecuador. Accordingly, the US dollar is the only legal method of payment and the currency in which all transactions, monetary and financial operations, and their accounting records must be denominated. The Monetary and Financial Code bans (1) making, copying, faking or partly or wholly mimicking money and currency, and also putting any other currency into circulation in any way, medium or form; and (2) circulating and accepting money and currency that are not authorised. Thus, cryptocurrencies are not recognised as an authorised method of payment in Ecuador.

While the use of cryptocurrencies as a means of payment is prohibited, Ecuadorian law does not prohibit the purchase, sale or ownership of cryptocurrencies, nor does it regulate it nor supervise it in any way. Thus, while cryptocurrencies may not be used to pay for goods and services in Ecuador, they may be purchased, held and sold like any other asset, with the understanding that such activities entail risks which Ecuadorian law does not specifically address.

However, for anti-money laundering purposes, parties that engage in the transfer, custody or management of 'virtual assets' (which are not defined under the law but presumably include cryptocurrencies), that provide or engage in financial or other services with respect to virtual assets, or that engage in the exchange of virtual assets for legal currency or for other virtual assets, must designate a compliance officer and submit reports to the Financial and Economic Analysis Unit for anti-money laundering purposes.[8]

Finally, there are no specific regulations, nor has the Ecuadorian Internal Revenue Services issued any relevant guidance, on the tax treatment of gains derived from the sale of cryptocurrencies. Nonetheless, profits obtained from the sale of cryptocurrencies would be subject to income tax. However, the lack of specificity and clarity afforded by the law on how and when gains from the sale of cryptocurrencies should be reported and calculated makes compliance and monitoring difficult.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

The Monetary and Financial Code regulates all financial services, including the National Payments System, which encompasses the set of policies, standards, instruments, procedures and services

7 *Código Orgánico Monetario y Financiero*, published in Official Registry No 332. 12 September 2014.

8 Unidad de Análisis Financiero (UAFE), Resolution No UAFE-DG-2022-0131, published in Supplement of Official Registry No 48, 22 April 2022.

through which the transfer of funds is carried out, transfers of resources managed through methods of payment, and the settlement of transactions among participants in the system.

The National Payments System consists of (1) the Central Payments System, which is administered by the Central Bank, for the transfer of funds and the clearing and settlement transactions among its participants; the requirements and conditions for access to this system are established by the Monetary Board; and (2) Auxiliary Payment Systems, which are private or public systems authorised by the Central Bank, established for the transfer of funds, remittances of money or compensation among its participants; the Monetary Board regulates the operational, governance, risk-control and financial requirements that Auxiliary Payment Systems must comply with.

Since the entry into force of the Fintech Law, the Ecuadorian legal framework regulating collection and payment services and electronic wallets has undergone significant modifications, supplemented by regulations issued by the Financial Board and the Monetary Board that regulate the scope and requirements for the development and delivery of these services.

The Fintech Law introduced two new categories of entities to the private financial sector:

- **Technological financial services entities**: these are entities that develop financial activities centred on digital and electronic technology or that carry out activities that represent financial risk as determined by the Financial Board; unless their activities relate to the payment system, which is regulated by the Monetary Board and supervised by the Central Bank. Technological financial services entities include (1) digital credit granting entities; (2) neobanks; (3) entities that provide personal-finance and financial advice; and (4) other entities determined by the Financial Board; and
- **Specialised deposit and electronic payment companies (SEDPES)**. These are entities whose sole purpose is the receipt of funds for the exclusive purposes of facilitating payments and transfers of funds through authorised electronic methods of payment, as well as sending and receiving financial orders.

Technological financial services entities and SEDPES must be incorporated as *sociedades anónimas* (limited companies) under the purview of the Companies Law of Ecuador and their business purpose must be exclusively the performance of fintech activities.

In order for these entities to provide services, they must be authorised to do so by the Superintendence of Banks and the Central Bank, which will establish the requirements for their authorisation, supervision and monitoring based on differentiated criteria according to the financial and technological risks generated by each entity.

With respect to methods of payment, the Fintech Law establishes that these consist of cheques, electronic wallets and electronic methods of payment, encompassing transfers for payment or collection; credit, debit, prepaid, rechargeable or non-rechargeable cards; electronic wallets with the category of fully digital banking that comply with requirements for liquidity funds, reserves and deposit insurance, and other methods of payment centred on technology, all of which must operate under licence from the Superintendence of Banks or Central Bank and subject to regulations issued by the Monetary Board.

The Monetary Board issued Resolution No 2023-014-M (the 'Fintech Rule'),[9] which determines the authorised methods of payment that can be used by the different economic agents within the financial environment and classifies them into: (1) physical methods of payment; (2) electronic methods of payment; and (3) electronic wallets.

Physical methods of payment consist of bills, coins and cheques, while electronic methods of payment are:

- electronic money transfers to make payments;
- electronic money transfers to make collections;
- credit cards;
- debit cards; and
- prepaid cards.

All these methods of payment must be operated by:

- the Central Bank;
- by the entities of the national financial system; or
- by entities that participate in the Auxiliary Payment System.

All transactions made with electronic methods of payment will be settled and, if applicable, cleared at the Central Bank.

Electronic wallets are defined as a method of payment that, through an electronic device or online service, allows the channelling of money in real time through electronic means to facilitate payments and transfers, and that allows for the delivery and receipt of financial drafts. Electronic wallets must be operated exclusively by:

- specialised deposit and electronic payment companies;
- financial entities only to facilitate transactions of their clients or partners; and
- by financial services payment auxiliary companies that have permission to manage and operate electronic wallets.

The Fintech Rule regulates Auxiliary Payment Systems, determining who may act as a participant in this system, among which are:

- financial entities;
- entities of auxiliary services of the financial system (authorised to provide transactional services, payment and network services, automated teller machines and credit-card administration);
- technological financial services such as neobanks;

9 *Norma que regula la Moneda, los Medios y Sistemas de Pago en Ecuador y las Actividades Fintech de sus Partícipes*, published in Official Registry No 378, 21 August 2023.

- specialised deposit and electronic payment companies; and
- administrators of Auxiliary Payment Systems.

The services that may be provided by the participants of the Auxiliary Payment Systems, after authorisation by the Central Bank, are:

- payment aggregation;
- payment initiation;
- payment gateway;
- administration and operation of electronic wallets;
- transactional switch for payment services; and
- money remittances.

Entities wishing to be considered as participants in the Auxiliary Payment Systems must qualify and be registered with the Central Bank and must request authorisation from the Central Bank for each service they offer. Resolution No GG-018-2023[10] of the Central Bank regulates the registration, qualification and authorisation of the services provided by Auxiliary Payment Systems participants.

With respect to SEDPES, the Fintech Rule establishes that only electronic methods of payment expressly authorised by the Central Bank may operate. These companies must open and maintain individual and identifiable electronic payment accounts for each client or user of electronic wallets. SEDPES may provide the following services:

- receiving monetary resources in electronic payment accounts, through deposits, transfers or receipt of payments;
- making payments, transfers and withdrawals;
- sending and receiving financial drafts;
- receiving remittances from abroad; and
- channelling the payment of public services and in general payments to the public sector.

Resolution No SB-2023-02416[11] of the Superintendence of Banks regulates the authorisation and operation of specialised electronic deposit and payment companies.

---

10 *Norma para la vigilancia de partícipes de sistemas auxiliares de pago*, published in Supplement of Official Registry No 417, 16 October 2023.

11 *Norma de calificación, supervisión y control para las entidades de servicios financieros tecnológicos; y de la emisión de licencia para el ejercicio de las actividades Fintech de las Sociedades Especializadas de Depósitos y Pagos Electrónicos*, dated 21 November 2023.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

Among the innovations in financial regulation introduced by the Fintech Law are regulatory testing environments (referred to as regulatory sandboxes). These are customised regulatory frameworks to be developed by the Superintendence of Banks or the Central Bank (within the scope of their competencies), to enable new businesses to develop novel models for the provision of technological financial services and technology-based payment services. The testing period of a regulatory sandbox may last up to 24 months.

Any company that is authorised to operate in a regulatory sandbox will be allowed to develop its services under the supervision and control of the competent regulator. To apply for such authorisation, the applicant must submit the following documents: (1) a structured business plan justifying that the project entails a new business model; (2) measures to be adopted for the protection of customers, according to the venture's risk level; (3) a plan for the cessation of operations; (4) a proposal of policies for the analysis and management of the risks of the products to be tested; and (5) a plan for an orderly exit from the temporary regulatory test environment, which provides for the mitigation of possible risks that may affect the other products or services offered by the entity and its customers.

In addition, the Central Bank has established an Inter-Institutional Committee on Payments, with the objective of coordinating the implementation of public policies relating to auxiliary payment systems and to address issues raised by participants in such systems.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

The Fintech Law[12] provides that the Financial Board must establish the conditions for the private financial system to provide open banking services, publishing application interfaces (APIs) for validation of account information to facilitate interoperability with fintech companies.

Accordingly, the Fintech Rule provides that the entities participating in Auxiliary Payment Systems must implement interoperability between their platforms and the other existing platforms in the payment system, complying with the rules and technical standards issued by the Central Bank for such purpose. Through such interoperability, a payment infrastructure or service will allow its users to transfer funds to any other user, regardless of the entity or infrastructure providing the payment services.

The Monetary Board has conducted a public consultation on the draft of Interoperability Standard on Immediate Low Value Payment Systems, requesting comments on the draft regulation. However, to date the Monetary Board has not issued any final regulations in this respect.

12 Second Transition Provisional of the Fintech Law.

Guyana

Shivani Lalaram
Dentons Delany, Georgetown
shivani.lalaram@dentons.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

Guyana currently does not have any laws and regulations specifically for financial technology.

The Bank of Guyana has a regulatory and supervisory role in the financial sector in Guyana. It regulates and supervises financial institutions including all commercial banks, finance companies, trust companies, merchant banks, money transfer agents (including licensed cross-border remittance service providers), currency exchange services and insurance companies.

In March 2018, the Bank of Guyana, in association with the World Bank, published the National Payments Development Vision and Implementation Plan (the Plan). This was the first step in the modernisation of the finance industry in Guyana. In accordance with the Plan, the vision is to:

> 'Build a robust, safe, sound, efficient and inclusive National Payment System (NPS) that meets the current and future needs of the economy, supports financial activity and financial sector development, advances the use of electronic payments, contributes to financial risk mitigation, achieves compatibility with international systems, adheres to the relevant international standards, guidelines and codes.'

As a consequence of this Plan, the National Payment Systems Act, Act No 13 of 2019 (NPSA) was created to modernise and regulate the payment systems in Guyana. The Act created a framework to allow the use of electronic money through various mediums, including:

- point of sale transfer;
- automated teller machines (ATMs);
- transfers initiated by telephonic instruments, including mobile phones;
- transactions through the internet and other communications channels; and
- credit card and debit card transfers.

The Act allows these services, in both financial institutions and non-financial institutions, as long as they are licensed.

The Bank, in order to grant licences, must consider in accordance:

- if the entity is registered under the Companies Act, Cap: 89:01 as a company;
- has the prescribed paid-up capital and capital adequacy requirement;

- has suitable and sufficient technical and organisational skills to provide a payment service, including the proper mechanisms to achieve internal control and risk management as related to the provisions of service;
- has a mechanism to safeguard funds which have been received from consumers of a payment service or through another payment service provider for the execution of payment transactions, by not making them commingled at any time with its own funds or the funds of third parties and making them insulated against the claims of the other creditors of the payment service provider in the event of insolvency;
- has a detailed strategy and business plan supported by realistic estimations in the budget forecast for five years;
- is fit and proper, and every officer is a fit and proper person;
- guarantees liquidity of settlement of orders accepted by the system and that this liquidity is protected from credit risk;
- being granted the licence is consistent with the protection of the financial stability and is in the interest of the public; and
- satisfies any other condition the bank considers necessary.

Additionally, there are regulations in place pursuant to the act regarding the agents, electronic funds transfer, and electronic money. These regulations require the registration of the customer with the entity and make provisions for the regulation for each service.

Fintech is now being further advanced outside of this Act and the aforementioned regulations, albeit at a slower pace than the NPSA. For example, the Anti-Money Laundering and Countering Financial Terrorism (Amendment) Act 2023, amended the definition of 'currency' to include cryptocurrency. Furthermore, the Guyana Compliance Commission Act, No 14 of 2023 makes provisions for licensing for the use of virtual assets, however it is subject to licensing which may only occur at the end of the year 2025.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto-assets and how are they regulated.

There is no law which specifically regulates crypto assets in Guyana. Crypto assets have only recently been mentioned in statutes in Guyana, per question 1 above.

The Guyana Compliance Commission Act No 14 of 2023 alludes to the use of cryptocurrency in non-financial institutions. Nevertheless, crypto assets are new in Guyana and currently Guyana does not have the infrastructure to support its use. As a result, the act has given a timeline for the usage.

There are no other statutes or regulations pertaining to this.

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

Payment service providers and/or digital wallets are regulated by the National Payment Systems Act, Act No 13 of 2019 and the regulations that follow the Act as mentioned in Question 1. The primary regulation is that the entity must be granted a licence by the Bank of Guyana, having satisfied the aforementioned requirements.

Additionally, under the regulations, they must have a record/register of the customer that is utilising the service. All other requirements and regulations that must be followed are described in Question 1.

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

The World Bank has offered support to the Bank of Guyana on the National Payments Systems Development Vision and Implementation Plan. In the Plan they have indicated that the vision is to be in conformity with international payment systems by 2030.

There has been no mention of any regulatory sandbox or accelerator programmes for further fintech support.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

There are no regulations regarding open banking in Guyana. Currently, the Bank of Guyana is the only financial entity that owns and operates the nation's interbank payments system infrastructure, the National Cheque Clearing House (NCCH). Entities can utilise this on payment of a fee.

The Data Protection Act, Act No 18 of 2023 may affect regulations as the Act deals specifically with the protection of processing personal data. Liability is attached if consent is not given for the data to be used, processed, or published by another processor. This enactment therefore may have some impact on open banking regulations.

Paraguay

Martín Carlevaro*
BKM/Berkemeyer, Asunción
Martin.Carlevaro@berke.com.py

Pedro Lacasa†
BKM/Berkemeyer, Asunción
Pedro.Lacasa@berke.com.py

1. Fintech regulatory framework: please provide a description of the most relevant laws and regulations on fintech and financial innovation in your country. Please also refer to any new law or regulation foreseen in the near future or any bill on fintech and financial innovation in your jurisdiction.

In Paraguay, there is not a specific regulation for fintech companies or enterprises (whether law or regulation such as a Regulatory Decree, Resolutions of the Central Bank, etc). However, Paraguay possesses a legal framework that relates to financial innovation and indirectly addresses technology applied in finance as follows:

1. Regulations on Electronic Transactions:
    a) Law 6822/2021 on Electronic Transactions Services and Electronic Documents
    b) Regulatory Decree 7576/2022 of Law 6822/2021 (3 August 2022).
2. Regulations on the Paraguayan Payment System (SIPAP):
    a) Law 4595/2012 on Payment and Securities Settlement Systems.
    b) Rules on the Paraguayan Payment System (adopted by Resolution 1 of the Central Bank – 17 May 2022).
3. Other regulations with impact on financial technology:
    a) Law 6534/2020 on Credit Data Protection Regulation.
    b) Rules on Cloud Computing Services (approved by Resolution 10, 28 July 2022).

* Martín is the Head of BKM/Berkemeyer's Project Finance, Infrastructure and PPP's practice. He has advised local and international companies and banks in major infrastructure projects and local business financial regulation.
† Pedro is an associate of BKM/Berkemeyer's Project Finance, Public Procurement and PPP's practice. He has advised local and international companies in local financial regulation and public procurement issues.

2. Regulations on crypto assets: please provide a summary of the legal framework of crypto assets in your country and how crypto assets are regulated in your jurisdiction.

In Paraguay's legal order, there is no current legal definition on digital assets (including crypto assets such as crypto currencies or NFTs).

However, there was a Bill presented before Parliament in 2021, which aimed to regulate crypto mining activities and crypto assets-based activities, which was sanctioned by Parliament in July 2022 but vetoed afterwards by the Executive Branch (29 August 2022). The Bill was later rejected by both chambers of Senators and Deputies.

Regardless, Paraguayan authorities have issued certain specific regulations concerning crypto asset activities.

1. Secretariat for the Prevention of Money or Property Laundering (SEPRELAD):

    a) Resolution 314 (1 September 2021) which approves the Rules on AML and CMT for Legal and Natural Persons established or domiciliated in Paraguayan ground that perform activities related to virtual assets.

    b) Resolution 008 (15 January 2020) which determines that legal and natural persons performing activities related to virtual assets are entities bound by the obligations of due diligence in their operations and information provision to the domestic AML authority (and others contained in Law 1015/1997).

    c) Resolution 009 (25 January 2020) which urges the entities bound by the obligations established in Law 1015/1997 (Anti-Money Laundering Act) to take on due diligence processes regarding legal and natural persons related with virtual asset activities.

2. (Paraguayan) Central Bank:

    a) Statement on virtual currencies of 31 May 2019[1] and 19 September 2020.[2]

3. Payment service providers and digital wallets: please describe how payment service providers and/or digital wallets are regulated in your country. Please mention any foreseen law or regulation in this respect.

In Paraguay there is not a specific regulation on payment service providers, but there are many regulations on digital wallets (*billeteras electrónicas*):

- Guidelines on Electronic Means of Payment, adopted by Resolution 6 of the Central Bank (13 March 2014) as modified by Resolution 6 of the Central Bank (16 April 2020);
- Guidelines on Information Provided by Electronic Payment Entities adopted by Resolution 10 of the Central Bank (31 January 2019); and

1 https://bcp.gov.py/comunicado-del-bcp-sobre-monedas-virtuales-o-criptomonedas-n1153.

2 www.bcp.gov.py/comunicado-sobre-monedas-virtuales-o-criptomonedas-n1381.

- Anti-Money Laundering/Combating the Financing of Terrorism Guidelines for Electronic Payment Entities adopted by Resolution 77 of the Secretariat for the Prevention of Money or Property Laundering (SEPRELAD) (6 March 2020).

4. Special support to fintechs: does your jurisdiction provide any special programmes supporting the fintech ecosystem, in particular fintech startups (eg, regulatory sandboxes, accelerator programmes). Are such programmes supported by the regulator in your country?

In Paraguay there are no special programmes supporting the fintech ecosystem (startup support, regulatory sandbox or accelerator programmes).

However, there is a regional desire to enhance digitalisation within the member countries of MERCOSUR through the Digital Agenda Group (DAG).[3]

At domestic level, the government is focused on the Digital Agenda programme, which aims to improve digital connectivity to strengthen the national digital economy.[4]

Besides the domestic and regional intentions to establish a Digital Agenda which may improve the fintech ecosystem *in totum*, the Central Bank through its academic branch (Instituto del Banco Central del Paraguay)[5] often gives free and public training, lectures and webinars regarding key fintech notions, financial inclusion and digital services in the banking sector, including blockchain technology, crypto assets and CBDC.

5. Open banking: Please advise whether in your jurisdiction there are regulations on open banking. If the response is no, please provide any reference to regulations that may directly or indirectly affect open banking. Please include any foreseen laws and regulations on open banking.

In Paraguay there is not a specific regulation on open banking. However, certain financial institutions are starting to use third-party services for analysing their consumer data base via SaaS (Software as Service) businesses through APIs.

3 Established in December 2017 (see www.mercosur.int/temas/agenda-digital/).

4 www.mitic.gov.py/agenda-digital/portada.

5 www.bcp.gov.py/ibcp/inicio.

Peru

Nydia Guevara Villavicencio[1]
Rodrigo, Elías & Medrano Abogados, Lima
nguevara@estudiorodrigo.com

1. Fintech regulatory framework: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

In Peru there are currently no specific regulations for fintechs. Nevertheless, there are certain pieces of regulation that indirectly relate to technology applied to financial services (eg, e-money, payment services providers and quick response (QR) codes) which are detailed in the following answers. In the specific case of financial innovation, we have in place a sandbox regulation applicable to innovation models, as detailed in Question 4.

Notwithstanding the above, the Peruvian Banking, Insurance and Pension Fund Administrator Superintendence (SBS), in a published report, has stated that it seeks to ensure that the regulatory framework applicable to fintechs is:

- comprehensive, covering all relevant risks;
- focused on best risk management practices;
- balanced, so that regulatory requirements are proportional to the scale and complexity of the various institutions that make up the systems;
- dynamic, allowing it to adapt to changes in the economic and financial environment that imply a potential accumulation of risks; and
- prospective, promoting the use of tools so that supervised companies can achieve long-term sustainability.

In July 2023, the Peruvian Congress enacted Law 31814, which promotes the use of artificial intelligence in favour of the economic and social development of Peru. Although there is no specific reference to fintechs in such law, it provides a general framework for the promotion of the use of artificial intelligence, which is, among others, an enabling technology indispensable for facilitating the development of fintech companies and their proper functioning, as has been explained by the SBS in a published report. Currently, the enactment of this law's regulation of is still pending.

2. Regulations on crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

Under the current Peruvian legal framework, there are no specific regulations on virtual currencies nor for crypto assets.

1 Nydia is a partner in the Finance and M&A practice. She specialises in the design, structuring and negotiation of multiple financing transactions including public and private offerings of securities, project finance, syndicated loans, trade finance and derivatives. She also has significant experience in financial and capital markets, regulatory matters and fintech advisory.

Since no specific local regulation exists, SBS and the Superintendence of Securities Market (SMV) have made certain public statements in connection to the collection of funds for the sale of virtual currencies and its offering in Peru, emphasising the risks involved when investing in those instruments. In addition, the Peruvian Central Bank (BCRP) has been upfront on its website and social media regarding the risks involved in dealing with virtual currencies (regarding the lack of support by a central bank or similar institution) and their pronounced value fluctuation.

However, neither the SBS nor the SMV have made an official statement clarifying whether any local regulations are applicable in connection with crypto assets, nor have they expressed interest in regulating those instruments in the near future.

However, there have been recent initiatives by Peruvian congressmen to regulate the marketing and commercialisation of crypto assets. Specifically, in June 2023, the Economics, Banking, Finance and Financial Intelligence Commission of the Peruvian Congress, approved Bill No 1042-2021-CR. This proposes a framework law for the commercialisation of crypto assets, which includes, among others, a registration obligation applicable to all the companies that provide crypto asset exchange services. Having been approved by the abovementioned commission, the Bill will be discussed by Congress in the near future.

By means of Supreme Decree No 006-2023-JUS, Virtual Asset Service Providers (VASP) were incorporated as obliged subjects to provide information to the Peruvian Financial Intelligence Unit, with the purpose of identifying offences of money laundering and terrorist financing. Pursuant to the Decree, VASP comprise any individual or legal entity, domiciled or incorporated in Peru, that is not covered by any other Financial Action Task Force (FATF) Recommendation and that, as a business, engages, for or on behalf of another individual or legal person, in one or more of the activities or transactions described in the Decree, all of them related to the provision of services related to virtual assets (such as exchange, transfer, custody, among others).

3. Payment service providers and digital wallets: a summary of regulations applying to payment service providers and/or digital wallets.

Payment service providers

In Peru, the Payment Systems and Securities Settlement Act, Law No 29440 (Payment Systems Law) and the Regulations of the Payment Systems (Payment System Regulations), enacted by the BCRP by means of Circular No 012-2010-BCRP, set forth the legal framework for payment systems and payment agreements that involve systemic relevance under BCRP's view (eg, payment systems between financial institutions and banks; payment agreements among electronic money issuers, etc).[2]

2 A payment agreement is defined as an agreement to transfer funds between participants, in which at least three parties are involved and one of them is a Peruvian financial system entity; it needs BCRP acknowledgment as such. On the other hand, a payment system is defined as a payment agreement with 'systemic relevance', and is, therefore, subject to the supervision of the BCRP. The BCRP has acknowledged as Payment Systems of Peru: (1) the LBTR system (*Sistema de Liquidación Bruta en Tiempo Real*) for interbank payments; (2) the CCE system (*Sistema para la compensación y liquidación de cheques y otros instrumentos compensables*); (3) the SLMV system (*Sistema de liquidación multibancaria de valores*); and (4) the SLV-BCRP system (*Sistema de Liquidación de Valores* BCRP). Additionally, BCRP has acknowledged ADPE as a payment agreement (*Acuerdo de Pago de Dinero Electrónico*), an agreement for the transfer and settlement of digital currency entered into by financial institutions, a digital currency issuer and Peruvian telecom companies.

These regulations also include a definition of payment services providers (PSPs) as any legal entity that offers payment services to transfer funds through a variety of means, including payment cards, digital wallets, and payments through mobile devices and the internet.

The BCRP does not demand a specific licence to act as a PSP. Nevertheless, pursuant to the Payment Systems Law, PSPs shall comply with the remittance of certain information annually to the BCRP. This includes:

- an annual questionnaire supplied by the BCRP;
- its annual report;
- the identity of the entities with whom it has entered into agreements as participant or entities that provide IT services;
- operational internal regulations and risk management policies; and
- monthly information in relation to the amounts and volume of their transactions and incident reports.

Furthermore, in October 2022, the BCRP published Circular No 0024-2022-BCRP which approves the Regulation on Interoperability of Payment Services Provided by Payment Providers, Agreements and Systems (Interoperability Regulations). By means of these regulations, the conditions and opportunities for the interoperability of certain payment services (mainly, digital wallets) provided by specific local entities have been set forth.

On another note, the BCRP published Circular No 0003-2020-BCRP (QR BCR Circular), which contains specific regulations for the payment services that are carried out with QR codes. The QR BCR Circular establishes: (1) standards for QR codes used for payments in Peru; and (2) regulatory requirements for payment services that are carried out with QR codes. This includes within its scope the providers of QR codes, the providers of digital wallets, and the payment networks that participate in such service.

Digital wallets

The provision of digital wallet services in Peru is mainly framed under the local e-money regulations. Pursuant to Peruvian law,[3] e-money is a representation of the local fiat currency that creates a credit in favour of its holder against the issuer of the e-money (ie, the company providing the e-money services, which is called *empresa de dinero electrónico* or EDDE). The legal features of e-money are:

- it is stored on an electronic medium. The devices that may be used include cell phones, pre-paid cards, equipment, or electronic devices that comply with the purposes of e-money regulations (this list of characteristics). Electronic wallets are included under this category provided that all features mentioned in this list are met;
- it is accepted as a means of payment by entities or people other than the issuer of the e-money and has cancellation effects;
- it is issued for the same value as the funds received by the issuer of the e-money;

3 See: Act No 26702, Act No 29985, Supreme Decree No 090-2013-EF, SBS Resolution No 6284-2013 and SBS Resolution No 6283-2013, as amended.

- it is convertible into cash according to the monetary value of the holder at nominal value; and
- it does not constitute a deposit and does not generate interest.

Regarding the issuance of e-money, the SBS has established that it includes the transactions of e-money itself, as well as its redemption to cash, transfers, payments, and any transaction related to the monetary value of the user and necessary for the foregoing. In that sense, according to the regulations above, e-money shall have the same value 'in' and the same value 'out'.

EDDEs are regulated entities that are authorised and supervised by the SBS. To perform activities as an EDDE in Peruvian territory, these entities must obtain both an incorporation authorisation and an authorisation to operate from the SBS. In addition, EDDEs have to comply with several legal requirements (including minimum capital levels, the creation of trusts for all funds received for the issuance of e-money to back up the e-money accounts created, limits on the transactions that can be performed depending on the type of e-money account created, and others).

4. Special support to fintechs: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

Despite the lack of specific regulation related to fintechs and financial innovation, Resolution SBS No 02429-2021 – Sandbox Regulations (the Sandbox Regulations) was recently enacted by the SBS, which was effective as of 1 February 2022. The purpose of these regulations is to create an environment for the temporary execution of innovation models by entities already supervised by the SBS, or those that are currently following an authorisation procedure under such entity's guidance/intervention, to improve the activities performed by entities supervised by the SBS.

Pursuant to the Sandbox Regulations, an innovation model is understood as a business or operating model that involves carrying out activities in a fashion different from the traditional way used by companies, and that requires pilot testing, regulatory flexibility or regulatory modifications.

Under the Sandbox Regulations, companies already authorised by the SBS or in the process of obtaining an authorisation from the SBS may carry out pilot testing of innovation models temporarily when they are based in activities already contemplated in current regulations and for which they are authorised by the SBS. Additionally, there are two special regimens of pilot testing innovation models:

- the flexible regime: to test activities linked to innovation models contemplated in current regulation that need temporal flexibility of legal requirements; and
- the extraordinary regime: to test activities linked to innovation models not contemplated in current regulations which are the competence of the SBS.

Any pilot testing must comply with three general requirements:

- a 12-month maximum term, extendable up to 24 months;

- a maximum number of participants (clients or users) which must be justified; and
- have received no objections from the risk committee or equivalent body of the company prior to its realisation, after acquiring knowledge of the risk report associated with the pilot test.

Note that in case of the flexible and extraordinary regime, further requirements must be complied with, such as seeking to improve user experience, having a plan with specific objectives and providing sufficient resources for the pilot testing.

Companies interested in doing pilot testing must file for authorisation before the SBS complying with the requirements set forth in the Sandbox Regulations.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect open banking.

Except for what is explained in the following paragraph, there are currently no specific regulations for open banking.

Nonetheless, a group of Peruvian Congressmen in March 2022 presented Bill No 1584/2021-CR (Bill) to declare the implementation of a public policy that promotes the massification of open banking to be of national interest and public necessity. The Bill is under study and discussion by the Economics, Banking, Finance and Financial Intelligence Commission of the Peruvian Congress.

Regarding this proposal, the SBS presented an institutional opinion suggesting an open finance approach for the Bill instead of an open banking one,[4] since it would be more beneficial in the long run for the users of financial services. Furthermore, it recommended that the BCRP and the Ministry of Economy join the SBS as the authorities participating in designing an open finance strategy.

Moreover, in the INDECOPI Fintech Market Study, the Peruvian National Institute for the Defense of Competition and the Protection of Intellectual Property (INDECOPI) recommended to the SBS and the BCRP that, for the progressive implementation of open banking or open finance, a framework of articulation and participation with the different public and private actors shall be established for the validation and consensus in the setting of standards associated with the protection of personal data, information security, cybersecurity measures, the use of application programming interfaces (APIs) for the exchange of information and payment initiation services, among other elements necessary for its adequate implementation, for the benefit of consumers.

Finally, as mentioned in Question 3, the only specific piece of regulation related directly to open banking is BRCP Circular No 0024-2022, which establishes that specific PSPs offering payment services (mainly digital wallet services) must allow the initiation of payments from any virtual account or bank account, even if such account is opened at a different PSP.

4 The concept of open banking includes the sharing and leveraging of customer data (with their authorisation) by banks with developers and (third party) companies to create applications and services, such as real-time payments and increased financial transparency options for account holders. The open finance concept extends this, since it includes banking and financial institutions, but also reaches out to other institutions (financial services in the broadest sense). The open finance model has greater potential than open banking because, by incorporating more entities, the information sharing and interrelationships that exist make it possible to offer a wider range of products and services to users.

Uruguay

Jean Jacques Bragard
Bragard, Montevideo
jbragard@bragard.com.uy

María Sofía Humaian
Bragard, Montevideo
shumaian@bragard.com.uy

1. Fintech regulatory framework: please provide a description of the most relevant laws and regulations on fintech and financial innovation in your country. Please also refer to any new law or regulation foreseen in the near future or any bill on fintech and financial innovation in your jurisdiction.

Currently, Uruguay continues to position itself as a regional fintech hub. This solution coexists harmoniously with traditional banking and financial institutions, fostering a favourable ecosystem for fintech companies. Tax benefits added to technological talent and the strong bancarisation in the country are some of the main factors which explain the success of fintechs in Uruguay.

The most relevant regulations arose last year, such as Act No 20,038, which established the new regulation of electronic and digital checks; the regulation of the figure of peer-to-peer lending companies and the incorporation of 'Companies managers of crowdfunding platforms' to the regulatory compendium of the securities market.

Within the Recompilation of Regulatory and Control Regulations of the Uruguayan financial system, the Central Bank has regulated 'credit granting entities'. The scope includes those individuals and legal entities that, without being credit management companies or financial services companies, habitually and professionally grant credits with their own resources or with credits granted by certain third parties.[1]

Excluded from this definition are those entities that grant credit to their own personnel, suppliers of goods and non-financial services that grant trade credit and commercial credit to their clients, and social security organisations that grant credit to their members.

The purpose of the regulation is to provide adequate information to consumers, to protect them from abusive practices and to prevent money laundering and the financing of terrorism.

In order to comply with these objectives, requirements have been established in this area that are enforceable on both large and small entities.

These entities may be financed through:

- individuals who are directors or shareholders thereof;
- national or foreign financial intermediation institutions;

1 See www.bcu.gub.uy/Circulares/seggci2411.pdf.

- international credit or development agencies;
- foreign pension funds or investment funds subject to a regulatory authority; and
- any other legal entity of financial activity, financial trust or similar type of assets.

Furthermore, the Superintendence of Financial Services introduced regulatory changes that expand the possibilities for financial system and securities market institutions to implement remote identity validation procedures by digital means.

In this way, new modalities have been introduced, by which institutions may comply with the personal contact required for certain customer segments in the Compilation of Rules for Regulation and Control of the Financial System and in the Compilation of Securities Market Rules.

These modalities are summarised below:

- the use of a process that allows remote verification of the customer's identity, accompanied by certain regulatory requirements; and
- validation of the customer's digital identity or advanced electronic signature, provided by providers within the framework of Act Nbr 18,600, its amendments and regulatory provisions.

Likewise, the advanced electronic signature based on certificates issued by providers accredited before the Unidad de Certificacion Electronica or recognised as equivalent when issued by entities not established in the national territory will be accepted.

2. Regulations on crypto assets: please provide a summary of the legal framework of crypto assets in your country and how crypto assets are regulated in your jurisdiction.

As of the time of writing, the regulation of crypto assets is ongoing. The paper presented by the Central Bank of Uruguay's technological innovation department entitled *Conceptual framework for the regulatory treatment of Virtual Assets in Uruguay* is undergoing parliamentary debate; the preliminary bill was approved by the Chamber of Representatives and is currently being discussed by the Chamber of Senators.

Two other bills related to crypto assets are also being analysed, one of which was proposed by a senator of the ruling party and the other by a senator of one of the opposition parties with similar dispositions.

Uruguay intends to regulate these disruptive technologies, not by creating an entirely new regulation, but by adapting its current law to the ongoing technology.

3. Payment service providers and digital wallets: please describe how payment service providers and/or digital wallets are regulated in your country. Please mention any foreseen law or regulation in this respect.

Principal payments regulation in Uruguay goes under Act Nbr 19,210, the Financial Inclusion Law, and its subsequent amendments and regulatory decrees. It includes as electronic means payment debit cards, credit cards, electronic money instruments and electronic fund transfers, as well as

any other analogous instrument that allows making electronic payments through automatic teller machines, through the internet or other means, as established by the regulations.

The electronic means of payment and the institutions participating in the payment system are regulated by the Central Bank of Uruguay. For such purposes, 'electronic money' is defined as any monetary value enforceable against its issuer, which has the following characteristics:

1. it is stored in electronic media, such as chips, hard discs or servers;
2. it is officially accepted as a mean of payment and has a cancellation effect in relation to the obligations of the issuer;
3. it is issued for a value equal to the funds received by the issuer;
4. it is exchangeable for cash at the holder's request, according to the monetary amount of the unused electronic money instrument issued; and
5. it does not generate interest.

All institutions issuing electronic money in Uruguayan territory must have a corresponding authorisation to carry out this activity.

In addition, regulations state that automatic debit payment services may be provided by (1) financial intermediaries, and (2) electronic money issuing institutions (known as *instituciones emisoras de dinero electrónico* or IEDE).

Finally, within the roadmap of the Uruguayan payment system, the Agenda 2023/2025, some of the main policies are:

- completing the implementation of comprehensive clearing systems with access to the entire regulated industry, 24/7 operation, and with high security standards that are the basis for the development of new products;
- the development of a conceptual framework and proposed roadmap for the issuance of an electronic currency by the Central Bank;
- promote the elaboration of a legal framework and the beginning of the operation of an open finance system; and
- elaborate a proposal for the legal adaptation of the payment system, guaranteeing its soundness, efficiency and accessibility.

In relation to the forthcoming regulation, a public consultation was recently launched, regarding the allowance of interoperability for electronic payment processing regardless of the access channel through which the payment transaction is initiated (point of sale or QR code).

This project establishes the principles, mechanisms and procedures that will govern the interoperability of the different networks of electronic payment processing terminals and the interconnection of their administrators with the different issuers of electronic means of payment and acquirers.

Its approval will create an adequate regulatory framework for the implementation of payments in commercial establishments using QR codes, a milestone that is part of the initiatives aimed at generating a quick payment system.

Finally, it allows interconnection agreements to be freely executed between the parties, subject – of course – to the legal system in force.

4. Special support to fintechs: does your jurisdiction provide any special programme supporting the fintech ecosystem, in particular fintech startups (eg regulatory sandboxes, accelerator programmes). Are such programmes supported by the regulator in your country?

Together with the Uruguayan Fintech Chamber (an association that brings together Uruguayan startups that undertake in the financial ecosystem) and other related private and public entities, the first Fintech South HUB Event took place this year, generating an opportunity to publicise the advantages offered by our country and reflecting the development of the different agents in the public and private sectors.

Likewise, to support fintechs, the Uruguayan Central Bank provides a space for exchange ('nodes'), created with the aim of promoting dialogue on financial innovation issues. In this way, it seeks to facilitate the understanding of the impacts of innovation for regulatory and supervisory purposes, as well as the regulatory framework in which financial innovation takes place. Representatives from the financial and software industries, public agencies and other parties interested in financial innovation participate in these events.

Among the aims of these events are increasing the visibility of the country and its fintech market abroad, and promoting and encouraging open banking in Uruguay.

Along with the public authorities' agenda to provide advantages for entrepreneurship, tax incentives for the software industry and free trade zones, Uruguay also launched a residence permit for foreigners working remotely as freelancers or for companies abroad (so-called 'digital nomads') that seeks to encourage the arrival of more talent from abroad to live and work in the country.

5. Open Banking: Please advise whether in your jurisdiction there are regulations on open banking. If the response is no, please provide any reference to regulations that may directly of indirectly affect open banking. Please include any foreseen laws and regulations on open banking.

Although Uruguay does not yet have a regulation regarding this matter, open banking is foreseen in the 2023–2025 Agenda published by the Central Bank of Uruguay.

In its *Roadmap for the modernisation of the payment system*,[2] it aims to promote the development of a legal framework and initiate the operation of an open finance system.

2 See www.bcu.gub.uy/Sistema-de-Pagos/Documents/Sistema%20de%20Pagos-hoja-de-ruta-2025.pdf.

Venezuela

Arnoldo Troconis*
D'Empaire, Caracas
atroconis@dra.com.ve

Daniel Bustos Novak†
D'Empaire, Caracas
dbustos@dra.com.ve

1. Fintech regulatory framework: please provide a description of the most relevant laws and regulations on fintech and financial innovation in your country. Please also refer to any new law or regulation foreseen in the near future or any bill on fintech and financial innovation in your jurisdiction.

In 2021, the Superintendency of Banks and Other Financial Institutions (Sudeban) issued the Rules Governing the Financial Technology Services of the Banking Sector (Fintech Regulations). These regulations introduce a structured framework for the operation of financial technology entities in Venezuela, particularly those engaging in services aimed at the banking sector.

Under the Fintech Regulations, financial technology institutions in the banking sector (*instituciones de tecnología financiera del sector bancario* or ITFBs) must obtain prior authorisation from Sudeban to provide financial technology services to licensed banks in Venezuela (fintech licence). These services include a wide range of offerings, including payment services, e-wallet features, onboarding, multiplatform banking, risk management, voice recognition solutions and banking as a service (BaaS) solutions.

ITFBs are required to comply with Sudeban's regulations (*Normativa Prudencial*), including Sudeban's anti-money laundering regulations. Moreover, these entities fall under Sudeban's supervision and oversight. Sudeban possesses substantial supervisory authority, allowing them to inspect, monitor, supervise and manage all aspects of ITFBs' operations. This authority extends to the examination of financial records, accounts, files, computer systems, documents, databases, electronic and printed correspondence, and other materials relevant to their operations.

The Fintech Regulations also include provisions governing advertising. Until financial technology companies obtain their licences from Sudeban, they are prohibited from advertising their services in Venezuela.

* Arnoldo specialises in corporate law; technology, media and telecommunications law; and mergers and acquisitions, representing both multinational and Venezuelan companies in the analysis of highly complex regulatory matters related to the implementation of new technology projects in the Venezuelan market.
† Daniel is a lawyer within the technology, media and telecommunications; arbitration; and public law practice groups at D'Empaire. Daniel advises national and international technology, media and telecommunications companies on regulatory issues, content, consumer protection, and data privacy.

In line with the Fintech Regulations, local banks are required to be responsible for monitoring the use of and access to their systems to ensure that unauthorised fintech activities are not offered.

2. Regulations on crypto assets: please provide a summary of the legal framework of crypto assets in your country and how crypto assets are regulated in your jurisdiction.

The regulatory landscape for crypto assets in Venezuela consists primarily of two key components: (1) the Constitutional Decree on the crypto assets integral system, and (2) the regulations established by the Venezuelan crypto asset regulatory agency, Sunacrip (Superintendencia Nacional de Criptoactivos y Actividades Conexas). This regulatory framework encompasses various aspects, including the general operating conditions for crypto asset exchanges, anti-money laundering (AML) regulations, and digital crypto mining regulations.

The Crypto Asset Law was enacted in January 2019 with the goal of providing a regulatory framework for the crypto asset ecosystem in Venezuela. It holds a broad scope, encompassing all goods, services, securities, or activities related to the 'constitution', issuance, 'organisation', operation, and use of crypto assets and sovereign crypto assets in Venezuela. Furthermore, it extends to the purchase, sale, use, distribution, and exchange of any products or services derived from crypto assets and their associated activities.

In 2019, Sunacrip issued the regulations on the operation of crypto asset exchanges (the Crypto Exchange Regulations), aimed at defining the operational rules governing crypto asset exchanges. These regulations establish the parameters for crypto exchanges, which serve as platforms facilitating lawful transactions using crypto assets within secondary markets.

Subsequently, in April 2021, Sunacrip issued the regulations on Anti-Money Laundering and Combat of the Financing of Terrorism (AML/CFT Regulations). The AML/CFT Regulations set out essential guidelines, actions and controls to be implemented by subject entities, with the aim of preventing and mitigating the risk of their operations being exploited for money laundering or terrorist financing purposes. The scope of the AML/CFT Regulations extends to include all individuals, and both public and private entities, engaged in activities involving virtual assets or crypto assets within or originating from the Venezuelan territory.

The crypto asset regulations are relatively recent, with most of them enacted in and after 2019. As a result, several services provided by offshore entities, such as crypto remittance and pool mining remittance services, are incompatible with the Venezuelan crypto asset regulations. Sunacrip has centralised these services within a specific platform under the management of the Venezuelan government.

In March 2023, the President of Venezuela ordered the restructuring of Sunacrip. Initially, the restructuring process was expected to last for a period of six months. However, in September 2023, an extension of the same duration was granted. During this period, the restructuring commission (composed of five members) should prepare (and submit to the President's approval) a restructuring plan that includes the new organisational, management and operational structure of the regulatory entity, the proposed changes to the entity's regulatory framework, and a timetable for the execution of the proposed changes to the entity's structure.

3. Payment service providers and digital wallets: please describe how payment service providers and/or digital wallets are regulated in your country. Please mention any foreseen law or regulation in this respect.

In 2018, the Central Bank of Venezuela issued the General Rules on Payment Systems and Non-banking Payment Services Providers'(PSP Regulations). Under the PSP Regulations, any public or private entity, other than those entities integrated into the payment infrastructures of banking institutions, that provides (or intends to provide) payment services in bolivars (PSP) will need to be authorised by the Central Bank of Venezuela.

Under the provisions of the PSP Regulations, payment services are defined as the execution of transfer orders initiated by customers, involving the debiting of the customer's payment account. Entities authorised by the Central Bank of Venezuela under these Regulations may:

1. open payment accounts, known as cuentas transaccionales;
2. provide customers with payment instruments for their payment transactions;
3. handle the receipt or withdrawal of funds in cash, which involves crediting or debiting payment accounts;
4. execute transfer and payment orders originating from a payment account; and
5. offer money remittance services in bolivars.

The PSP Regulations restrict PSPs to providing services in local currency only. Also, payment accounts offered by a PSP are limited to payment transactions. Such accounts may not accrue interest and are subject to the operating and commission rate restrictions set forth in regulations issued by the Central Bank of Venezuela.

Carrying out payment services activities without the relevant authorisation may constitute an infraction punishable by a fine.

4. Special support to fintechs: does your jurisdiction provide any special programme supporting the fintech ecosystem, in particular fintech startups (eg, regulatory sandboxes, accelerator programmes). Are such programmes supported by the regulator in your country?

There are no special programmes or initiatives tailored to support fintech companies or startups. The Fintech Regulations do not mention any regulatory sandbox, accelerator programme, nor other incentive for fintech innovation. On the contrary, it imposes several requirements and restrictions on ITFBs.

5. Open banking: please advise whether in your jurisdiction there are regulations on open banking. If the response is no, please provide any reference to regulations that may directly or indirectly affect open banking. Please include any foreseen laws and regulations on open banking.

In Venezuela, there is no dedicated open banking framework in place at present. However, open banking activities in the country are subject to regulation through existing legal frameworks.

- The Banking Sector Law prohibits banks and other financial institutions from sharing active and passive operations data with third parties without obtaining explicit consent from users. Unauthorised data sharing is punishable by law, including potential imprisonment.
- Decision No 1318 of the Constitutional Chambers of the Supreme Court outlines guidelines for obtaining user consent to collect and transfer data. These guidelines ensure that data sharing practices adhere to constitutional principles and protect user rights.
- Regulations issued by Sudeban impose restrictions on financial data storage, including geographic limitations.
- The Fintech Regulations include a broad range of activities that can be carried out by ITFBs. These regulations create a framework that could potentially be utilised for open banking purposes.

While Venezuela currently lacks specific open banking regulations, these existing legal provisions and regulations serve as a foundation for governing data sharing and financial technology activities in the country. As the fintech landscape continues to evolve, these regulations may provide a basis for the development of open banking practices within Venezuela.

the global voice of
the legal profession®

International Bar Association

Chancery House, 53–64 Chancery Lane
London WC2A 1QS, United Kingdom
Tel: +44 (0)20 7842 0090
Website: www.ibanet.org