the global voice of
the legal profession®

International Bar Association
Banking Law Committee

Fintech: how is the world shaping the financial innovation industry?

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

5 Chancery Lane

London WC2A 1LG

United Kingdom

www.ibanet.org

Table of contents

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 obtaining a prior approval of the Financial Regulatory Authority (FRA). Other applications/services may be authorised provided said applications/services:

- are suitable for the nature of the financial activity in question;

---

* 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.

- 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 the 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.

On the other hand, although the FRA has issued Decree No 58 of 2022 in connection with the licensing of companies providing fintech, upon inquiry, the FRA has verbally advised that it has not yet issued detailed licensing regulations.

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, the Fintech Law stipulates that companies providing fintech services have a grace period to obtain the FRA fintech licence and comply with the Fintech Law for six months as of the date of issuing the FRA Decree in this respect. FRA Decree No 58 of 2022 was issued 16 March 2022, and the FRA has not issued the detailed requirements.

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

Regarding NBFS companies using financial technology, in order 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;

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.

7 Article 4, Fintech Law.

- 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]

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 many press releases reiterating its warning against trading in all kinds of cryptocurrencies, mainly Bitcoin, due to the extremely high risk associated 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 the answer to 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;

8 Article 5, Fintech Law.

9 Article 206, Banking Law.

- 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 yet issued, the Banking Law stipulates that the PSP or PSO licences may be revoked and the company conducting such activities may be de-registered 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;
- 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;

10 Article 185, Banking Law.

- 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, and 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 regulation 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.

11 CBE circular dated May 2019.

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.

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.

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: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

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 GHS 800,000 to GHS 20m (approximately US$80,000 to US$2m) 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 GHS 30,000 to GHS 84,000 (approximately US$3,000 to US$8,400).

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 the date of creation of the 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 is held in trust and shall not be encumbered in case of insolvency or liquidation. Electronic money issuers are required to keep 100 per cent of the electronic money float in liquid assets.

---

* 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.

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 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.

Fintech companies using digital signatures are required to 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)

This Act imposes a 1.5 per cent electronic transfer levy on electronic transfers above GHS 100 (approximately US$10) on a daily basis. Fintech companies are required to charge the levy at the time of transfer. 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 in order 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 GHS 3,000 (approximately US$300).

In Ghana, the processing of a customer's personal data is necessary for the purpose of a contract, authorised by law, to 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 bureaus where such data relates to details of a loan which is past due by over 90 days.

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 commission of any other unlawful activity. 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.

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 put in place measures to identify politically exposed persons by exercising enhanced identification, verification, and customer due diligence procedures.

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

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.

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 exercise caution 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.

The Anti-Money Laundering Act enacted in 2020 however lists virtual asset service providers as part of accountable institutions. Virtual asset service providers are defined to focus on cryptocurrencies and other digital assets. Thus, crypto assets are subject to the Anti-Money Laundering Act.

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

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 licenses issued by BOG. These are:

- Dedicated electronic money issuer licence: this licence 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 EMV (Europay, Mastercard and Visa) cards. It also allows the PSP to provide inward or international remittances services, merchant acquiring, point-of-sale 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 Question 1. In addition to these laws, where a PSP has foreign shareholders, the PSP must register with the Ghana Investment Promotion Centre and meet the 10 per cent equity participation requirement. 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: a description of special programmes supporting the fintech ecosystem, fintech startups (eg, regulatory sandboxes and accelerator programmes) and regulations regarding special support.

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 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 a specified period, subject to extension. Testing is monitored and evaluated periodically by the sandbox technical team and the applicant exits the sandbox after submission of final testing report.

To facilitate testing, BOG may issue restricted authorisations 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.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect 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 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 inter-operating 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*
ENSafrica, Nairobi
bongonga@ENSafrica.com

Diana Achieng†
ENSafrica, Nairobi
dachieng@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 aims 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.

---

* Belinda is an associate at ENSafrica 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.

† Diana is a lawyer at ENSafrica Kenya specialising in corporate and commercial law. Her experience includes legal research and analysis, risk management, negotiating multinational commercial contracts, out-of-court dispute resolution, employment law and private client management.

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 exempts 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 and 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, whilst '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 require 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 with 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. There are currently no equity crowdfunding regulations in Kenya; however, the CMA may issue a letter confirming that a crowdfunding product/service does not need to be regulated by the CM Act. For instance, the CMA has previously issued a no-objection letter to a company seeking to operate its debt-based crowdfunding platform in the Kenyan market.

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 (MPSPs) 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. 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 a public warning 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.

From a tax perspective, the Kenya Revenue Authority (KRA) introduced a digital service tax (DST) payable on income derived or accrued in Kenya from services offered through a digital marketplace. A digital marketplace is a platform that enables direct interaction between buyers and sellers of goods and services through electronic means. The rate of DST is 1.5 per cent of the gross transaction value (1) in the case of the provision of digital services, the payment received as consideration for the services, and (2) in the case of a digital marketplace, the commission or fee paid to the digital marketplace provider for the use of the platform. Cryptocurrencies may fall within the definition of a digital marketplace as they are electronic platforms that enable users to sell crypto assets to other users. This makes dealings in cryptocurrencies subject to DST.

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 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 Kenyan Senate introduced the Start-up Bill on 14 September 2020 (the Bill). This Bill aims at creating 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*
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'.

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).

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.

---

* 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.

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 24x7 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.

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

Through a guidance note issued in 2018, the FSC indicated that it considers 'cryptocurrency' as a sub-category of virtual assets.

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 ML-TF 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 requirements 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 the VAITOS, holders of the above licences are also subject to a local anti-money laundering and prevention of terrorism financing legal framework, which includes the Financial Intelligence and Anti-Money Laundering Act among others.

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 of the regulatory requirements and 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*
Udo Udoma & Belo-Osagie, Lagos
Yinka.Edu@uubo.org

Joseph Eimunjeze†
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

---

* 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*.

† 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 recognized by the IFLR1000 2022 Nigeria jurisdiction reviews as a Highly Regarded Lawyer in the practice areas of banking & finance and M&A.

payment operator in Nigeria. Furthermore, the CBN subsequently issued the approved new licence 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 organization 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 Nigerian Startup Act

The Nigeria Startup Act was a joint initiative of the Presidency and stakeholders in the Nigerian fintech space. The Act defines a start-up 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, 2022

In 2022, the CBN issued the exposure draft of the Operational Guidelines for Open Banking in Nigeria, 2022 (Open Banking Regulations) to the general public. The Open Banking Regulations, which are yet to be issued by the CBN, seek to regulate, among other things, open banking activities and operations of financial institutions in Nigeria. The regulations will be applicable to banking and other related financial services and service providers as categorised and determined by the CBN.

Service providers covered by the Open Banking Regulations will be required to adhere strictly to certain security standards when accessing and storing data, and will be subject to minimum privacy standards, operational standards, risk management standards and customer experience standards as prescribed by the CBN. It is anticipated that the Open Banking Regulation will, when issued and becoming operational, drive competition and improve accessibility to banking, financial and payments services in Nigeria.

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

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 can be 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 tractions in cryptos.

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 and we have provided a high-level overview of each category and the permissible activities in the table below as stipulated by the CBN.

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, subscription 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 which 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.

In Nigeria, we currently have 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.

South Africa

Bright Tibane*
Bowmans, Johannesburg
bright.tibane@bowmanslaw.com

Kirsten Paulo†
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;
- 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;
- 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

---

* 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.

† 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 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 Conduct of Financial Institutions (CoFI) Bill is anticipated in 2023, which will seek to enable open finance and provide for the licensing of crypto asset service providers (including crypto asset trading platforms).

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.

It is well established (and confirmed by the relevant regulators) that crypto assets are currently not regulated in South Africa. As such, activities in respect of crypto assets are therefore generally not regulated in South Africa.

Crypto assets may, however, have a different regulatory treatment if they have characteristics similar to traditional financial instruments or products that are 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 in order 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 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 arrangements may permit them to offer banking-related services in conjunction with registered banks. As such, if a digital wallet constitutes e-money, the issuer is able to 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 Financial Sector Conduct Authority (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.

In 2018, the Crypto Assets Regulatory Working Group (CARWG) was formed under the auspices of the IFWG to specifically review the position on cryptocurrencies.

In April 2020, the IFWG issued a policy position paper on crypto assets that aimed to provide recommendations for the development of a regulatory framework for crypto assets. The policy position paper recommends that Schedule 1 to the Financial Intelligence Centre Act, 2001, South Africa's chief anti-money laundering legislation, be amended to include crypto asset service providers (CASPs) to the list of accountable institutions (that is, for CASPs to be listed as their own category). CASPs would become accountable institutions if they have not already.

In November 2020, the FSCA published a draft Declaration (Draft Declaration) that crypto assets be included as a 'financial product' as defined in section 1 of FAIS. The Draft Declaration (once effective) would require any person furnishing advice or rendering intermediary services in relation to crypto assets to be authorised under FAIS as a financial services provider (FSP) and to comply with the requirements of FAIS. This will include crypto asset exchanges and platforms, as well as brokers and advisers. At this stage, there is no indication of when the Draft Declaration will be finalised and

there is a belief that the Draft Declaration may not be implemented until the CoFI Bill has been promulgated into law.

In June 2021, the IFWG, through the CARWG, published a position paper on crypto assets. Essentially, the position paper provides a roadmap for putting in place a phased and structured framework for regulating crypto assets through the regulation of CASPs. It also serves to initiate the process for the individual financial sector regulators to implement the various recommendations which concern three main areas: anti-money laundering and combating the financing of terrorism, cross-border financial flows and application of financial sector laws.

The IFWG has established regulatory sandbox and innovation accelerator initiatives, both of which form part of the IFWG Innovation Hub. The regulatory sandbox is aimed at giving 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.

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 so as 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.

Asia Pacific

Australia

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

Richard Francis†
Gilbert + Tobin, Sydney
rfrancis@gtlaw.com.au

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

Broadly, 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.

Licensing obligations apply to entities that carry on a financial services business in Australia or engage in consumer credit activities. The financial service and financial product definitions are broad, and generally capture any investment or wealth management business, payment service (ie, non-cash payment facility), advisory business (including robo-advice), trading platform, and crowdfunding platform, triggering the requirement to hold an Australian financial services licence (AFSL) or rely on an exemption. Similarly, engaging in peer-to-peer lending activities will generally constitute consumer credit activities and trigger the requirement to hold an Australian credit licence (ACL) or be entitled to rely on an exemption. Certain crypto assets can be captured by the financial product and financial services definitions and trigger the AFSL and ACL regimes.

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 (which may capture certain crypto assets) are regularly made and accepted (ie, an exchange). Any entity operating a clearing and settlement mechanism (CS) which enables parties transacting in financial products to meet obligations to each other, must hold a CS facility licence or otherwise be exempt.

The Australian Consumer Law applies to all Australian businesses that engage or contract with consumers. 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.

The Anti-money Laundering and Counter-terrorism Financing Act 2006 (Cth) (AML/CTF Act) applies to entities that provide 'designated services' with an Australian connection. Generally, the AML/CTF Act applies to any entity that engages in financial services, credit (consumer or business) and payment activities, and the operation of digital currency exchanges in Australia. Obligations

---

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

† Richard is a senior lawyer in Gilbert + Tobin's Tech + IP group focusing on fintech, crypto assets and financial services. Richard draws on extensive experience to deliver holistic and innovative client solutions across a wide range of issues.

include enrolment with the Australian Transaction Reports and Analysis Centre (AUSTRAC), reports and customer due diligence.

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 Banking Executive Accountability Regime (BEAR), which is also administered by APRA and establishes, among other things, accountability obligations for ADIs and their senior executives and directors, and deferred remuneration, key personnel and notification obligations for ADIs.

The Payment Systems (Regulation) Act 1998 (Cth) (Payment Systems Act) regulates purchased payment facility providers in relation to stored value facilities. Generally, such holders of stored value must be an ADI or be exempt from the requirement.

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, and APRA collects data from registered financial corporations under FSCODA. Generally, registered financial corporations with assets greater than AUD 50m need to regularly report to APRA statements of financial position.

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.

The Privacy Act 1988 (Cth) (Privacy Act) regulates the handling of personal information by Government agencies and private sector organisations with an aggregate group revenue of at least AUD 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.

The Notifiable Data Breaches (NDB) scheme, introduced in 2018, mandates that entities regulated under the Privacy Act are required 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 NDB scheme applies to agencies and organisations that the Privacy Act requires to take steps to secure certain categories of personal information.

The Reserve Bank of Australia (RBA) has completed a framework review of the regulatory regime supporting various payment methods. Key outcomes of the review include 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. In addition, given the complexity of the regulatory issues, the RBA will continue to engage with Treasury in relation to buy now pay later (BNPL) service providers removing their no-surcharge rules.

During the second half of 2021, numerous other government reviews in relation to payments, crypto asset and crypto asset-adjacent services were completed, including the Treasury's review of the Payments System, the Final Report of the Senate Select Committee on Australia as a Technology and Financial Centre (Senate Report) and the Parliamentary Joint Committee Inquiry into Mobile Payments and Digital Wallets.

It is expected that the recommendations from these reviews will have significant effects on the current regulatory regimes relevant to payments and crypto assets. In December 2021, the Australian Government issued its response to the recommendations arising from these reviews and planned to deliver a number of outcomes in the second half of 2022.

Recognising the recent revolution in payment systems, these outcomes included having a strategic longer-term plan for the payments system, proposed enhanced regulatory powers for the Treasury and modernising the existing payment legislation, including in respect of BNPL products and digital wallets.

Crypto asset-related outcomes included:

- completing consultations on establishing a licensing framework for digital currency exchanges and the providers of crypto custody or depository services;
- settling a framework for updating the payment licensing arrangements;
- completing a review on an appropriate taxation framework for digital transactions and assets; and
- considering the establishment of a new digital autonomous organisation company structure.

In connection with these outcomes, during the first half of 2022, the Treasury consulted on a regulatory framework that was proposed for crypto asset secondary service providers (referred to by Treasury as CASSPrs). The framework proposes either:

1. implementing a CASSPr licensing regime, separate from the AFSL regime which includes similar obligations to the AFSL regime;
2. defining crypto assets as financial products and bringing such businesses within the existing AFSL regime (with the ability to carve out certain crypto assets); or
3. self-regulation.

The principles-based obligations for the proposed new regime include similar obligations to those that apply to AFSL holders, fit and proper person requirements, capital requirements, client money obligations, anti-hawking, regular independent audits, breach reporting and custody arrangements. At the time of writing, the Treasury has not reported on the outcome of the consultation; the change of government in May 2022 has created uncertainty around the payments and crypto asset-related outcomes slated for completion in 2022. Once an option for regulation is determined, significant additional time will be required to implement the new regime.

In July 2022, Stephen Jones, Assistant Treasurer and Minister for Financial Services, announced an upcoming consultation on improving the regulation of credit in Australia and made comments

suggesting that the BNPL products will be regulated in a tailored way. BNPL providers are currently regulated under a voluntary BNPL Code of Practice which came into effect on 1 March 2021.

On 22 August 2022, the Treasury announced it will improve the way Australia's regulatory system manages crypto assets, to keep up with developments and provide greater protections for consumers. The government is seeking to take a balanced approach to regulation which allows consumers to participate in the market while also better protecting them. As the first step in a reform agenda, and consistent with the recommendations of the Senate Report, the Treasury will prioritise 'token mapping' work in 2022. A consultation paper is expected to be released soon. The mapping exercise will help identify how crypto assets and related services should be regulated.

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.

Currently, 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 and must register with AUSTRAC. Exchange operators are required to keep certain records relating to customer identification and transactions for up to seven years.

As noted in Question 1, there have been numerous government reviews that are ongoing or have recently been completed in connection with how crypto assets and crypto asset-adjacent services should be regulated. It is expected that the recommendations from these reviews will have significant effects on the current regulatory regimes relevant to crypto assets.

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 both ASIC and APRA.

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 also provide these financial services under licensing exemptions which apply when the services are provided on behalf of an AFSL holder.

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

Many payment service providers also provide a designated service under the AML/CTF Act regarding 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.

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.

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

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 more broadly 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, which could include blockchain-related businesses.

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 class orders 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 class orders (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 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.

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

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 and Consumer Act 2010 (Cth) (CCA), the Privacy Act 1988 (Cth) and the Australian Information Commissioner Act 2010 (Cth) (AIC Act) to establish a 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 Australian Competition and Consumer Commission (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 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. Under open banking, as of 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 starting 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.

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 and 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, trust and foreign exchange etc. Meanwhile, the People's Bank of China (PBOC) as 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, assets 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 crypto currency/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 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, process, 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 fintech business typically relies heavily on personal data to develop their business, such as through precision marketing, online ads and personal profiling, such data protection laws and regulations mentioned above can potentially apply to most fintech business.

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.

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 fund and are not allowed to engage in sales of money market fund.

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 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 is also 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 of 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 or not 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 - Macau 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:

- 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.
- 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 (API) and software development kits (SDK) 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

Simon Lin†
Fangda Partners, Hong Kong
simon.lin@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 the CWUMPO as well as the authorisation requirements under the SFO. Fintech companies should evaluate whether their business activities would trigger any obligations under the 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.

† Simon works at Fangda's Hong Kong office and is admitted to practice in Hong Kong. He 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 excepted 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 lender 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 or 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 the answer to 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 crypto assets: a summary of the legal framework regarding crypto assets and how they are regulated.

In Hong Kong, crypto assets are considered as virtual assets (VA) and do not qualify as money and are not regulated as legal tender by HKMA.

Generally, VA can be classified into two categories, being securities-type VA and non-securities VA. Apart from the existing 'regulated activities' regime under the SFO, the regulators in Hong Kong have been regularly updating the regulatory framework in relation to VA in recent years. The relevant legal framework of VA is summarised below.

Securities-type VA

Securities-type VA refers to VA which falls within the definition of 'securities' under the SFO. Accordingly, any activity relating to it may become a 'regulated activity' such that a SFC's licence is required.

The SFC implemented a voluntary opt-in licensing regime allowing virtual asset trading platforms which offer trading of at least one security token on its platform to apply for a licence from the SFC for Type 1 (*Dealing in securities*) and Type 7 (*Providing automated trading services*) regulated activities. If a trading platform only offers non-securities VA, it may operate as an unregulated business. This position will be changed following the implementation of the new licensing regime for VA service providers (VASPs) (see below).

According to the SFC's Guidelines on Online Distribution and Advisory Platforms and paragraph 5.5 of the SFC's Code of Conduct for Persons Licensed by or Registered with the SFC (SFC Code of Conduct), securities-type VA would likely be regarded as complex products and therefore additional investor protection measures would be applicable.

It is also worthwhile to note that OSL Digital Securities Limited has recently become the first SFC-digital asset licensed broker to conduct security token offering to professional investors in Hong Kong.

VASPs

The Anti-Money Laundering and Counter-Terrorist Financing (Amendment) Bill 2022 was passed on 7 December 2022. Under the amended AMLO:

A new licensing regime for VASPs will come into effect on 1 June 2023.

A VA is defined as a cryptographically secured digital representative of value that is expressed as a unit of account or a store of economic value; is used (or is intended to be used) as a medium of exchange accepted by the public as a payment for goods or services or for the discharge of a debt, or for investment purposes or provides rights, eligibility or access to vote on the management, administration or governance of the affairs in connection with, or to vote on any change of the terms of any arrangement applicable to, any cryptographically secured digital representation of value; can be transferred, stored or traded electronically and satisfies other characteristics prescribed by the SFC.

The definition of VA expressly excludes: (1) digital representations of fiat currencies; (2) limited purpose digital tokens; (3) securities or future contracts; (4) any float or SVF deposit of a stored value facility as defined by section 2 of the PSSVFO; or (5) satisfies other characteristics prescribed by the SFC.

VASPs will be required to apply for a licence from the SFC.

The new licensing regime is primarily intended to capture the operation of a VA exchange and thus the scope of 'VA service' currently only covers VA exchanges. However, the Hong Kong government could expand the scope of 'VA services' to cover other forms of VA activities in the future.

VA exchange is defined as the provision of services through means of electronic facilities whereby: offers to sell or purchase VAs are regularly made or accepted in a way that forms or results in a binding transaction; or persons are regularly introduced, or identified to other persons in order that they may negotiate or conclude, or with the reasonable expectation that they will negotiate or conclude sales or purchases of VAs in a way that forms or results in a binding transaction; and where client money or client VAs comes into direct or indirect possession of the person providing such a service.

Any person who seeks to carry on a business of operating a VA exchange is required to apply for a licence from the SFC. The new licensing regime will also prohibit a person, whether in Hong Kong or elsewhere, from actively marketing to the Hong Kong public a regulated VA activity or associated services, unless that person is properly licensed and regulated by the SFC to carry out that activity. This means that a VA exchange targeting investors in Hong Kong will be required to obtain a licence from the SFC even it only trades non-securities VAs.

Only Hong Kong incorporated companies with a permanent place of business in Hong Kong or foreign incorporated companies registered under the Companies Ordinance will be permitted to apply for a licence.

A licensed VASP should meet the prescribed regulatory requirements concerning, amongst other things: financial resources, knowledge and experience, soundness of the business, risk management, and segregation and management of client assets.

The relevant person of the applicant will be subject to meeting a fit and proper test as well as AML/CTF and other regulatory requirements.

It is expected that, at the initial stage, a licensed VASP will only be able to offer services to professional investors, and that this restriction will be imposed by the SFC as a licence condition.

There will be a transition period. A person will not contravene the new licensing regime for the period until 1 June 2024 if it is a corporation that was carrying out the business of a VA service in Hong Kong on 1 June 2023 and it makes an application to be licensed to provide the VA service between 1 June 2023 and 31 May 2024.

Distributing/dealing in/advising on VA and VA-related products

In January 2022, the SFC and HKMA issued a joint circular which sets out regulatory guidelines for traditional financial intermediaries and banks to follow when they are:

- distributing VA-related products;
- providing VA-dealing services; and
- providing VA advisory services to clients.

The Insurance Authority also issued a circular to insurers on regulatory approaches of the Insurance Authority in Relation to VA and VASP.

Stablecoins

The regulators in Hong Kong are contemplating the need to introduce a regulatory regime for stablecoins. In January 2022, HKMA issued a discussion paper on crypto assets and stablecoins in order to seek feedback on its proposal to regulate certain activities related to stablecoins.

2022 Policy Statement on VA

On 31 October 2022, the Financial Services and the Treasury Bureau issued a policy statement which sets out the Hong Kong government's latest police stance and approach towards developing a vibrant sector and ecosystem for VA in Hong Kong. The Hong Kong's government has proposed certain initiatives, including:

- to conduct a public consultation on how retail investors may be given a suitable degree of access to VA, while being careful and cautious about the risks to retail investors, including by enhancing investor education and ensuring that suitable regulatory arrangements are in place;
- to open up the possibility of having exchange traded funds (ETF) on VA; and
- to review the property rights for tokenised assets and the legality of smart contracts.

The Hong Kong government and the regulators are also exploring certain pilot projects to test the technological benefits brought by VA and its applications in the financial markets, eg green bond tokenisation and e-HKD.

It is expected that Hong Kong is shifting towards becoming a more friendly jurisdiction for crypto assets.

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 RPS 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 or not an RPS should be designated, and also requirements that the 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.

Stored value facilities

Digital wallets, 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 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 HKD$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 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, the HKMA, the SFC and the 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 the HKMA's supervisory requirements. To date, the 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. The HKMA also participated in the Global Financial Innovation Network on cross-border testing of pilot schemes.

The SFC sandbox

The SFC Regulatory Sandbox invites licensed corporations and startups that wish to carry out a regulated activity under the Securities and Futures Ordinance 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 innovate 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 as a means 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 recommend 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 January 2023, of the 28 participating banks, 23 banks have launched the Phase III API functions for retail customers, 19 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*
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.

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

* 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.

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, enables 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) relating to payment systems operated by them, in India. 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 KYC norms. Similar guidelines have also been enabled for non-banking financial companies and payment system operators.

The Reserve Bank issued and invited stakeholder comments on the Draft Master Directions on Outsourcing of IT Services on 23 June 2022, which govern outsourcing relationships between regulated entities (such as banks, credit information companies, non-banking financial companies etc) with their information technology service providers.

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

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 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 and 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 also report certain questionable/suspicious transactions.

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, issuers of prepaid payment instruments, such as 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 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 vs 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, Government of India has mandated all companies to include disclosures in their financial statements on virtual currency and cryptocurrency transactions undertaken by them in a financial year.
- Pursuant to a notification by the Ministry of Electronics and Information Technology, Government of India, 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 had 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.

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 or 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, the primary regulator in the financial services sector has 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.

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 for 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 of 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 Inter Operable Regulatory Sandbox, which tests fintech products and solutions that would typically fall within the regulatory purview of multiple financial sector regulators.

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).

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 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 eco-system (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 several 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 previous legislation. It sets the scope of P2P lending practice, from business activities, registration and licensing procedures, the relationship between the P2P lending providers and users, risk mitigation, and IT system maintenance, to prohibitions in P2P lending and the minimum requirements concerning agreements between the lender–borrower and lender–service provider.

---

* 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.

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 a regulation in 2019 to regulate the trading mechanism for crypto assets, namely Bappebti Regulation 5/2019. This was then amended by Bappebti Regulation No 8 in 2021. 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).

Reg 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;
- 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

2 Islamic law.

Regulation No. 23/POJK.04/2016, as amended by OJK Regulation No. 2/POJK.04/2020 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.

IT-based expert advisory services

Bappebti recently issued a regulation to outlaw rogue robot trading but 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 that have been approved by the Bappebti (FA) 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.

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.
- 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.

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.

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 was amended several times, the latest being issued last year through Bappebti Regulation No 8 of 2021 on Guidelines for the Physical Trading of crypto assets on the Futures Exchange (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.

To be appointed as a crypto asset exchange, crypto asset clearing agency, crypto asset trader, crypto asset client, and 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]

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:

5 Peraturan Badan Pengawas Perdagangan Berjangka Komoditi No 8 Tahun 2021 tentang Pedoman Penyelenggaraan Perdagangan Pasar Fisik Aset Kripto di Bursa Berjangka.

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

- 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 a final income tax with the tariff of:

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

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 provider, or *penyedia jasa pembayaran* (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 provider, or *penyelenggara infrastruktur sistem pembayaran* (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:

For fintechs related to the payments systems

Bank Indonesia Regulation No. 23/6/PBI/2021 on Payment Services Provider.[7] 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 fintechs 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.[8] 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.[9] This regulation sets out protocols and instructions that facilitate open interconnection between applications in payment transaction processing.

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

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

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

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, KYC, record-keeping, reporting, 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.

Digital banks

During the past decade, digital banking has thrived in Iran in part as a result 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.

Legal mining now requires permission from the Ministry of Industry. Mining facilities must not be in the vicinity of large population centres, they must pay for their electricity at unsubsidised rates and may not operate during peak hours of consumption. The Ministry of Energy has introduced detailed regulations on electricity tariffs applicable to mining facilities.

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 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 indicate the CBI's plans to introduce its rial CBDC, known as crypto-rial. Crypto-rial and tokens based on the former may be used as means of payment.

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.

Wallets' and transactions' 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 programs 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 taskforce 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 therefore 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.

Japan

Yuri Suzuki*
Atsumi & Sakai, Tokyo
yuri.suzuki@aplaw.jp

Naoki Kanehisa†
Atsumi & Sakai, London
naoki.kanehisa@aplaw.jp

Kenichi Tanizaki‡
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 allowed to operate a remittance service by registering as a Funds Transfer Service.

There are three types of fund transfer services. For Type 1, fund transfer services do not have a limit on the value of remittances. 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 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 either as prepaid payment instruments for one's own business or as prepaid payment instruments for third-party business. In this

---

* 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.

† 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.

‡ Kenichi is a submanager 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.

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, and such instruments are issued by funds transfer service providers.

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 is 31 March and 30 September each year). The 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 in the Cabinet Office Order) (see Question 3).

The Banking Act – regulation of electronic payment services

Electronic payment services include electronic remittance services, which receive remittance instructions online and relay the instructions 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 (as a business purpose) requires registration as an electronic payment service under the Banking Act.

Regulations on crypto assets

Please see Question 2 for further details.

The Payment Services Act – regulations of stablecoins

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

Financial Action Task Force (FATF) – Fourth Mutual Evaluation of Japan

In response to the conclusions contained in the report of the Fourth Mutual Evaluation of Japan by the FATF – namely that further enhancement and optimisation of transaction filtering and monitoring

is required in Japan – 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 the permission of the competent authority. Due to this amendment, the Japanese Bankers Association is 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, it is expected, would 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 applications.

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

In Japan, applicable laws and regulations on crypto assets vary depending on the types of digital assets, and 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 regulation under the PSA 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 purpose 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 as 'over-the-counter transactions of derivatives' and conducting such transactions on a regular basis is regulated as a 'financial instruments business'. Therefore, any person who conducts financial instruments business falls within the scope of regulation under the FIEA 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 thus 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 regulation under the FIEA and must be registered with the regulator.

Stablecoins

Amendments to the PSA, the Banking Act and other laws concerning electronic payments were promulgated in June 2022. The new provisions under the amendments include a new regulatory framework for stablecoins, which will be introduced in 2023. Under this new framework, stablecoins will be categorised as follows:

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

While the category of stablecoins described in (2) is regulated as 'crypto assets' under the pre-existing provisions of the PSA, as discussed in this section 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 are intended to regulate the stablecoins described in (1), and a new licensing regime will be 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 will be 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, as such financial institutions are already 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 instrument (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 each customer when the customer holds more than JPY 1million in their accounts, to determine if (and ensure that) funds in such accounts 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 are currently not subject to Anti-money laundering and know your client (AML/KYC) regulations in Japan, even if customers can charge high amounts for such prepaid payment instruments and transfer them to other customers, which raises money laundering concerns. The provisions of the newly amended PSA and the Act on Prevention of Transfer of Criminal Proceeds, which will both come into force in 2023, requires issuers of prepaid payment instruments for third party business to comply with AML/KYC regulations, specifically in situations where the issuer issues prepaid payment instruments that can be charged at 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 given period (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, the METI enhances Japan's industrial competitiveness through two systems under the Industrial Competitiveness Enhancement Act.

Under the System to Remove Gray Zone Areas, where there is uncertainty over whether or not existing laws and regulations will be applied to innovative products and services due to their innovative nature, the METI, together with the competent ministry, can provide clarity and confirmation, regarding the applicability of existing regulations, to the concerned company.

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

Financial Services Agency (FSA)

The 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.

The 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 is 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, the TMG offers various programmes to increase the number of players participating in the Tokyo market, including the fintech industry. The TMG's programmes include:

- a project to attract overseas financial companies, including fintech companies;
- 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 base of operations of overseas financial corporations; and
- a financial award system, including accelerator programme for fintech companies.

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

A regulation targeting open banking is the amendment to the Banking Act, which came into force on 1 June 2018.

This amendment introduced the concept of 'electronic payment services', which includes:

- a service to provide funds transfer instructions via the internet at the request of depositors (Write API); and
- a service 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 obligated 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 scheduled amendments to 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 factor 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.

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 (emoney), merchant acquiring services and insurance and takaful 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 has announced the names of the five applicants who have been granted digital bank licences in Malaysia.

Given the rise of alternative payment methods in Malaysia and the growing significance of merchant acquirers in the payment landscape, BNM has made a timely move by issuing a new 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.

In relation to the issuance of e-money, the primary guidelines applicable to issuers of e-money in Malaysia are the Guidelines on Electronic Money (e-money) (E-Money Guidelines), which outline

* 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.

the broad principles and minimum standards to be observed by e-money issuers in relation to the operation of their e-money schemes. BNM issued an exposure draft on the Policy Document of Electronic Money (E-Money Draft) on 11 June 2021 to elicit public comments on the proposed requirements and guidance for issuers of e-money approved pursuant to Section 11 of the FSA. To date, the E-Money Draft has not been finalised by BNM. The E-Money Draft, once finalised and issued as a policy document by BNM, will supersede the E-Money Guidelines.

With regard to the insurance and takaful business, in particular digital insurance business and digital takaful business, BNM published a discussion paper on the licensing framework for digital insurers and takaful operators on 4 January 2022, to request feedback on the proposed entry requirements and key assessment criteria for the licensing of digital insurers and takaful operators (DITO), potential temporary or foundational regulatory flexibilities, overall regulatory framework and the market infrastructure to support the digital insurance and takaful development in Malaysia. However, the finalised licensing framework for digital insurers and takaful operators has yet to be issued.

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 and money-changing 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.

In light of the current market development in the remittance space, BNM has published a consultation paper on proposed amendments to the Money Services Business Act 2011 to elicit public feedback on the proposed amendments to MSBA. The aforesaid consultation paper makes several suggestions, including extending the definition of 'remittance business' to cover different types of remittance transactions and the *modus operandi* used to undertake remittance transactions. To date, there have been no amendments to the MSBA following the issuance of the said consultation paper.

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.

In order 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 22 November 2021, which set out the requirements for the registration as an RMO and ongoing requirements that apply to RMOs. A recognised market essentially covers 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 market of a stock exchange or derivatives market 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 limited to '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, setting 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, which has increased the risk of unfair or predatory practices, the Public Consultation Paper on Consumer Credit Act (Part 1) has been prepared and 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 requests opinions on the proposed regulatory framework and the authorisation approach to encourage professionalism and fair conduct of credit providers and credit service providers when dealing with credit consumers.

MOF, BNM, SC and such other regulators are working towards the consolidation of a credit industry regulatory framework through the enactment of the Consumer Credit Act. Please note that the deadline for the submission of the feedback to the Task Force has closed on 5 September 2022.

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 (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 obtain the approval of 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 within the definition of 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 operated by an IEO operator which hosts IEO must be registered 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 a third party. 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 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 a 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, with a view to making the funds available 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 obtain approval from BNM.

BNM issued the Policy Documents on Governance, Risk Management, and Operations for Money Services Business on 30 June 2022, which outline 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 favorable 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 and fulfil the following specified criteria, namely:

- enter 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;
- facilitate the merchant's acceptance of payment instrument; and

- be a direct participant of payment instrument networks to provide merchant acquiring services.

Merchant acquirers are classified as large acquirers and small acquirers under the MAS Policy Documents, depending on their actual or projected amount of average monthly transaction value. While generally the requirements under the MAS Guidelines 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 (ie payment facilitators, merchant recruitment agents, payment gateway service providers, IT service providers) under the outsourced arrangement.

Digital wallets

E-money is defined under the Financial Services (Designated Payment Instruments) Order 2013 as a designated payment instrument 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.

There are two types of e-money schemes (small schemes and large schemes), which are determined by the purse size and the outstanding e-money liabilities. The specific requirements under Part C of the E-Money Guidelines are only applicable to issuers of large e-money schemes that are not licensed institutions.

The E-Money Guidelines set out the broad principles that must be observed by e-money issuers:

- establish adequate governance and operational arrangements;
- ensure proper risk management is in place;
- ensure that the risks of using e-money, and rights and responsibilities of all stakeholders, are clearly defined and disclosed;
- ensure prudent management of funds;
- ensure timely refund of stored value in the e-money; and
- implement adequate measures to prevent the use of e-money for money laundering, and ensure compliance with other requirements.

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 introduced the Technology Regulatory Sandbox Framework on 18 October 2016 to enable financial institutions and fintech players (either on their own or in collaboration with

financial institutions) to deploy and experiment on innovative fintech solutions and business models in a live environment, within well-defined parameters and duration.

BNM has recently revealed its strategies to advance digitalisation of the financial sector in its five-year Financial Sector Blueprint 2022–2026, which includes the enhancement of existing pathways for digital innovation to test, scale and exit, such as by refreshing the Fintech Regulatory Sandbox to accelerate time-to-live testing under the Sandbox.

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.

Both SC and BNM regularly organise fintech conferences to bring together policymakers, innovators, investors and financial service providers for networking, collaborations 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.

Furthermore, BNM has also collaborated with a number of partners as part of 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 the legal, compliance and regulation requirements for their development of innovative products and services.

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.

New Zealand

David Craig*
Bell Gully, Wellington
david.craig@bellgully.com

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

Zac Kedgely-Foot‡
Bell Gully, Wellington
zac.kedgley-foot@bellgully.com

Richard Massey§
Bell Gully, Wellington
richard.massey@bellgully.com

Lothar Krumpen**
Bell Gully, Wellington
lothar.krumpen@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 with the same regulatory concepts applying 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.

---

* David is a partner who specialises in banking and finance law and financial services regulation. He advises on domestic and international banking and capital markets transactions and the regulation of financial products, services and markets in New Zealand and is recognised as New Zealand's leading derivatives lawyer.

† 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.

‡ Zac is a senior associate 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.

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

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

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, and 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 crowd funding intermediaries

There is no requirement for a peer-to-peer (P2P) lending or crowd funding 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 NZD 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 issuer

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 client's 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 product

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 widespread criticism of the extensive reach of the new obligations, the government has recently announced a series of targeted amendments to the responsible lending regulations, to partially reduce the compliance burden on lenders. In addition, the government is currently consulting on the extent to which buy now pay later (BNPL) products should be regulated, including whether BNPL products should be captured under the CCCFA.

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 definition 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 this issue. 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 program 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. This review is considered to be a 'once in a generation' review of the existing regime that will likely bring in substantial changes and modernisations to the AML/CFT Act. More specifically, it has been noted that the current regulatory regime does not have specific obligations for virtual asset service providers (eg, providers of services relating to crypto assets). Therefore, as part of the statutory review, the regulators are exploring how AML/CFT obligations can be tailored to virtual asset service providers.

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.

A new prohibition on unconscionable conduct has been introduced in connection with recent changes to the FTA. Under this prohibition, a person must not, in trade, engage in conduct that is

unconscionable. 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 is remarkably broad in application because it applies whether or not (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 e-mail, 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 Bill being in the final stages of preparation. It is expected that this Bill will be introduced into Parliament within the coming months.

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

Aside from taxation, 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 programs) 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 section 1 above) 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 market' under Question 1) if one or more of the crypto assets traded on the platform are 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 and crypto assets are treated as property under New Zealand law so 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 is expected.

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;
- the statutory review of the AML/CFT Act currently underway will likely result in changes in this area;
- 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
- a Parliamentary inquiry was established in July 2021 to consider 'the current and future nature, impact and risks of cryptocurrencies'.

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

Similarly to 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 e-mails, 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 and 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.

There is currently no open banking legislative framework. However, in July 2021, the Government confirmed its decision to implement a new legislative framework for a Consumer Data Right (CDR) (following a consultation period in 2020 and extensive submissions from a range of industries).

The proposed CDR is intended to enable consumers to require data held about them to be shared with trusted third parties. To protect the security of transfers of consumer data, third party data recipients will need to be formally accredited. In addition, any data shared through the CDR will only

take place with a person's informed consent and would be used only for purposes agreed with the relevant consumer.

As in Australia, it is expected that primary legislation will create the overarching framework of the CDR. Designations will then specify, for specific sectors, the type of data that is covered and the functionality that must be enabled. The government has not yet announced which sectors should be considered for designation first. However, it is likely that the banking industry will be one of the first sectors for implementation of the CDR when it is introduced. The banking industry has already taken independent steps to support data portability, including through an API centre operated by Payments NZ, but the government has nevertheless identified the banking sector as a key priority for the mandatory data portability requirements under the CDR.

In December 2022, the government published a Cabinet paper, which set out its further decisions on the implementation of a CDR regime. The government has confirmed that banking will be the first sector assessed for designation, under criteria to be set out in the CDR bill. A draft of the CDR bill is expected to be issued for consultation in early 2023, although the proposed timeframe for implementation is yet to be confirmed.

Singapore

Adrian Ang*
Allen & Gledhill, Singapore
adrian.ang@allenandgledhill.com

Shrinidhi Muthappan†
Allen & Gledhill, Singapore
Shrinidhi.Muthappan@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 the type of licence that will need to be issued by the relevant authority or licensing exemptions that may be applicable to a fintech product or service), technology contracts, data protection, intellectual property issues and financing (ie venture capital investments in fintech companies). Businesses in the Singapore fintech space should consider if they are undertaking any regulated activities, which would require a licence from a regulatory authority.

Key regulatory authorities

The Monetary Authority of Singapore (MAS) is Singapore's central bank and an integrated supervisor overseeing all financial institutions in Singapore such as banks, insurers, capital market intermediaries, financial advisers, the stock exchange and also commodity future contracts.

The Registry of Money Lenders 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, which regulates activities involving spot commodity trading.

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.

---

* 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.

† Shrinidhi is a trainee in the Fintech and Financial Regulatory and Compliance Practice at Allen & Gledhill. Her areas of practice include capital markets, banking and payments work in Singapore.

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 most significant ongoing regulatory initiative affecting fintech in Singapore is probably the PS Act. On 19 November 2018, the Payment Services Bill (B48/2018) was introduced for its first reading in Parliament. The Bill was subsequently passed in Parliament as the Payment Services Act 2019 (PS Act) on 14 January 2019. 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
- the provision of '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.

Subsidiary legislation

Financial institutions also have to consider subsidiary legislation, notices and guidelines under each Act. Regulations and notices have the force of law and must be complied with. Guidelines set out MAS' expectations and should be complied with, commensurate with the level of risk and complexity of the financial institution's activities. These legislations would only need to be complied with if the business is undertaking a regulated activity, which would require a licence.

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

Legal status

The specific structure and characteristics of the crypto asset must be examined individually to determine its legal characterisation. It is the legal characterisation of the crypto asset that determines the legislation that would apply to it. For example, if a crypto asset is seen as a share, debenture, unit in a business trust or a securities-based derivatives contract, it is likely to be regulated under the Securities and Futures Act, Chapter 289 (SFA). In contrast, a crypto asset such as Bitcoin and Ether will be characterised as a DPT and activities relating to DPT may be regulated under the PS Act.

AML/CFT measures

Typically, anti-money laundering and combatting the financing of terrorism (AML and CFT) rules will apply to regulated financial institutions. Specific anti-money laundering notices and guidelines have been published with respect to DPT. These notices and guidelines generally follow the guidance provided by the Financial Action Task Force (FATF).

Payment Services Act

The MAS regulates the provision of 'payment services' – including DPT services in the PS Act. Under the PS Act:

- One of the seven regulated activities includes the provision of DPT services. Currently, two activities are regulated and will require a licence: firstly, 'facilitating the exchange of' DPTs (ie, operating a platform allowing persons to buy or sell DPTs on a centralised basis); and secondly, 'dealing in' DPTs (ie buying or selling DPTs as a service).
- Some of the distinguishing characteristics of DPT are that: (1) DPT is not denominated in or pegged by its issuer to any fiat currency; and (2) DPT is, or is intended to be, a medium of exchange accepted by the public or a section thereof as payment for goods and services or for the discharge of a debt (ie, cryptocurrencies such as Bitcoin and Ether).

The Singapore parliament passed the Payment Services (Amendment) Act on 4 January 2021, for (amongst other activities) three more DPT-related activities to be regulated in the near future, but these have not yet come into force. The three new activities to fall under the expanded scope of 'DPT services' are the provision of custody services for DPT, DPT transmission services and DPT brokerage services.

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

Different pieces of legislation may apply in respect of different payment-related activities. This will depend on the specific scope of the product or service being offered. All products and services are regulated at a national level, and while the regulator may differ, the relevant regulator for fintech products and services is typically MAS.

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.

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. MAS has also announced Sandbox Plus, an

improvement to the existing Regulatory Sandbox framework to further aid financial innovation and fintech adoption.

There are also various funds and initiatives to facilitate access to capital for fintech entities, such as:

- MAS announced a SGD 125m support package on 8 April 2020, for the financial and fintech sectors to deal with the immediate challenges from Covid-19, and position strongly for the recovery and future growth. MAS also launched a SGD 6m MAS–SFA–AMTD Fintech Solidarity Grant to help Singapore-based fintechs sustain operations, retain staff, and offset proof of concept (PoC) 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 2023.
- Startup SG Accelerator, Startup SG Equity, Startup SG Founder, Startup SG Tech, Startup SG Loan and Startup SG Talent (all operated by Enterprise Singapore Board), which provide governmental co-investment, mentorship support and startup capital grants.
- The MAS National Artificial Intelligence Program in Finance was launched to build deep artificial intelligence (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.

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).

In addition, the ASEAN Financial Innovation Network (AFIN), a not-for-profit entity that was jointly formed by the MAS, the World Bank Group's International Finance Corporation (IFC) and the ASEAN Bankers Association, has launched APIX. APIX is a global, open-architecture platform

that supports financial innovation and inclusion in ASEAN and around the world. APIX helps market players to connect with one another, design experiments collaboratively and deploy new digital solutions. On the global APIX marketplace, financial institutions and fintech companies can discover and connect with one another easily and cost-effectively. The APIX sandbox allows financial institutions and fintech companies to collaboratively design experiments to validate digital solutions in different scenarios via APIs. APIX facilitates financial institutions' adoption of APIs and enables them to rapidly deploy new digital solutions to underserved markets in ASEAN and other parts of the world.

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); and
- the Special Act on Support for Financial Innovation governing fintech innovation.

Electronic Financial Transactions Act (EFTA)

Under the EFTA, there are seven types of electronic financial business licence:

- electronic funds transfer business;
- electronic currency business;
- electronic prepayment business;
- electronic debit payment business;
- electronic payment settlement agency business;
- payment deposit business; and
- electronic notification settlement business.

* Doil Son is Head of the IP & Technology Practice of Yulchon. He also serves as Senior Vice 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.

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 business as of 1 September 2022 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	75
Electronic debit payment business	24
Electronic payment settlement agency business	139
Payment deposit business	39
Electronic notification settlement business	15
Total	292 registrations (by 174 companies)

Table 1: Types of business licence

Amendments to the EFTA have been discussed since 2020, as the current EFTA fails to encompass integrated and comprehensive financial services such as fintech. The proposed amendment bill to the EFTA at the National Assembly intends to simplify the existing seven types of electronic financial business licences into three by re-categorising/consolidating the types by function, and adding 'payment instruction service business' and 'comprehensive payment settlement business' licences (see Figure 1).

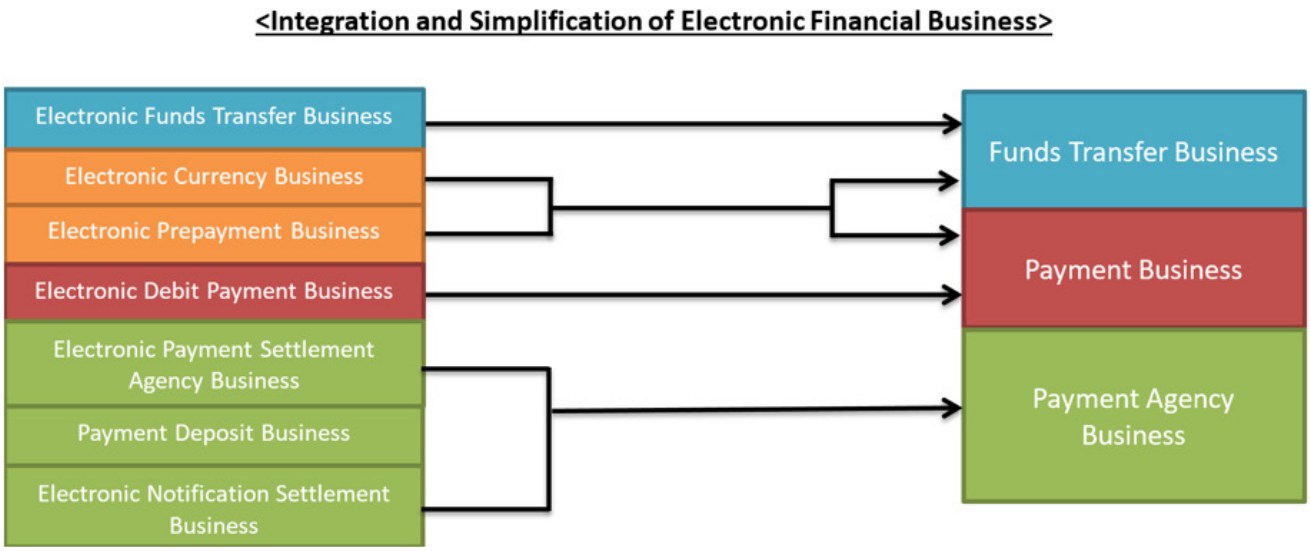

Figure 1: Integration and simplification of electronic financial business

The current EFTA includes provisions regarding securing the safety of electronic financial transactions, and the details of such safety measures are stipulated in the Electronic Financial Supervisory Regulations. The FSC recently announced the following amendments to the relevant 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. Recently, the FSC announced that it will:

- ease the regulations on the physical separation of networks for development or test servers;
- allow exceptions through regulatory sandboxes for the operating systems that are unrelated to financial transactions and do not handle customer and transaction information; and
- allow the use of internal networks for non-important tasks that utilise software as a service (SaaS).

On 29 April 2022, the FSC made a legislative notice to include the aforementioned short-term improvements in the proposed amendments to the Electronic Financial Supervisory Regulations. These improvements are also expected to be reflected in the Revised Guidelines on Cloud Computing Services in the Financial Sector, which will be released at the end of this year.

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 the aforesaid laws.

In addition, the 'Three Data Acts' (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 refer to Question 2 for details.

Special Act on Support for Financial Innovation

Regarding the Special Act on Support for Finance Innovation, please refer to Question 4 below.

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 on crypto assets.

In May 2018, the Supreme Court ruled that 'Bitcoin is a property that has an economic value and can be confiscated if it has been acquired as proceeds of crime' (Supreme Court Decision 2018D02619, decided 30 May 2018) whereby the court indirectly acknowledged the economic value of virtual assets for the first time at the national level.

The Amendment to the Act on Reporting and Using Specified Financial Transaction Information, effective as of 25 March 2021, defines the term 'virtual assets' and imposes 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 shall 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.

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).

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. However, please note that this can be changed once the National Assembly passes the amendment to the EFTA.

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 of the EFTA).

Any person who intends to provide electronic payment settlement agency services shall be registered with the FSC (Article 28(2), Subparagraph 4 of the 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 of the 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 'special persons' prescribed by Presidential Decree), and (2) it shall be able to purchase goods or services which belongs to at least two different business categories (Article 2, Subparagraph 14 of the EFTA).[3]

Although, there are no specific laws on this point, foreign payment service providers and digital wallets may not, in practice, be subject to the licensing requirements if they satisfy the following requirements for 'reverse solicitation':

- there should be no active solicitation or advertisement to any Korean customers;
- there should be no intent to 'target' Korean buyers (ie, no marketing to Korean buyers via e-mail, phone, or post);
- the website and platform should not provide any Korean translations; and
- there should be no employees in Korea.

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 There is an exemption for the registration obligation for 'electronic prepayment means' under the EFTA. When the total balance of the issued amount does not exceed KRW 3 billion, this exemption applies. The term 'total balance' is the average of 'outstanding unused balance' at the end of each quarter. There is, however, a pending amendment bill to the EFTA which intends to exclude the above exemption when the total 'accumulated' balance is above a certain level (to be specified in the Presidential Decree).

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 of the 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 (that 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 Joint Banking Open platform, a predecessor of the open banking service.

- 25 February 2019: Announcement of the 'financial settlement infrastructure innovation plan' to establish an innovative infrastructure in the financial sector (ie, an open joint payment system) after close cooperation with the banking sector, and preparation of detailed action plans.
- 30 October 2019: Pilot implementation of the open banking service.
- 18 December 2019: Full implementation of the open banking service.

The open banking service is currently operated under private agreements among participating institutions, such as financial institutions and electronic financial companies.

Although it is not definitive, it is assumed that the amendment to the EFTA may include provisions for establishing the legal grounds for designating electronic payment transaction clearing systems (open banking) by the FSC, and empowering the FSC to authorise the Financial Telecommunications and Clearings Institute (KFTC) as an electronic payment transaction clearing institution to perform electronic payment transaction clearing business.

Taiwan

Robin Chang*
Lee and Li, Taipei
robinchang@leeandli.com

Eddie Hsiung†
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

Please see Question 3.

Open Banking

Please 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 without 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

* 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.

† Eddie Hsiung is an associate 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.

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 the 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 release, the FSC started to accept applications for establishment of digital-only insurance companies in August 2022.

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, 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 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.

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 (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 (AML)

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 in 2021. According to these regulations, the designated operators of crypto assets and exchanges are required to establish, among others, internal control and audit mechanisms, reporting procedures for suspicious transactions. know-your-client procedures, and so on. The regulations took effect from 1 July 2021, except for the effective date of the provision requiring the crypto-related service provider to obtain the relevant identity information of both the transferor and transferee in case of 'transfer-out' of the cryptocurrency. The effective date of such provision would be further determined and announced by the FSC.

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-advisors.

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.

United Arab Emirates

Nadim Bardawil*
BSA Ahmad Bin Hezeem & Associates, Dubai
nadim.bardawil@bsabh.com

Hala Harb†
BSA Ahmad Bin Hezeem & Associates, Dubai
hala.harb@bsabh.com

Marina El Hachem‡
BSA Ahmad Bin Hezeem & Associates, Dubai
marina.elhachem@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 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 that 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.

† Hala is an associate in the TMT department with both private practice and in house experience. Hala's expertise lies in advising technology and media companies, both in commercial and regulatory matters as well as advising on data privacy regulations.

‡ 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.

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 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, managing portfolios etc) 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 new regulatory framework in 2021 for the authorisation and supervision of fintech companies providing third-party services to customers of financial institutions.

This new 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. It is intended that the introduction of the new regulatory framework will encourage more fintech companies to enter the ADGM market and provide innovative new services to customers.

Regulatory and insurance technology

In the wake of Covid-19, financial institutions were forced to move to remote working models, which was 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 engrained 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.

It is worth noting that we have seen traditional insurance companies collaborating with insurtechs to improve their efficiency which is an indicator of the potential and benefits of the insurtech industry.

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 licence 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.
- The service provider must be licensed by the SCA.

DIFC

Having previously excluded crypto assets from the scope of application of issued regulations regarding security tokens and investment tokens, the DFSA issued a consultation paper on the regulation of crypto tokens in early March 2022. The DFSA was influenced by the increase in the use of cryptocurrency as a means for financial transactions. Following this public consultation paper, the DFSA will enact legislation as needed.

ADGM

The FSRA has released a framework in conjunction with its 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.

Dubai World Trade Centre

The Virtual Assets Law No 4/2022 (VAL) was issued whereby establishing a framework for the regulation of virtual assets in Dubai and creating a regulatory authority for virtual assets called the

Virtual Assets Regulatory Authority (VARA). While implementing regulations of the VAL have not been issued yet, we anticipate permission for comprehensive cryptocurrency related activities.

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'.

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 has 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.

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 couple of years, many government authorities have shown an increasing interest in fintech. In fact, many initiatives to encourage the emergence of fintech in the UAE has 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 on the contrary, 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 program named the Regulatory Laboratory to encourage cutting-edge fintech solutions for leading financial institutions. Pursuant to this program, 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 program, 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 targeting open banking have expressly been issued. Several regulations can notably be relied on to conclude the UAE's position on open banking. For example, we note 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 AIS and PIS 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.

Europe

France

Jean-François Adelle*
Jeantet AARPI, Paris
jfadelle@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 (assurtech), 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) and 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);
- Regulation on e-marketing, hawking and distance delivery of financial services (Articles L341-1 to L343-2 of the Monetary and Financial Code);
- 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);

* Jean-François is a finance partner of Jeantet AARPI. He serves as Co-Chair of the Banking Law Committee of the IBA and is a member of the PRIME Finance panel of experts. His practice covers general and structured debt finance transactions, regulatory advice related to credit disintermediation and fintechs, and litigation relating to financial arrangements.

- 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, GDPR).

Further regulation is being contemplated, namely:

- The Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937;
- 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;
- 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).

Soft law regulation also complements the above laws.

As regards artificial intelligence (AI), a regulation in this regard that would further complete the contemplated EU Proposal 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 Prudential Control and Resolution Authority (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, tokens and other digital assets, both of which exclude financial assets that are regulated by other regimes, such as financial securities.

Tokens are defined by article L552-2 of the Monetary and Financial Code as 'intangible assets' representing, in digital form, one or more rights that can be issued, transferred or stored by means of a shared electronic device making it possible to identify directly or indirectly the owner of said property.

The legal nature of the intangible property token refers to a clear notion of civil law, putting an end to previous uncertainties. Since the represented rights are neither enumerated nor defined, they may therefore be any type of rights of shareholder, partner, lender, user or creditor rights, or unnamed rights or any combination of these rights. They therefore cover:

- utility tokens which give access to services or products offered by the issuer or a third party (utility tokens);
- tokens representing the ownership of underlying assets, in particular non-fungible tokens (NFT) which represent all kinds of digital assets, digital land, etc;
- tokens conferring political or economic rights such as the right to dividends or the right to appoint governance bodies (security tokens).

They escape the specific regime of digital assets to fall under the law of financial securities.

The Pact Law provides for the legal framework for the issuance of utility tokens. The applicable regimes are built on that applicable to financial instruments. Issuers may apply for an optional visa from the *Autorité des Marchés Financiers* (AMF), which is a label of the seriousness and quality of the offer, or, subject to a warning before the realisation of the initial coin offering (ICO) indicating that the operation presents financial risks. The AMF publishes the list of ICOs that have received its approval.

Other digital assets are defined as any digital representation of value that is not issued or guaranteed by a central bank or public authority that is not necessarily attached to a legal tender and does not have the legal status of a currency, but is accepted by natural or legal persons as a means of exchange and can be transferred, stored or exchanged electronically.

This category mainly covers cryptocurrencies, which also use blockchain technology, and make it possible to directly or indirectly identify the owner of the property, but are excluded from the category of tokens and do not have the legal status of currency, not being issued by a central bank and not being a legal tender.

Unlike tokens, these assets are considered as intangible assets, in accordance with case law of the Council of State issued before the entry into force of the Pact Law, regarding the legal qualification of Bitcoin.

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 approval from the AMF. This approval is optional. It entails more stringent obligations. Only DASPs approved by the AMF have the right to solicit new customers in France. CFDs on crypto assets may only be marketed by a service provider approved as an investment services provider.

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 approved 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 approval as a payment institution 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 700 companies totalling 30,000 jobs, and is expected to create more than 10,000 additional jobs in 2022.

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 and 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 approval of 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.

On its part, 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, provides 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 approved 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. 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.

Germany

Christian Schmies*
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* – KWG) and the German Investment Institution Act (*Wertpapierinstitutsgesetz* – 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* – ZAG) and the management of investment funds is regulated under the German Capital Investment Code (*Kapitalanlagegesetzbuch* – 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 crypotcurrencies, 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:

---

* 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 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* – eWPG). In addition, operators of the cryptocustody business 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* – 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 (Anti-Money Laundering Directive – AMLD) and, therefore, closely mirror the European template, German lawmakers have recently 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.

In recent times – 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 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) will substantially affect 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, will become subject

to an EU-wide licence and ongoing prudential and good conduct requirements. In contrast to today's national regulation, this licence could 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 ZAG. 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 2021, there were 83 companies domiciled in Germany with a licence for payment services or e-money business. CRR credit institutions 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 of 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.

Italy

Alessandro Portolano*
Chiomenti, Milan
alessandro.portolano@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 the 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 of course to the area that has 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 – ie, 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 not adopted a specific and comprehensive legislation governing alternative finance activities. The competent authorities are the Bank of Italy and the National Commission for Companies and the Stock Exchange (CONSOB).

Italy has arguably been the first European Union Member State to provide a specific regulation for equity crowdfunding (namely, 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 (EU Regulation), with the aim to harmonise the different EU jurisdictions and to introduce a common framework for all crowdfunding platforms operators.

The Italian provisions of law governing those new rules have not yet been issued. Below are the most relevant areas in which the EU Regulation affects the domestic crowdfunding provisions.

* 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.

Lending-based crowdfunding activities

In Italy, the performance of lending-based crowdfunding activities and the activity on the platform by borrowers and lenders may require specific authorisation (or be freely lent), depending on the manner in which they are performed.

The EU Regulation profoundly affects this setup, as it makes (1) the activity of providing of funding and of potential financed parties on the platform a free activity (not subject to any prior authorisation), and (2) the activity of the platform an activity reserved to persons authorised under the Regulation.

Lenders

According to the domestic legal regime being in force before the EU Regulation, lenders which lend to the public (ie on a professional basis and *vis-à-vis* third parties), must be authorised to carry out the activity of granting loans under Article 106 of the Consolidated Banking Act (ie be banks or financial intermediaries). Therefore, the platforms provide for maximum limits on the amount that an individual lender may disburse in a given period of time.

The new Regulation provides that Member States may not require potential investors to obtain prior authorisation in order to lend via a crowdfunding platform. Under the new legal framework, (1) lenders will not necessarily need the relevant authorisations to operate on a platform in a professional manner; and (2) platforms will no longer provide for maximum limits to the amount disbursable by each investor. While it will be necessary to analyse the legislation which will adapt the Italian framework, this change is likely to generate a particularly relevant impact in Italy.

The project owner (the borrower)

According to the domestic provisions, borrowers are (except in special cases) subject to the special legal regime regulating the activity of collecting savings from the public pursuant to Article 11 of the Italian Banking Law (TUB). The Bank of Italy has, however, specified that the operation of the borrower does not require the aforementioned authorisation if the loan is granted as a result of individual negotiations. Moreover, the Authority (the Bank of Italy) has recommended that the platforms define a maximum limit on the funds that may be borrowed through such platforms in order to limit the activity of collecting funds from the public by non-bank entities.

The new Regulation, in turn, requires that borrowers are not subject to prior authorisation. The limits on maximum financeable amount (€5m) will still apply. The EU Regulation, however, excludes from the category of potential borrowers: (1) persons who seek borrowing outside the scope of their professional activity (ie consumers); and (2) persons applying for financing in an indirect form, in particular through the assignment of credits.

The impact of such new provisions on the domestic legal regime will likely be that the conditions dictated by the Bank of Italy in order not to fall under the reservation provided under Article 11 of TUB (in particular, the need for individual negotiations), will no longer apply. Invoice trading platforms and peer-to-peer lending for consumers should, however, continue to be subject to the regulations applicable to date in the absence of subsequent regulatory adaptations. Again, while the details of the new changes will have to be further analysed, this will be a major change in the Italian regulatory landscape.

The current Italian legal regime provides that the activity of managers of peer-to-peer platforms is considered to be reserved to specific entities if banks and financial intermediaries are included among the lenders.

The activity, which consists of 'bringing together banks or financial intermediaries with potential customers for the granting of financing in any form whatsoever', is in fact reserved to credit brokers. The platform operator must also refrain from managing payment flows as this activity is reserved to entities authorised to provide payment services under the second EU Payment Services Directive (PSD2). As the new EU Regulation introduces a specific authorisation for platform operators, regardless of the nature of lenders, it is no longer possible for platform operators to carry out this activity without any authorisation and without being subject to specific regulation, as well as under supervision by the competent authorities.

Investment-based crowdfunding

In contrast to lending-based crowdfunding, investment-based crowdfunding is an activity regulated primarily at the European level. Equity-based crowdfunding, to the extent that it concerns securities and, more generally, financial instruments, consists in the provision of an investment service. Therefore, this activity falls within the scope of application of the second EU Markets in Financial Instruments Directive (MiFID II) and is reserved to persons who, in accordance with this Directive, are authorised to provide investment services.

Article 3 of MiFID II, however, allows Member States to exempt from the application of MiFID II people who provide the service of reception and transmission of orders in relation to transferable securities and/or units of undertakings for the collective investment in transferable securities (UCITS), subject to certain conditions.

In recent years, a special legal regime in force in Italy allowed entities that are not authorised to provide investment services to offer the investment-based crowdfunding services, provided that they are authorised as portals for the online collection of capital, pursuant to Article 50-*quinquies* of Legislative Decree No 58/1998 (The Italian consolidated Law on Finance or TUF), and the corresponding implementing regulation of Consob No 18592 of 26 June 2013 (Consob Regulation).

Following the entry into force of these new regulations, a dual track has been created for the provision of the investment-based crowdfunding services. In particular:

- portals authorised pursuant to Article 50-*quinquies* of TUF are required to provide such services in accordance with the rules laid down in the aforementioned provisions and their implementing rules; and
- people authorised to provide investment services corresponding to those involved in the operation of the crowdfunding portal (placement or reception and transmission of orders) – the so-called 'managers by right' – may provide such services in accordance with the rules dictated by MiFID II and the corresponding implementing regulations.

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

Under the Italian regulatory framework, crypto assets are not subject to any specific regulatory framework, except for anti-money laundering regulation.

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 TUF. It includes: 'financial instruments and any other form of investment having financial nature'.[2]

By implementing Directive 2018/843 (AMLD 5), the 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). The 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', including 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 a number of obligations, including obligations concerning customer due diligence, record-keeping, reporting of suspicious transactions and other requirements linked to the AML/CFT risk prevention.

Furthermore, Italy has recently introduced a special domestic registration framework for entities providing services related to virtual currencies in Italy, also through digital means. More specifically, Legislative Decree No 90/2017 amended Legislative Decree No 141/2010 by introducing, in Article

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 the MiFID II and the Italian Consolidated Financial Act and, therefore, is reserved to duly licensed entities (eg, investment companies, 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.

3 Legislative Decree 90/2017.

17-bis, paragraph 8-bis, the obligation for virtual asset service providers (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 (OAM – Organismo Agenti e Mediatori), and be supervised by Guardia di Finanza. By virtue of paragraph 8-ter of the same article, the Italian Treasury then 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]

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 important changes over the last decade, particularly regarding the regulation of the entities authorised to provide payment services. As it is well known, 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, on the one hand, and of Directive No 2009/110/EC, on the other, Title V-bis (dedicated to the Electronic Money Institutions), and Title V-ter of TUB (concerning Payment Institutions) were introduced into the TUB.

Lastly, with the transposition of Directive No 2009/110/EC, Title V-bis of TUB was further amended, aligning the electronic money institutions (EMIs) discipline 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, which usually is 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 emoney 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.

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, 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 will result in any activity being considered abusive. Among the requirements for registration of entities other than individuals is to have a registered and administrative office in Italy or, for EU entities, a permanent establishment in the territory of the Republic.

If digital wallets are used, PSPs will have to apply the security standards provided for in the 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.

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 at creating 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. In order 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, admissible corporate structures).

Access to the sandbox depends on meeting some 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 would like to test a particular activity subject to authorisation or registration in any list kept by one of the supervisory authorities, or who would like 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.

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, in order to ensure that 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. 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

* 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.

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 guideline

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 (ecommerce), 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 intial 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, in 2023, new regulatory opportunities are expected to be introduced, such as the Markets in Crypto-Assets Regulation (MiCA). According to the current proposal, MiCA is to apply to all people who want to issue crypto assets or provide services related to crypto assets in the EU. The MiCA proposal is intended to lay down uniform rules on transparency and disclosure requirements for the issuance, offer to the public and the admission to trading of crypto assets. In addition, there are rules on the authorisation and supervision of crypto asset service providers and their issuers. The main focus lies with the issuers of asset-referenced tokens and e-money tokens. The Regulation intends to regulate the operation, organisation and governance of issuers of asset-referenced tokens and emoney tokens, and crypto asset service providers. There will also be investor protection rules for the issuance, trading, exchange and custody of crypto assets. In addition, measures to prevent market abuse are to be included in the Regulation to ensure the integrity of the crypto assets markets.

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. Furthermore (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.

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.
- 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 also decided to develop the PSD2 API in accordance with the Berlin Group standard that will enable access to customer data for all participants.

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.

For the time being there is no single comprehensive piece of legislation that governs the fintech area in Poland. Regulations in this respect are scattered over 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 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 as well as 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, but also 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 also Question 3.

---

* Krzysztof is a partner at Wardyński & Partners, where he leads the new technologies 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 the 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 such providers to obtain a licence in order to pursue crowdfunding business in the EU. Such providers will be supervised by the Polish Financial Services Authority (FSA).

Artificial intelligence (AI)

In April 2021, the European Commission published a proposal for an EU-level Artificial Intelligence Act.[5] The proposal focuses mainly on risks associated with AI and their mitigation by way of enhancing accountability and transparency of such systems. Depending on a risk classification of a specific AI system, different obligations connected with deployment and use of such AI system will apply. The regulation is not expected to enter into force before the second half of 2024.

Cloud computing

At present, there is no single piece of legislation which would regulate 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).

Cloud computing is also garnering increased interest on the EU level. In July 2021, the European Commission launched the European Alliance for Industrial Data, Edge and Cloud which will feature

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 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.

the development of the EU Cloud Rulebook. Other initiatives on the EU level include works on standard cloud service level agreements (SLAs).

Digital ID

At present, the basis for electronic identification, authentication and certification is set out in the eIDAS Regulation.[6] 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 EDIR Regulation,[7] 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.

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. There are, however, certain EU-level regulatory developments underway relating to harmonisation of the crypto assets legislation. For further details, see Question 2.

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 the 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 where 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.

6 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.

7 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.

8 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.

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). In accordance with last year's changes to the AML Act (resulting from the implementation of the AMLD V[9] to the Polish legal system), entities rendering VASPs 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;
- 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 one substantive piece of legislation that is being worked on in the EU level – MiCA.[10] MiCA's objectives are to harmonise the EU crypto assets market and ensure a high level of consumer protection. MiCA will introduce a new category of market players – crypto assets service providers (CASPs) – and impose 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 planned to be complemented by changes to the EU AML framework, which will expand 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, are expected to benefit from the DLT Pilot Regime.[11] The DLT Pilot Regime is

9 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.

10 Proposal for a Regulation of the European Parliament and of the Council on markets in crypto assets, and amending Directive (EU) 2019/1937.

11 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.

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 the PSD2 and the E-Money Directive into the Polish legal system.

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 case). In order 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 his/her 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 Sp. z o.o.

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 in order 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 in order 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 the 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 the 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 the 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.

Spain

José Canalejas*
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 the last 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 our 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 2021, the Spanish Government adopted a draft of a law to promote the startup ecosystem, currently being processed by the Spanish Parliament. After the approval of the mentioned startup law, important measures and incentives will promote the competitiveness of the Spanish economy even more, 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. Mr Canalejas 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.

Crypto assets are not explicitly regulated in Spain except for the measures adopted 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 shall 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 does not imply a modification of book entry form requirements applicable in Spain, the Spanish government recently adopted a draft of a new law on securities markets, currently being processed by the Spanish Parliament. After the approval of such new securities markets law, certain questions will be clarified, and new private law provisions will apply 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 and the Spanish Finance Ministry has also published a draft 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 this form has not yet been approved and there is a disclosure obligation.

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 proceed to do 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.

The EBA recently published an Opinion and Report in response to the European Commission's Call for Advice on the review of PSD2. EBA's proposals aim to enhance competition, facilitate innovation, protect consumers' funds and data, foster the development of user-friendly services, and prevent exclusion from access to payment services, as well as ensure a harmonised and consistent application of the legal requirements across the EU.

According to EBA, it may be convenient to implement further measures 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'.

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 has to 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 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. According to new legislation, which is expected to come into effect in July 2023, the Federal Government will be able to exempt innovative insurance companies in whole or in part from supervision by means of an ordinance.

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 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 (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.

Regarding cryptocurrencies, the Federal Government attaches great importance to ensuring that the same rules apply to crypto currencies 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.

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 in particular 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 in particular 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 under 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.

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 BA stipulates inter alia that, if settlement of the received funds 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 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). Furthermore, 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 start-ups 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 especially to coordinate and facilitate frameworks and standardise technical interfaces while other financial institutions voluntarily offer application programming interface (API) services.

Turkey

Halide Çetinkaya*
Çetinkaya Taktak Semiz Baltalı Yörükoğlu Avukatlık Ortaklığı (CCAO), İstanbul
halide.cetinkaya@ccaolaw.com

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

In Turkey, while there are currently no laws addressing to fintech as a whole, several laws and regulations set forth provisions related to the usage of technologies in financial services. The most relevant laws and regulations are listed below.

Bank cards and credit cards: Bank Cards and Credit Cards Law No 5464 (Bank Cards Law)

The Bank Cards Law regulates the principles and procedures applied to the issuance and use of bank cards and credit cards, as well as the functioning of the card payments system. The law sets forth detailed provisions on obtaining an operating permit for institutions wishing to provide card services, issuance of cards, obligations of institutions issuing credit cards, agreements with the workplaces where payment can be made with cards, etc. The Regulation on Bank Cards and Credit Cards expands on the obligations and requirements set forth in the Bank Cards Law.

Amendment to Article 76 of the Banking Law No 5411

The amendment to the second paragraph of Article 76, titled 'Customer Rights', of the Banking Law No 5411 (Banking Law), enables customers, regardless of whether they are retail or commercial, to become bank customers through remote access without visiting bank branches. With this amendment, agreements between banks and customers may be concluded in writing or online through remote communication tools, or through other methods determined by the Banking Regulation and Supervision Agency (BRSA) as a substitute for the written form. This may be performed through an information or electronic communication device. The Regulation on the Methods to be Used by Banks to Confirm Identities Online and Establishment of Contractual Relationships in Electronic Environments issued by the BRSA provides additional rules and principles in this regard.

Payment systems: Law on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions No 6493 (Law No 6493)

This law regulates the principles and procedures related to the payment systems to be used during the provisions of payment services. Law No 6493 provides rules for system operators and obtaining

* Halide has 20 years of experience in M&A, private equity, banking finance and acquisition finance with a particular focus on the finance, insurance, healthcare and energy sectors. She has been an IBA Banking Law Committee member since 2012.

of operating permits from the Central Bank of the Republic of Turkey (CBRT), supervision of the payment systems by the CBRT, relevant measures to be taken by the system operators, transfer orders, netting, collaterals and designation of the payment systems.

The Regulation on Operations of Payment and Securities Settlement Systems (Payment Systems Operations Regulation), the Regulation on Oversight of Payment and Securities Settlement Systems (Payment Systems Oversight Regulation) and the Communiqué on Information Systems Used in Payment and Securities Settlement Systems (Payment Systems Communiqué), are secondary legislations related to payment systems that expand on the rules and provisions set forth by Law No 6493. Please see Question 3 for more information.

Payment services

Payment services are regulated by Law No 6493 and its secondary legislation issued by the CBRT. Law No 6493 sets forth definitions, rules and principles for the provision of payment services, payment service providers, payment and electronic money institutions, issuance of electronic money, operating permits to be obtained by such institutions from the CBRT, supervision of the payment services and payment service providers by the CBRT.

Secondary legislation regarding the payment services area is:

- the Regulation on Payment Services and Electronic Money Issuance and Payment Service Providers (Payment Services Regulation);
- the Regulation on the Generation and Use of TR QR Code in Payment Services (QR Code Regulation);
- the Regulation on the Non-Use of Crypto Assets in Payments (Crypto Regulation);
- the Communiqué on the Management and Supervision of the IT Systems of Payment and Electronic Money Institutions and the Data Sharing Services of Payment Service Providers in Payment Services Area (Payment Services Communiqué); and
- the Communiqué on the International Bank Account Number (International Account Communiqué). Please see the answer to Question 3 for more information.

Crypto assets

While it is not clear whether crypto assets are considered as a security or currency in Turkey, the Crypto Regulation prohibits the use of crypto assets as payment instruments and the provision of services for the direct or indirect use of crypto assets in payments. However, this prohibition does not apply to all crypto assets due to the exceptions provided in the Crypto Regulation.

A new bill proposed before the Turkish Grand National Assembly in 2021 (the Draft Bill) is expected to enter into force after the elections in June 2022. The Draft Bill provides additional termination, principles and rules regarding crypto assets.

Since the Capital Markets Board is the regulatory authority for crypto assets, the qualification of crypto assets seems to be a form of security. In addition, crypto asset service providers are also included in the scope of the Regulation on Prevention of Laundering Proceeds of Crime and Financing of Terrorism and therefore the regulations of Financial Crimes Investigation Board. Please see Question 2 for more information.

Open banking

The amendment 22 dated November 2019, to Law No 6493 (the Amendment) included the services of 'initiating a payment order' and 'providing account information' as payment services in the Turkish legislation.

The CBRT was authorised by the Amendment to regulate the sharing of data from one payment service provider with another payment service provider within the scope of payment order initiation and account information provision services as defined in Law No 6493. Accordingly, the CBRT issued the Payment Services Communiqué governing the sharing of information.

In addition, the definition of open banking services and the rules and principles regarding the provision of open banking services were issued by the BRSA with the Regulation on Information Systems and Electronic Banking Services of Banks (Electronic Banking Services Regulation).

The Regulation on the Operating Principles of Digital Banks and Banking as a Service Model (Digital Banks Regulation) issued by the BRSA – published in the Official Gazette dated 29 December 2021 and numbered 31704 – regulates the service model banking as a form of open banking to be provided by digital banks.

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

With the Crypto Regulation issued by the CBRT, published in the Official Gazette dated 16 April 2021 and numbered 31456, crypto assets have been defined for the first time in Turkish law, albeit with a secondary regulation.

According to the Crypto Regulation, crypto assets are 'intangible assets which are created artificially by using distributed ledger technology or another similar technology and distributed through digital networks, however not qualified as fiduciary money, representative money, electronic money, payment instrument, security or other capital market instrument'.

Section 3 of the Crypto Regulation prohibits the use of crypto assets in payments either directly or indirectly, and the provision of services towards such purposes. Section 4 of the Crypto Regulation prohibits payment service providers from developing business models which directly or indirectly use crypto assets in the provision of payment services or issuance of electronic money, and from providing any services related to such business models. In addition, payment and electronic money institutions are banned from acting as intermediaries to platforms providing purchase, custody, transfer or issuance services related to the crypto assets and to fund transfers made through such platforms.

However, such restrictions do not apply to all crypto assets due to the definition of 'crypto assets' provided in the Crypto Regulation excluding 'fiduciary monies, representative monies, electronic monies, payment instruments, securities or other capital market instruments'. Therefore, in theory, if a crypto asset is legally qualified as one of the abovementioned exceptions, the prohibitions set forth in the Regulation will not be applied.

In this regard, there are no legal provisions in Turkish law explicitly qualifying crypto assets as fiat money, representative money or payment instruments. With regard to the possibility of crypto assets being qualified as electronic monies, Section 3 of Law No 6493 defines electronic money as a monetary value issued in return for funds accepted by the electronic money issuer, stored electronically, used to perform the payment transactions stipulated in Law No 6493 and accepted as a payment instrument by real and legal persons other than the electronic money issuer. Law No 6493 also requires electronic money issuers to obtain a permission from the CBRT.

Therefore, for Bitcoin to be qualified as electronic money, it must first be issued by an institution authorised to issue electronic money under Law No 6493 and in exchange for a fund. However, Bitcoin is not issued by an institution authorised to issue electronic money and against a fund. Therefore, as stated in the BRSA press release dated 25 November 2013, Bitcoin and other cryptocurrencies are outside the scope of application of Law No 6493 as they cannot be considered as electronic money in terms of their current structure and functioning.

However, the Payment Services Regulation stipulates that asset-backed crypto assets (stablecoins) issued against one-to-one fiat money shall be considered as 'electronic money' if they are issued, stored, used for payment transactions and accepted as payment instruments by the issuing institutions. With this regulation, such crypto assets are included within the scope of Law No 6493.

Likewise, the Capital Markets Board does not qualify crypto assets as securities due to the definition of 'security' provided in the Capital Market Law No 6362, which requires a security to be based on an actual asset. There is also no stipulation qualifying crypto assets as other capital market instruments.

However, the Draft Bill has been proposed before the Turkish Grand National Assembly in 2021. The Draft Bill has the same definition of crypto assets as the Crypto Regulation, save for the exceptions. The Draft Bill also defines the terms 'wallet', 'crypto asset purchase platform', 'crypto asset custody service' and 'crypto asset service provider'. The voting on the Draft Bill is expected to take place after the new elections in June 2022. According to the Draft Bill:

- purchase of crypto assets may only be conducted through platforms which obtain permission from the Capital Markets Board;
- the Capital Markets Board will be authorised to issue legislations on the purchase of the crypto assets;
- crypto asset custody services will be provided by banks or other institutions authorised by the Capital Markets Board and approved by the BRSA;
- shareholders, board members and representatives of the platforms will be required to meet the conditions set forth in the Draft Bill;

- crypto assets owned by the platforms' customers will be monitored separately from the assets of the platforms and such assets cannot be made subject to attachments and pledges due to the debts of such platforms;
- agreements to be made between the platforms and the customers regarding the purchase of crypto assets will be made in writing or online, and the Capital Markets Board will be authorised to determine the principles regarding such agreements;
- crypto asset service providers will have first-degree responsibility for the default, cyber-attacks, technical failures, and operational mistakes;
- capital market instruments may be issued as crypto assets; and
- customers can transfer their crypto assets only to other platforms. The platforms will be working on a closed-circuit basis and there will be no transfers to the personal wallets.

On 1 May 2021, a regulation was issued in Turkish law in line with the Financial Action Task Force (FATF) and International Organization of Securities Commissions (IOSCO) recommendation report. Accordingly, crypto asset service providers were also included in the scope of the Regulation on Prevention of Laundering Proceeds of Crime and Financing of Terrorism. Following this, on 4 May 2021, the Financial Crimes Investigation Board (MASAK) under the Ministry of Finance and Treasury in Turkey published a guideline detailing the obligations of crypto asset service providers in accordance with the relevant legislation.

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

Payment service providers and digital wallets are mainly regulated with Law No 6493 and its secondary legislation.

Prior to the Amendment, the authority responsible for the regulation and supervision of the payment services systems was the BRSA. With the Amendment, such authority has been passed to the CBRT as of 1 January 2020.

Pursuant to Law No 6493, payment services must be performed through payment systems, consisting of a set of instruments, procedures and rules which facilitate the transfer of funds or securities among their participants and operated by payment system operators authorised by the CBRT. Due to this requirement, the payment service providers must firstly participate in payment systems in order to provide relevant payment services.

In Turkey, payment systems are regulated by Law No 6493 and the following secondary legislations: the Payment Systems Operations Regulation, the Payment Systems Oversight Regulation and the Payment Systems Communiqué.

According to the legislation, in order to be a payment system, a structure should (1) contain at least three participants, (2) provide an infrastructure through which funds circulate in an electronic environment and (3) have common rules. Bilateral structures established by two institutions that operate in financial markets among themselves, structures which only provide messaging services

among members but do not engage in any clearing or settlement activity regarding transactions within those messages and structures that an institution establishes within itself to conduct funds or securities transfer transactions on behalf of itself or of its clients are not considered payment systems.

In order to be accepted as system operators, institutions must obtain a permit from the CBRT. System operators and their managers must meet several criteria set forth in the legislation. The legislation also sets forth several requirements for system operators related to issues such as risk management, information technologies, confidentiality, transparency, website, backups, emergency plans, independent audit, etc. In Turkey, current payment and settlement systems and their authorised operators are as follows:

- Payment and securities settlement systems operated by the CBRT:
    - Electronic Fund Transfer System (EFT):
        - Turkish Lira Interbank Payment System;
        - Turkish Lira Customers Payment System;
    - Electronic Securities Transfer System (ESTS); and
    - The Instant and Continuous Transfer of Funds (FAST) System;
- Payment and securities settlement systems licensed by the CBRT:
    - Interbank Card Center (BKM) – Domestic Clearing and Settlement System;
    - Istanbul Clearing, Settlement and Custody Bank Inc (TAKASBANK):
        - Equity Market Clearing System;
        - Debt Securities Market Clearing System;
        - Takasbank Cheque Clearing System;
    - Central Registry Agency (MKK) – Central Registry System;
    - Garanti Payment Systems Inc (GÖSAŞ) – Takasnet System;
    - Paycore Payment Services Clearing and Settlement Systems Inc (Paycore) – Paycore Clearing System; and
    - Bileşim Financial Technologies and Payment Systems Inc (Bileşim Inc) – TAM Clearing Settlement System.

In order to participate in a payment system, a payment service provider must sign a written agreement with the relevant system operator. The payment service provider must also comply with the system rules determined by the relevant system operator.

As stated above, when Law No 6493 first entered into force in 2013, the regulation and supervision responsibility for 'payment services', 'payment service providers', 'payment institutions' and 'electronic money institutions' was given to the BRSA, while the regulation and oversight responsibility for 'payment systems' and 'securities settlement systems' was given to the CBRT.

With the Amendment, the responsibilities given to the BRSA passed to the CBRT as of 1 January 2020. In this regard, the secondary legislation issued by the CBRT in relation to the payment services are (1) the Payment Services Regulation, (2) the QR Code Regulation, (3) the Crypto Regulation, (4) the Payment Services Communiqué and (5) the International Account Communiqué.

Law No 6493 and its secondary legislation follows the European Union's Payment Services Directive and developments made in the European Union in this regard. In fact, Turkey is one of the first countries outside of the EU implementing EU regulations related to payment services.

According to the Turkish legislation, the following services are considered as payment services:

- all transactions required for operating a payment account, including the services enabling cash to be placed on and withdrawn from a payment account;
- execution of payment transactions, including transfers of funds on a payment account with the user's payment service provider, direct debits, including one-off direct debits, payment transactions through a payment card or a similar device, credit transfers including standing orders;
- issuing or acquiring payment instruments;
- money remittance;
- execution of payment transaction, where the consent of the payer to execute a payment transaction is given by means of any telecommunication, digital or IT device and the payment is made to the telecommunication, IT system or network operator, acting only as an intermediary between the payment service user and the supplier of the goods and services;
- corresponding services enabling bill payments;
- at the request of the payment service user, the payment initiation service related to the payment account at another payment service provider;
- upon approval of the payment service user, the online provision of consolidated information of one or more payment accounts held at payment service providers by payment service users; and
- other transactions and services reaching the level to be determined by the CBRT in terms of total size or impact in payments.

The following services are not considered as payment services:

- payment transactions made in cash directly from payer to payee, without any intermediary intervention;
- payment transactions from payer to 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;
- payment transactions consisting of cash collection and delivery within the framework of a non-profit or charitable activity;
- services where cash is provided by the payee to the payer as part of a payment transaction following an explicit request by the payment service user just before the execution of the payment transaction through a payment for the purchase of goods or services;

- cash to cash in foreign exchange operations, where the funds are not held on a payment account;
- payment transactions based on valuable papers, foreign bank cheques, traveller's cheques and paper-based postal money orders within the scope of the Turkish Commercial Law No 6102;
- payment transactions executed by the CBRT, settlement institutions, central counterparties, clearing houses, payment service providers and other participants of the system on behalf and account of their own in the systems;
- payment transactions regarding capital markets activities under Capital Market Law No 6362 performed by the legal persons and capital market institutions designated in the above paragraph;
- services provided by technical service providers, without them coming into possession of the funds to be transferred at any time, to support the provision of payment services, and include processing and storing data, trust and privacy protection services, data and entity authentication, information technology (IT) and communication network provision, provision and maintenance of terminals and devices used for payment services;
- services based on instruments that can be used to acquire goods or services only on the premises used by the issuer or under a commercial agreement with the issuer either within a limited network of service providers or for a limited range of goods or services;
- payment transactions executed by means of any telecommunication and IT device, where the goods or services purchased are delivered to and are to be used through a telecommunication and IT device, provided that the telecommunication and IT operator does not act only as an intermediary between the payment service user and the supplier of the goods and services;
- payment transactions carried out between payment service providers, their agents or branches on their behalf and on their own account;
- payment transactions between a parent undertaking and its subsidiary, or between subsidiaries of the same parent undertaking, without any intermediary intervention by a payment service provider other than an undertaking belonging to the same group; and
- services by providers to withdraw cash by means of automated teller machines (ATMs) acting on behalf of one or more card issuers, which are not a party to the framework contract with the customer withdrawing money from a payment account and do not conduct any payment services.

Pursuant to Section 13 of Law No 6493, the institutions that are eligible to provide payment services and thus are considered as payment service providers are:

- the banks operating within the scope of the Banking Law;
- payment institutions;
- electronic money institutions; and
- the Postal and Telegraph Corporation.

Among such institutions, banks and the Postal and Telegraph Corporation are not obliged to obtain additional permission from the CBRT in order to provide payment services. Payment and electronic money institutions, on the other hand, must obtain an operating permit from the CBRT in order to provide payment services. The institutions that have obtained operating permits from the BRSA until 1 January 2020 are not required to apply to CBRT for permission. Such permissions remain valid. Also, the electronic money institutions authorised by the CBRT are not required to apply to the CBRT to provide payment services. On the other hand, the payment institutions authorised by the CBRT must obtain an additional permit from the CBRT if they wish to issue electronic money as well.

Only joint stock companies can operate as a payment institution or an electronic money institution. To obtain an operating permit, the institutions must meet the requirements set forth in the legislation relating to capital, founders, shareholders and managers qualifications, organisation and so on. The applications for the operating permit must be made according to the Payment Services Regulation together with the documents stated therein. The payment and electronic money institutions must also become a member of the Payment and Electronic Money Institutions Association of Turkey. The Statute of the Payment and Electronic Money Institutions Association of Turkey was published in the Official Gazette dated 28 June 2020 and numbered 31169. The association is a public professional organisation having a legal personality.

In Turkey, there are currently 30 payment institutions and 42 electronic money institutions which have obtained an operating permit from the CBRT.

Payment and electronic money institutions cannot extend loans to their customers and can operate only within the scope of their operating permit. All payment service providers are subject to the CBRT's supervision regarding their activities within the scope of Law No 6493. In addition, share transfers of payment and electronic money institutions are subject to the CBRT's permission.

The Payment Services Regulation imposes detailed obligations to the payment and electronic money institutions regarding the corporate governance, internal control, risk management, accounting, reporting, independent audit, continuance plans, information technology systems, equity, protection of funds and collateral matters. The Payment Services Communiqué also imposes additional requirements regarding the information technology systems and sharing of information. The QR Code Regulation, on the other hand, requires the payment service providers to use a TR QR Code in each payment transaction realised using a QR code.

Payment service providers must sign a framework contract with their customers prior to providing payment services. The contract must be made in writing or online and must contain the minimum content stated in the Payment Services Regulation. There are also requirements to inform customers prior to signing contracts and providing services.

The International Account Communiqué allows payment service providers to open and use international bank accounts in providing 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.

The Technology and Innovation Support Programs Directorate (TEYDEB) of TÜBİTAK, which continues its activities in line with the science, technology and innovation policies of our country, supports the research-technology development and innovation activities of private sector organisations.

Among the applications for R&D incentives allocated by TEYDEB to private sector enterprises, the software industry ranks first with a share of approximately 30 per cent. Fintech projects have been one of the most important agenda items in the software category in the recent years.

In the *Investigation Report on Financial Technologies in Payment Services* prepared by the Competition Authority, it was underlined that the design of regulations and government policies for the fintech ecosystem to eliminate market dynamics that make it difficult to enter the market is also important for the establishment of a competitive structure, and it was suggested that various financing methods should be adopted on behalf of small and medium-sized enterprises, especially by clarifying the programs for public capital support.

In addition, the Financial Centre Law No 7412 provides tax incentive schemes and a regime for financial institutions operating within the financial centre by providing a reduction in corporate income tax, exclusion from banking and insurance transaction tax, exclusion from duties and stamp tax for financial service exports, a reduction in employee income taxes, exclusion from duties and stamp tax for rental agreements within the centre.

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

The 11th Development Plan, covering the 2019–2023 period and published in the Official Gazette dated 23 July 2019 and numbered 30840 (bis), lists harmonisation of legislation with the second EU Payment Services Directive (PSD2) as one of the planned actions to strengthen the legal infrastructure for open banking.

Accordingly, in parallel with the developments in PSD2, the scope of payment services was expanded by an Amendment by defining two new payment services. In this framework, the following services are considered as 'payment services' subject to the supervision of the CBRT:

- At the request of the payment service user, the payment initiation service related to the payment account at another payment service provider.
- Upon approval of the payment service user, the online provision of consolidated information of one or more payment accounts held at payment service providers by payment service users.

Thus, the services of 'initiating a payment order' and 'providing account information' have been included in the Turkish legislation as similar services to those in PSD2. The Payment Services Regulation, which came into force after the Amendment, also set forth additional detailed provisions

and requirements regarding these services, such as access rules for the payment account and information during the provision of such services, responsibilities arising from the non-realisation or false or delayed realisation of the payment, provision of information to the receiver etc.

With the Amendment and the Payment Services Regulation, the CBRT was authorised to regulate the sharing of data from one payment service provider with another payment service provider within the scope of payment order initiation and account information provision services. Accordingly, CBRT issued the Payment Services Communiqué regulating several issues such as risk management, operation of information technology systems, continuance plans, information security, inspections, electronic certificates, identity confirmation as well as data sharing services.

Other steps in Turkey were taken by the BRSA in line with the developments in the European Union regarding open banking.

The Electronic Banking Services Regulation, published by the BRSA in the Official Gazette dated 15 March 2020 and numbered 31069, defined 'open banking services' for the first time and accepted open banking services as a form of electronic banking service. According to the definition, 'open banking services' refers to an electronic distribution channel through which customers or parties acting for and on behalf of customers may execute banking transactions or may instruct the bank for execution of banking transactions through remote access to financial services offered by the bank via such methods as APIs, web services, file transfer protocols, etc. The Electronic Banking Services Regulation generally regulates risk management and control of information technology systems used during the provision of electronic banking services as well as identity confirmation, transaction security, monitoring of transactions and provision of information to the customers.

Another step taken by the BRSA related to open banking was the publication of the Digital Banks Regulation in the Official Gazette dated 29 December 2021 and numbered 31704. The Digital Banks Regulation defines 'service model banking' as 'the service model in which customers can perform banking transactions by directly connecting with the systems of service banks through open banking services, via the interface offered by the interface providers'.

It also defines 'interface providers' as 'businesses established as capital companies that enable their customers to perform their banking transactions by accessing the banking services offered by the service bank through the bank's open banking services via its mobile application or internet browser-based interface'. The Digital Banks Regulation generally regulates the operation principles and operating permits of digital banks as well as principles in banking as a service model.

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

David Verghese§
Slaughter and May, London
david.verghese@slaughterandmay.com

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

There is no single overarching regulatory regime specific to fintech companies in the United Kingdom. Whether a particular fintech company or service will be subject to regulation is determined by whether the relevant underlying activities fall within the 'regulatory perimeter' set out in UK law, including the Financial Services and Markets Act 2000 (FSMA) (and associated secondary legislation); the Payment Services Regulations 2017 (PSRs); the Electronic Money Regulations 2011 (EMRs); and the Consumer Credit Act 1974 (CCA). This legislation sets out a number of 'specified activities' which, subject to a range of tests, exemptions and exclusions, a company must be formally authorised to conduct by way of business in the UK.

Responsibility for financial regulation in the UK (including for fintechs) is split between a number of bodies. Banks, insurers and certain systemically important investment companies designated by the PRA for the purpose are regulated both by the Prudential Regulation Authority (PRA) (in respect of their prudential regulation and supervision) and the Financial Conduct Authority (FCA) (in respect of their conduct of business). The FCA also acts as the sole regulator for all non-PRA regulated companies. The FCA shares responsibility for the regulation of payment companies firms with the Payment Systems Regulator. The Bank of England (BoE) has direct responsibility for regulating financial market infrastructure and for the resolution of failing banks where necessary. Other entities may be involved in the regulation of financial institutions in certain circumstances, such as in relation to financial crime.

---

* 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 standalone 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.

§ David is an associate in the Financial Regulation group at Slaughter and May with experience advising a range of institutions – including banks, brokers and market infrastructure – on regulated activities.

General details of the regimes applicable to certain fintech services are set out below.

Payment services

In general, fintech companies which provide services relating to the transfer of money (including but not limited to money remitters, non-bank credit card issuers and account information service providers) will fall within the regulatory regime set out in the PSRs, and may have to be authorised or registered depending on a number of factors, including size and operating model.

Lending money and taking deposits

Under the UK regime, the key banking activity is the taking of deposits: while banks are permitted to carry out commercial lending (and may, subject to appropriate permissions, carry out regulated consumer credit lending), the performance of that activity does not, unlike deposit taking, require an entity to hold a banking licence.

Deposit-taking is only generally permitted by entities which have been authorised as a bank by the PRA, and which are therefore exposed to the full extent of bank regulation.

It should be noted that recent technological innovations have meant that fintech companies can provide services which have many of the same features as traditional banking services without needing to be authorised as a bank. For example, electronic money ostensibly offers many of the same features as a traditional banking service (ie the creation of an account, the ability to use a balance to pay third parties) without requiring the issuer of that electronic money to be authorised as a bank. While such a company would need to be authorised to issue electronic money, that regime is materially less burdensome than that applicable to banks.

Nonetheless, schemes seeking artificially to disguise banking services as other forms of financial services to evade regulation, especially when involving maturity transformation, are likely to be noticed by regulatory authorities, which adopt a purposive approach to their interpretation of statutes.

Open banking

Open banking refers not to a particular regulated activity but rather to the philosophy of maximising secure access to customers' account information for the purposes of increasing competition and improving consumer outcomes. The UK is considered to be globally pre-eminent in its implementation of this philosophy, with open banking having been encouraged at both governmental and regulatory levels. Under the PSRs, payment service providers are required to permit third parties who are authorised under the PSRs to access relevant account information with much additional requirements relating to how this must be done also provided for under the PSRs.

Buy now pay later

Services which enable consumers to purchase items and then spread the cost over several instalments without interest (so-called 'buy now pay later') are a form of consumer credit which is not presently

included within the regulatory perimeter, as they currently benefit from an exemption from regulation. However, the government is proposing to bring such services within the scope of the regulatory perimeter, it is likely that legislation regulating such services will be set forth in the near future.

Crypto assets

See Question 2.

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

Crypto assets are generally only regulated in the UK for anti-money laundering (AML) purposes – crypto asset exchange providers and custodian wallet providers are required to register with the FCA and comply with a number of requirements regarding the prevention of money laundering through the services the company offers in respect of crypto assets. While this is nominally a registration regime, the FCA has subjected companies applying for such registration to a level of scrutiny more ordinarily associated with full authorisation.

In addition, conducting certain regulated activities in respect of certain crypto assets does bring with it a requirement to be authorised under FSMA, on the basis that the FCA has determined that they constitute specified investments within the regulatory perimeter. Such crypto assets include security tokens (crypto assets with features akin to equities) and e-money tokens (crypto assets which are caught by the definition of electronic money under the EMRs).

It is important for businesses dealing in crypto assets to analyse the features of each crypto asset in respect of which they offer services to determine whether it constitutes a specified investment for these purposes. The separate financial promotions regime imposes restrictions upon how regulated crypto assets are marketed and it is currently proposed that the regime be extended to all crypto assets in due course.

Conventional specified investments which are linked to crypto assets will be regulated by the FCA, which may impose more onerous requirements in relation to such assets. For example, where a specified financial instrument is linked to a crypto asset, it will fall within the general regulatory perimeter.

The regulation of crypto assets is a rapidly developing area which is highly responsive to changes in political leadership and climate; it is likely that more crypto assets (and more related activities) will be brought within the regulatory perimeter in the next couple of years.

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

All entities which provide payment services as a regular occupation or business activity from an establishment in the UK maintained by them or their agent(s) are defined under the PSRs as payment service providers (PSPs). Generally speaking, PSPs will either require authorisation as an authorised payment institution or (where the volume of payments falls below certain thresholds)

registration as a small payment institution.

Payment services are defined broadly (see Question 1 for examples) and are set out fully at Schedule 1 to the PSRs. There are a number of specified exemptions, covering activities including transfers executed wholly in cash, data processing services and payments through certain financial market infrastructure. Banks and certain other largely regulated institutions do not have to be separately authorised to provide payment services.

'Digital wallets' is a broad concept referring to mobile applications whose common denominator is that they store consumer payment information, allowing users to make small payments. Generally speaking, these will also be regulated under the PSRs; however, such wallets can also be used to hold more unconventional assets such as crypto assets, with a consequent additional regulatory overlay. We discuss the regulation of crypto assets in Question 2.

The regulation of payment services is conducted jointly by the FCA and the Payment Systems Regulator. The FCA leads on the majority of provisions set out in the PSRs, with the Payment Systems Regulator responsible for a number of discrete supervisory points.

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 FCA operates a regulatory sandbox programme. Firms accepted into the programme can benefit from a specialised form of authorisation that enables them to test out new financial services and business lines in a controlled and limited way, and to receive certain waivers of especially onerous regulations which would otherwise apply. The regulatory sandbox has accepted cohorts of fintechs annually since 2016, and a number of businesses which began in the sandbox have gone on to considerable commercial success.

Further developing the UK fintech sector is a strategic priority for the British Government. In the first quarter of 2021, the Kalifa Review was commissioned to examine the state of the fintech sector in Britain and to consider ways in which its growth may be encouraged and facilitated. A number of proposals were raised, many relating to financial and practical support for early-stage fintechs. The British government is continuing to consider the Kalifa Review and is likely to implement many of its proposals over the course of the next few years.

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

As discussed in Question 1, the main piece of legislation relevant to open banking as a concept are the PSRs: these do not 'regulate' open banking, given open banking is not a service in itself, but they do provide the framework within which open banking is facilitated.

The PSRs apply to all PSPs involved in the provision of payment services; both account providers and third parties which seek to obtain account information for the purposes of supplying services linked to the overall objective of open banking.

Third parties seeking to access account data for open banking purposes must register as an account information service provider (an entity which aggregates account details such as balances or outgoings and displays them, generally in a user-friendly format) or be authorised as a payment initiation service provider (as appropriate) with the FCA. Their activities are highly regulated to ensure consumer protection, and such third parties are required to obtain informed consent from consumers before any data is shared.

PSPs are required to grant access to authorised (or in the case of AISPs, registered) third parties under the PSRs. The terms of this access are specified in the Retail Banking Market Investigation Order 2017, which sets out the technical details of the APIs to be used to access this data.

Open banking forms a major part of the UK's fintech strategy and is under regular review. In the first quarter of 2022, a joint statement by the major state stakeholders on the future of open banking was issued, and a a joint regulatory oversight committee was set up. This committee continues to meet on a regular basis and is likely to lead to further regulation to assist with the wider rollout of open banking (and open finance more generally).

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.

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,

* 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.

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.

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 exemption. 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 addition, there are certain self-regulatory organisations which have been established to supervise specific areas of the securities market. These include the Investment Industry Regulatory Organization of Canada (IIROC) and the Mutual Fund Dealers Association of Canada (MFDA). Furthermore, the CSA continues to issue new rules and guidance for fintech businesses dealing with cryptocurrencies. Examples of this include, *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.*

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 Regulatory Sandbox can provide exemptive relief to these requirements in specific circumstances (see Question 4).

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 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.

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

Payment service providers

See Question 1. 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'. Any PSP who falls under this definition must register and provide the prescribed information with the Bank of Canada before they begin engaging in retail payment activities. This includes any MSB engaged in retail payment activities. On 11 February 2023, the Department of Finance published the long awaited proposed Retail Payment Activities Regulations, which set out the new regulatory regime applicable to PSPs carrying out retail payments activities. Amongst other obligations, PSPs will have obligations with respect to risk management and incident response and with respect to the safeguarding of funds.

Digital wallets

See Question 1. In addition, while there has been no definitive position of the regulators on this matter, entities offering digital wallets should review their activities under the laws and regulations applicable to deposits. Closed-loop wallets, gifts 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 and the Industrial Research Assistance Program (IRAP). The CSA has also established the 'regulatory sandbox', an initiative aimed at supporting fintech businesses and other innovative business models in seeking exemptive relief from certain securities law requirements, such as the prospective requirement. The regulatory sandbox allows companies to test their products under faster and more flexible conditions.

Provincial

Certain provinces have established more fintech-specific initiatives. As an example, Ontario's FinTech Accelerator Office established consists of a programme used to connect startups to businesses. Moreover, 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 'Tech Team' that is dedicated to supporting the innovation and adoption of new technologies in the financial services sector. In Quebec, the Autorité des marchés financier (AMF) has created a think-tank known as the Fintech Lab, whose purpose is to explore entity applications with respect to new technologies.

In addition, 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. In this regard, in 2018, an Advisory Committee on Open Banking (the Committee) was appointed by the Minister of Finance. In August 2021, the Committee released its final report on the matter.

The implementation was initially planned to roll out in two stages: (1) a first initial phase of low-risk implementation by January 2023; and (2) a second phase of ongoing evolution and administration of the open banking system, but the current state of progress indicates that this implementation will most likely be delayed. Based on these plans, all federally regulated banks would be required to take part in phase one, while all provincially regulated financial institutions would be implicated on a voluntary basis.

Mexico

Miguel Gallardo Guerra*
Bello, Gallardo, Bonequi y García (BGBG), Mexico City
mgallardo@bgbg.mx

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

In Mexico, 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 to regulate fintech entities. On 9 March 2018, the Law to Regulate Financial Technology Institutions (the Fintech Law) was published in the Official Federal Gazette. These institutions are legal entities authorised by the National Banking and Securities Commission (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).

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.'

---

* 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, also 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.

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.

The Tax Administration Service and virtual assets

In addition, the Tax Administration Service (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), 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 purposes of 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 MXN96.22 per UMA – even if that threshold is reached by virtue of 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 internally 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 Authorizations 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 Organizations 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. 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. Therefore, 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.

5. 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.

United States

Eric M Rosof*
Wachtell, Lipton, Rosen & Katz, New York
EMRosof@wlrk.com

David M Adlerstein†
Wachtell, Lipton, Rosen & Katz, New York
DMAdlerstein@wlrk.com

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

Unlike some global jurisdictions with a unitary national regulatory scheme and/or a regulator with plenary power, the United States has a dual regulatory system, whereby authority is vested in both federal (eg national level) and state (eg New York) regulators. Banks are chartered at either the national or state level, and functional responsibility is allocated among various regulators at both the federal and state level, as well as with certain self-regulatory organisations. Although federal laws may pre-empt state laws in certain cases, US regulation over fintech and financial innovation is a complex mosaic with many overlaps, compounded by the fact that fintech and financial innovation encompass multiple financial services (money transmittal, lending, insurance, 'roboadvising', etc).

As a threshold matter, the following are some of the key US regulators with functional responsibility for fintech and financial innovation (depending on the nature of the activity and who is engaging in it).

- The Board of Governors of the Federal Reserve System (the Fed): the US central bank, whose regulatory authorities include the supervision of bank holding companies and state-chartered banks that are members of the Federal Reserve System.
- Office of the Comptroller of the Currency (OCC): an independent bureau of the US Department of the Treasury that charters and has primary supervision of national banks.
- Federal Deposit Insurance Corporation (FDIC): a federal agency that insures bank deposits and is the primary federal supervisor of state-chartered banks that are not members of the Federal Reserve System.
- Consumer Financial Protection Bureau (CFPB): a federal agency responsible for consumer protection and enforcement of federal consumer protection laws.
- Securities and Exchange Commission (SEC): the federal agency with responsibility for investor protection and capital formation through the administration of US securities laws, including

---

* Eric is a partner at Wachtell, Lipton, Rosen & Katz, where he leads the acquisition finance practice. Eric advises on financing for corporate transactions of all types, including domestic and cross-border mergers and acquisitions, dispositions, spinoffs, joint ventures, restructurings, refinancings and recapitalisations.

† David is counsel in the Corporate Department at Wachtell, Lipton, Rosen & Katz. His practice focuses on mergers and acquisitions, capital-raising transactions, corporate governance, and other corporate and securities law matters, with a focus on financial institutions and technology transactions. David has worked on a broad array of public and private company acquisitions, divestitures, joint ventures (including numerous credit card programmes), securities offerings and corporate governance matters.

registration requirements for public offerings and the regulation of investment advisers and broker/dealers.

- Commodity Futures Trading Commission (CFTC): The federal agency with responsibility for regulation of derivatives in respect of commodities (including in respect of certain crypto assets).
- State banking and insurance regulators: individual states have regulators with responsibility for chartering and supervising banks and insurance companies and granting licensing for certain financial activities, such as lending and money transmittal.

Key laws and regulations relevant to fintech and financial innovation include (among others):

- State money transmittal licensing regulations: non-bank payment service providers are required to obtain money transmittal licences under the laws of virtually every US state (see Question 3).
- State lender licensing regulations: non-bank lenders (such as providers of 'buy now, pay later' products) are required to obtain lending licences under the laws of many US states.
- Securities Act of 1933: federal law requiring issuers of securities to register offers and sales of securities with the SEC unless there is an available exemption from registration. This law may in many circumstances implicate crypto assets; see Question 2.
- Investment Advisers Act of 1940: federal law mandating the registration of investment advisers (including so-called robo-advisers, who typically must register with either the SEC or one or more state securities authorities).
- Bank Secrecy Act: A federal law that (together with associated anti-money laundering regulations) requires banks and other financial institutions to perform KYC checks and report cash transactions over $10,000 to the Financial Crimes Enforcement Network (FinCen) of the US Department of the Treasury.
- OCC Risk Management Guidance: OCC guidance requiring that federally chartered banks assess and manage risks associated with third-party relationships, which can subject fintech market participants partnering with banks to enhanced due diligence requirements and regulatory examination.
- Consumer Financial Protection Act: a federal law prohibiting unfair, deceptive or abusive acts and practices in the course of providing financial products, including fintech products. Similar laws exist at the state level.
- Gramm-Leach-Bliley Act: a federal law which protects consumers' non-public personal information and requires dissemination of privacy notices regarding how consumer data is used.
- California Consumer Privacy Act of 2018: a statute analogous to the European General Data Protection Regulation (GDPR) which gives California consumers the right to know about the personal information a business collects about them and how it is used and shared, the right to require deletion of collected personal information, the right to opt out of the sale of personal information, and the right to non-discrimination for exercising rights under the Act.

- Notable emerging laws and regulations relevant to fintech and financial innovation (other than in respect of crypto assets; see Question 2) include:
- Anti-Money Laundering Act of 2020: federal legislation reforming aspects of anti-money laundering law, including by imposing corporate transparency requirements which require reporting companies (including fintechs) to report information regarding their beneficial ownership with FinCen, with possible civil and criminal penalties.

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

There remains considerable uncertainty regarding the regulation of crypto assets in the US, particularly at the federal level with respect to the extent certain crypto assets constitute securities. Under the so-called Howey test under US case law, securities include an 'investment contract', which exists in circumstances where there is an investment of money in a common enterprise with an expectation of profits primarily from the efforts of others. While regulators are aligned that Bitcoin is a commodity, the SEC has expressed the view that most crypto assets are securities, such that their offering and sale must either be registered with the SEC under the Securities Act of 1933 or fit into an exemption from registration, and such that issuers of crypto assets could be subject to periodic reporting under the Securities Exchange Act of 1934 (ie, required to file annual, quarterly and current reports with the SEC).

Of particular note, the SEC's view is that many crypto assets themselves – notwithstanding that they may lack traditional indicia of equity or debt, and as opposed to the arrangements whereby crypto assets are sold – constitute securities. This view undergirds the SEC's ongoing litigation against Ripple in respect of the crypto asset XRP, as well as the SEC's view that spot markets in crypto assets should be under its purview. This was also the basis for the SEC's 2017 determination that the Ethereum DAO constituted a security, and that most so-called 'initial coin offerings' constitute securities offerings.

However, under guidance promulgated by the SEC in 2018, a token project that is sufficiently decentralised (lacking an 'active participant' that drives the project) would not constitute a security. However, to date very few token projects have endeavoured to register with the SEC, a task made more difficult by the orientation of SEC registration and reporting forms towards traditional centralised issuers of traditional securities.

An additional regulatory gap arises from the fact that, under prevailing law, the CFTC only has regulatory authority over derivative markets, not spot markets. Some proposed federal legislation would vest the CFTC with regulatory authority over spot markets, but in its absence, both centralised and decentralised crypto asset exchanges have generally avoided comprehensive federal regulation. However, it is the case that most centralised exchanges are registered with FinCen and licensed as money transmitters, and in some cases are subject to state-level prudential regulation and licensing (notably under the State of New York's relatively comprehensive Bitlicense regime).

Stablecoins have also been the focus of significant regulatory attention both at the federal and state level. In late 2021, a President's working group of federal financial regulators issued a report on the regulation of stablecoins. The upshot of the report is that federal regulators expect to

comprehensively regulate stablecoins and 'stablecoin arrangements' (an undefined term that may be interpreted broadly to include crypto wallets and exchanges). As part of this, the regulators expressed a clear preference that stablecoins be issued only by regulated banks that are subject to the proscription on the mixing of banking and commercial activities, and also suggested that crypto wallet providers be subject to the same limitations.

At the time of writing, there have been many regulatory actions and proposals at both federal and state levels with respect to crypto assets, and numerous proposals are pending.

- President Biden's 2022 Executive Order: in early 2022, President Biden issued the Executive Order on Ensuring Responsible Development on Digital Assets. The Executive Order contemplates a comprehensive approach to the regulation of digital assets, creating an action plan for more than 20 federal agencies (including federal banking regulators) and executive departments to further a national policy for digital assets across six key priorities: consumer and investor protection; financial stability; illicit finance; US leadership in the global financial system and economic competitiveness; financial inclusion; and responsible innovation.
- Lummis-Gillibrand Bill: this bipartisan bill proposed in 2022 (but not enacted) would, among other things, propose a regulatory framework that provides for the issuance of stablecoins by depository institutions and other supervised entities, clarify instances in which a crypto asset is considered a security, establish a special SEC reporting regime for crypto assets issued pursuant to an investment contract (implying that crypto assets without indicia of traditional securities would not themselves be securities), subject spot markets in such assets to CFTC jurisdiction, and enhance consumer protection, including in respect of crypto asset lending and borrowing.
- Stabenow Bill: another bipartisan bill legislation proposed in 2022 (but not enacted) would vest the CFTC with authority to regulate spot markets in non-security crypto assets and require digital commodity platforms to register with the SEC, and would clarify that Ether is a commodity.
- OFAC sanction of Tornado Cash: in 2022, the Office of Foreign Assets Control (OFAC) designated the virtual currency mixer Tornado Cash as a sanctioned person. Given that Tornado Cash is a decentralised project based on open-source software, the sanction may portend further attempts at regulating so-called decentralised financial protocols that enable peer-to-peer exchanges, collateralised lending and automated market making.
- State law: several states have promulgated legislation to provide clarity with respect to digital assets and to attract the industry to their jurisdictions. Of particular note was Delaware enacting amendments to its state corporate law to specifically enable the use of blockchain technology for corporate purposes. Wyoming also enacted blockchain-related legislation, including laws enabling digital asset companies to apply to become special purpose depository institutions and laws allowing decentralised autonomous organizations (DAOs) to form and obtain limited liability company status.

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

There are three particularly noteworthy bodies of regulation applicable to the provision of payment services and digital wallets (ie, provision of stored value products; see Question 2 with respect to crypto assets) in the US: state money transmittal licensing requirements, federal anti-money laundering (AML) requirements, and federal and state data privacy requirements.

With the exception of banks, any business providing money transfer services is required to obtain a money transmittal license in any US state (with the sole exception of Montana, which requires registration but not licensing) where they engage in this activity. The licensing process is time-consuming because state definitions of money transmission vary, such that a particular activity may require licensing in one state but not another, because documentary requirements are extensive, and because licensing must be renewed annually.

With respect to AML, with limited exceptions, the Bank Secrecy Act requires payment service providers (so-called 'money services businesses' or MSBs) to register with FinCen within 180 days after establishment. MSBs are required to develop and implement an AML compliance program, including rigorous know your customer requirements, and a requirement to file so-called 'suspicious activity reports' with FinCen with respect to any cash transaction in excess of $10,000.

With respect to data privacy, financial services companies collecting and using personally identifiable information from natural persons are subject to federal regulation such as the Gramm-Leach-Bliley Act and some state regulation such as the CCPA, as noted 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 US does not currently have broadly applicable fintech support programmes (such as regulatory sandboxes or accelerator programmes) at the federal level.

At the state level, in an effort to promote state economic growth, regulatory sandboxes have been adopted by certain states. Generally, under these arrangements, market participants may, on a limited scale, test applicable fintech products and services without complying with applicable licensing and supervisory requirements for a transitory period. As noted in the response to Question 2 above, some states (including in particular Wyoming) have also adopted crypto-friendly legislation.

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

The US has yet to implement open banking, with the limited exception of so-called 'screen scraping', whereby a consumer can provide access credentials to third-party data aggregators.

In November 2020, the CFPB promulgated an advance notice of proposed rulemaking with regard

to consumer financial services providers making available to consumers information in the control or possession of the provider concerning the consumer financial product or service that the consumer obtained from the provider. In November 2021, President Biden issued an Executive Order on promoting competition in the American economy which, among other things, encouraged the director of the CFPB to 'facilitate the portability of consumer financial transaction data so consumers can more easily switch financial institutions and use new, innovative financial products'.

South America

Argentina

Carlos María Melhem*
Allende & Brea, Buenos Aires
cmelhem@allende.com

Micaela Boruchowicz†
Allende & Brea, Buenos Aires
mboruchowicz@allende.com

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

Currently, there are no specific regulations for fintech in Argentina. Argentina does not have a fintech law. Nevertheless, certain pieces of regulation indirectly relate to technology applied to financial innovation, the most relevant of which are summarised below.

Transferencias 3.0

In 2020, the Argentine Central Bank passed regulations creating a new standardised payments interface that allows the matching of payments through an open and interoperable digital ecosystem in the frame of the Argentine National Payment System (T3.0 Regulations). These regulations provide that all banks and non-bank institutions offering virtual payment accounts will be 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 transfers system entered into operation on 7 December 2020 for debit cards and the provision of QR codes for the initiation of such payments, except for prepaid cards – the use of which for T3.0. transfers were not allowed until 31 May 2021.
The T3.0 transfers real-time payment system mainly comprises the following participants:

- a payer;
- a receiver;
- one or more financial institutions, banks and/or payment service providers who offer virtual payment accounts; and
- an administrator.

Entities authorised by the Central Bank to function as administrators of T3.0 so far are: Compensadora Electrónica SA, Interbanking SA, Prisma Medios de Pago SA and Red Link SA.

---

* Carlos is the co-head of Allende's banking and financial practice and FinTech law practice. He is an expert on commercial and banking law, having advised local and international companies and banks.

† Micaela is a semi-senior associate of Allende's banking and financial practice and FinTech law practice. She advised local and international companies, banks and payment service providers in relation to commercial and banking law.

Payment service providers

Central Bank regulations contemplate two types of payment service provider: (1) payment service providers 'that offer virtual payment accounts' (PSPs), and (2) payment service providers 'that perform payment initiation activities' (ie, digital wallet services) (PSIs). Both PSIs and PSPs must register with the Registry of Payment Service Providers of the Central Bank. Please see Question 3.

Registry of Interoperable Mobile Wallets

Central Bank regulations provide that PSPs, PSIs, financial institutions and banks that allow the initiation of payments with interoperable QR codes must register with the Registry of Interoperable Mobile Wallets of the Central Bank. Please see Question 3.

Open banking

Central Bank regulations provide that PSPs and banks that also offer digital wallet services must allow the initiation of payments from any virtual or bank account, even if the account is held with a different PSP or bank. Please see Question 5.

Crowdfunding

The Entrepreneurial Support Act (Law No 27,349) and Resolution 717/2017 of the Argentine Securities and Exchange Commission (CNV for its acronym in Spanish) provide for a crowdfunding regulatory framework for equity crowdfunding in Argentina.
This framework establishes a set of requirements:

- crowdfunding platforms (PFCs) must register as corporations with the relevant Public Registry and obtain authorisation from the CNV;
- the corporate purpose of the PFCs must be to connect investors with entrepreneurs, within a professional framework and exclusively through web platforms, for the financing of projects;
- PFCs must hold a minimum net worth of 65,350 UVAs;[1]
- PFCs 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 12 months;
- entrepreneurs must comply with an annual and quarterly reporting regime; and
- investors are limited to a maximum investment of 10 per cent of the subscription or 150 UVAs per project, whichever is lower.

1 UVA is the acronym for *unidad de valor adquisitivo* (unit of purchasing value). Currently, UVA 1 = AR$188.49.

Crowdlending

The Central Bank regulates companies that provide lending services through technological platforms by connecting one or more credit providers with potential borrowers in order to carry out credit transactions in Argentine pesos (credit service provider platforms).

Credit service provider platforms must register with the Registry of Peer-to-Peer Credit Service Providers through digital platforms enabled by the Superintendence of Financial and Exchange Entities (SEFyC). The regulation establishes a set of requirements:

- credit service provider 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 provider platforms shall neither commit to repay the credits to the investors nor acquire such credits;
- credit service provider platforms must provide all the information to identify the potential borrowers;
- funds transfers may be carried out through bank or payment accounts;
- credits granted through credit service provider platforms must be kept apart from the credit service provider platforms' net worth; and
- credit service provider platforms must have a specific manual showing the process through which the investments are carried out.

In addition, credit service provider platforms may provide credit analysis, administration, and collection management services, provided that the investors retain the final decision regarding the granting of the loans.

QR codes

The Central Bank has issued new regulations regarding QR codes in the frame of the T3.0 payment schemes. In this respect, the T3.0 Regulations specifically contemplate payment through QR codes to promote 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 acquirers of the T3.0 payment scheme make available to their clients must comply with some requirements and meet the standards set by the Central Bank; and
- all financial institutions, PSPs and PSIs that make available to their clients the reading of QR codes, must adapt their systems to allow the capture of QR codes associated with any payment request, without discrimination.

Hence, the administrators of T3.0 may not, under any circumstance, enable an acquirer to receive transfer payments initiated with QR codes if they have not verified that such QR codes are readable by all financial institutions, PSPs and PSIs.

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

In Argentina, there are no specific regulations giving a legal definition of crypto assets. Thus, under the general law applicable in Argentina, cryptocurrencies are regarded as intangible assets rather than as currency or securities, and are subject to section 16 of the Argentine Civil and Commercial Code since they have patrimonial value.

The Central Bank and the CNV have clarified 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 this sense, the Central Bank and the CNV have 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'.

The first regulation specifically referring to cryptocurrencies in Argentina was Resolution 300/2014, whereby the Argentine Information Unit (the Argentine AML Authority) established that entities required to file money laundering and terrorism financing prevention reports must perform enhanced due diligence on clients using digital assets for their transactions.

From a taxation perspective, under an income tax amendment passed in 2017, capital gains from the sale of cryptocurrencies are taxable events subject to a 15 per cent tax in Argentina.

Finally, the Central Bank has issued certain regulations pertaining to cryptocurrencies and crypto assets. For example, Communiqué A 6823, issued in 2019, bans the use of credit cards (issued by local entities) for the 'acquisition of crypto assets in their different modalities' in foreign currency with foreign crypto exchanges.

In addition, Communiqué A 7506 provides that banks and financial institutions are not allowed to carry out any transaction with digital assets – including crypto assets (eg, NFTs) – or facilitate any such transactions to their clients.

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

According to Sections 4. G) and 14. J) of the Central Bank's Charter (Law No 24,144), the Central Bank is the regulatory and supervisory authority responsible for regulating payment services in Argentina.

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 Law;

- 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 governing the National Payment System provide that all parties involved must operate through the Central Bank and the Electronic Payment System, and hold an account with the Central Bank. They further provide that every transaction involving debits and credits from a financial entity or any other legal entity within the Electronic Payment System must have the Central Bank's prior validation.

The Central Bank is the governmental entity that regulates, controls, and provides the legal framework for payment service providers and digital wallets. Such regulations provide two types of payment service providers: (1) PSPs; and (2) PSIs, both of which must register with the Registry of Payment Service Providers of the Central Bank.

The regulations define PSPs as those that offer virtual payment accounts. If they were to perform digital wallet services (ie, initiation of payments) as well, they should adapt their 'operational and commercial description' accordingly and update their registration as PSPs with the Payment Service Providers Registry of the Central Bank.

On the other hand, the regulations define PSIs as those that offer digital wallet services through a mobile app or a web browser, which allow: (1) immediate payments, and/or (2) credit, debit and/or prepaid card transactions. If the PSIs were to offer virtual payment accounts, they should only register as PSPs with the Payment Service Providers Registry of the Central Bank.

In addition, PSPs, PSIs, financial institutions and banks that allow the initiation of payments with interoperable QR codes must register with the Registry of Interoperable Mobile Wallets (as per Central Bank Communiqué 'A' 7533).

Registration with the Registry of Interoperable Mobile Wallets requires registration as a PSP or PSI and filing of the following documents and information with the Central Bank:

- a certificate issued by each of the administrators of the T3.0 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 is ready to be used by the general public to make transfer payments by reading of the QR codes generated by each such acceptor;
- 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;

- the location of the 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 is no special programme supporting the fintech ecosystem, in particular fintech startups, such as regulatory sandboxes and accelerator programmes.

Nevertheless, in recent years (since 2016), the Central Bank has organised the so-called 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 items on the agenda discussed at the Financial Innovation Table can be summarised as follows:

- payment infrastructure;
- technology applied to payment schemes;
- alternative credit and savings channels; and
- 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 regarding taxation matters.

Moreover, the Central Bank has developed a Financial Innovation Program for all professionals, entrepreneurs, and students specialised in the financial innovation field. The main purpose of the programme is to develop a wide range of projects related to:

- digitalisation;
- digital payments;
- alternative scoring;
- data and end-user protection regulations; and
- financial opportunities, among others.

The programme aims to foster financial inclusion through collaborative work between public and private stakeholders.

Lastly, there are government incentives for startups and fintech businesses (ie, small and medium-sized businesses), such as tax incentives for technology investment and development. Particularly, in 2019, Law No 27,506 (*Ley de Promoción de la Economía del Conocimiento*) 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:

- an income tax reduction;
- a reduction in social security contributions; and
- exemptions for application of VAT withholding under certain conditions.

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 Argentina other than Central Bank Communiqué 'A' 7514 (as amended), as explained above. Argentina does not have an open banking law like the European model developed in recent years. Nevertheless, some companies in Argentina have launched their business incorporating some of the principal characteristics of the European model for the commencement of the open banking system development.[2]

In addition, as mentioned in Question 1, the only specific piece of regulation directly related to open banking is Central Bank Communiqué 'A' 7514 (as amended), which provides that PSPs offering digital wallet services must allow the initiation of payments from any virtual or bank account, even if such account is held with a different PSP.

2 '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 interesting Argentine use case was the ANK application, which, using the DEBIN product, allowed access to a user's bank accounts to make debits from them and make payments or money transfers. Finally, there is an initiative that is an associative model made by a consortium of 30 public, private and cooperative banks that created the digital wallet MODO'. Jose Marcos, 'First steps towards Open Banking in Argentina (Open Banking Excellence, 9 September 2021), see 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.

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 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:

---

* 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.

- 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 2021, 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.

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.
- 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.
- 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 Advogados, São Paulo
bbalduccini@pn.com.br

Nicolás Alonso†
Brigard Urrutia, Bogotá
nalonso@bu.com.co

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

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. 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 framework applicable both to payment institutions and digital lending fintechs are:

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:

---

* Bruno is a partner of the Banking and Financial Regulation practice group with more than 30 years of experience. He focuses his practice on banking and financial regulation, fintech, payments, crypto assets, and related matters.

† Nicolás was a visiting attorney that worked at Pinheiro Neto Advogados for approximately two years. He is originally from Colombia and works at Brigard Urrutia, focusing his practice on banking and fintech matters.

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]

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.

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.

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; once they hit specific volume thresholds, they 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:

- minimum capital requirements;
- prudential requirements;
- reporting and risk administration system requirements;
- data protection laws;
- bank secrecy regulations;
- consumer protection laws, etc.

1 Clients' funds contained in such accounts are bankruptcy remote and cannot be used by the payment institution to fund its operation. In addition, clients' funds, while not being used, must be either deposited at the Central Bank or used to purchase government bonds.

Digital lending fintechs

- Law 4595 of 31 December 1964; and
- CMN Resolution No 4.656 of 2018, as amended.

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, unlike 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. Digital lending fintechs are classified as follows.

Direct credit companies (SCDs)

A financial institution entitled to grant loans and financing to borrowers exclusively by means of electronic platforms and by using its own capital. SCDs are not entitled to offer deposit-taking products and, thus, are not entitled to perform financial intermediation to leverage its lending activity with its deposit-taking activity.

Besides granting digital loans, SCDs are also entitled to offer the following services:

- credit rights acquisition operations;
- credit analysis services for third parties;
- collection of credit rights services;
- acting as an insurance representative in the offering of insurance products related to the services mentioned above;
- issuance of electronic currency (eg, issuer of pre-paid cards) and post-paid payment instruments (eg, credit cards).

Person-to-person loan companies (SEPs)

A financial institution that offers a digital platform that creates a lending marketplace between companies, securitisation vehicles and individuals as lenders and companies and individuals as borrowers. SEPs are also entitled to perform

- credit analysis services for third parties;
- collection of credit rights services;
- acting as an insurance representative in the offering of insurance products related to the services mentioned above; and
- issuance of electronic currency (eg, issuer of pre-paid cards).

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, and financing entities, SCDs and SEPs are types of financial institutions that are authorised to lend.

SEPs are not entitled to fund directly the loans offered within its platform and are not entitled to retain the funds disbursed by the lenders within the platform.

As mentioned, both SCDs and SEPs require prior authorisation from the Central Bank to start operations. They should also comply with several regulatory requirements including:

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

Like other Latin American countries, until 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 at regulating the crypto assets market in Brazil. Although published, the Law will come into force only after 180 days from its publication. 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 focuses on combatting crypto-related crimes, removes crypto assets from the regulatory and supervisory scope of attributions of the Brazilian Securities Exchange Commission (CVM) and creates instruments to reduce the ecological footprint of the mining process through tax incentives.

Therefore, after coming into force, the 'digital assets service providers' (which is the name that the bill grants to those entities involved in a crypto transaction) virtual assets service providers (VASPs) wishing to operate in Brazil will require a regulator prior authorisation. The 'digital assets service providers' that were already operating before the new law was enacted will have at least six months to adapt themselves to the new applicable regulations and may continue to operate until the relevant authorisation is granted. Such digital assets service providers must comply with certain minimum regulatory requirements such as risk management, operational and capital requirements, etc.

Please note that pursuant to the approved text of Law No 14,478/22, a '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:

1. trade between digital assets and national or foreign currency;
2. trade between one or more digital assets;
3. transfer of digital assets;

4. custody or management of digital assets or instruments that confer control over digital assets; or

5. participation in financial services and provision of services relating to the offering by an issuer or sale of digital assets.

Despite the above and until Law No 14,478/22 comes into force, the following applies to the crypto assets industry in Brazil:

- 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' (*valor mobiliario*). Conversely, if the crypto asset falls within the definition of a 'security', then the following would need to be complied with: (1) the issuer needs to be previously registered with the CVM and the offering needs to be listed and authorised by the CVM; and (2) the offering and distribution needs to be performed by a regulated entity such as a broker.
- Despite the foregoing, any acquisition or sale of crypto assets between a Brazilian individual or entity and an offshore individual or entity requires a foreign exchange transaction to be entered into with a local financial institution authorised to operate in foreign exchange. This means that, in practice, the remittance of funds abroad to purchase a crypto asset needs to be performed with the intermediation of a regulated financial institution.
- 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.
- Crypto exchanges need to comply with the general anti-money laundering regime applicable to any non-regulated entity.

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

Please refer to 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 Central Bank has 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. LIFT is truly an ecosystem aimed at innovation.

Finally, other regulators such as the CVM and the Superintendence of Private Insurance have their own regulatory sandboxes with similar purposes and regulations, aiming to foster innovation in their relevant industries.

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

Brazil has a specific legal framework and a highly developed open finance system.

According to the current regulatory framework applicable to the Brazilian Open Finance system 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 in order to receive a better financial product or service.

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. The Brazilian open finance system follows the following principles:

- 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 this, 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.
- The open finance system does not modify or alter the Brazilian General Data Protection Law, which needs to be strictly complied with among the participants.
- The main purpose of the open finance system is to foster competition and provide transparency to the users.
- Users are the owners of their data; thus, the open finance system is based on the principle that data sharing is only legally and practicably possible upon a user's express consent.

The Central Bank has regulated the minimum governance and technical standards to be mandatorily adopted among participants in order to be plugged to the open finance system.

Chile

Matías Langevin Correa*
HD Legal, Santiago
mlangevin@hdycia.cl

Ignacio Araya Paredes†
HD Legal, Santiago
iaraya@hdycia.cl

Fernanda Aillach Núñez‡
HD Legal, Santiago
faillach@hdycia.cl

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

Until recently, there were no specific laws or regulations concerning fintech companies or financial innovation in Chile, but Congress recently published in January 2023 the so-called Fintech Law, which came into force on 3 February 2023. Before the introduction of the Fintech Law, these activities were governed exclusively by general constitutional, legal and regulatory provisions.

In general terms, article 19 No 21 of the Chilean Constitution enshrines the right to pursue any economic activity that is not contrary to morality, public order or national security, abiding to the applicable legal requirements and standards. This means that anyone can undertake different economic activities, if they comply with the aforementioned limitations, which include fintech companies or businesses related to financial innovation.

From a legal perspective, in Chile, natural and legal persons can develop and commercialise different financial products and services without prior authorisation from our financial authorities. The exception being those that require by law some type of authorisation or licence,[1] which must comply with the pertinent legal and regulatory requirements in order to carry them out. These include, among others:

- banking activities (banking licence pursuant to the General Banking Law);

---

* Matías is the head of HD Legal's fintech law practice. He has an extensive experience in financial matters and digital markets, including digital payment processing systems, crypto assets, digital lending, digital financial platforms, among others. He also has expertise in corporate matters, with an emphasis on international transactions, in the areas of M&A, capital markets, project finance and the corporate reorganisation of corporate structures, advising both local and international clients.

† Ignacio is a senior associate in HD Legal's fintech law practice. Ignacio focuses his practice on corporate affairs and in matters related to financial regulation, corporate law, stock market and corporate financing, mainly advising fintech companies, including cryptocurrency exchanges, open banking, remittance companies and digital lending platforms. He advises various local and international clients, focusing mainly on startups.

‡ Fernanda is an associate in HD Legal's fintech law practice. Fernanda works on corporate matters and especially in matters related to fintech companies, including cryptocurrency exchanges, open banking, remittance companies and digital lending platforms. She advises local and international clients, focusing mainly on startups.

1 See General Banking Law (Decree with Force of Law No 3, of 1997); Securities Market Law (Law No 18,045); Single Funds Law (Law No 20,712); Financial Instruments Clearing and Settlement Law (Law No 20,345); Law on the Deposit and Custody of Securities (Law No 18,876); Insurance Law (Decree with Force of Law No 251, of 1931), among others.

- public offering of securities (register issuer of securities, pursuant to the Securities Market Law); and
- securities exchange and brokerage (authorisation for the former, registration for the latter, pursuant to the Securities Market Law).

Moreover, the commercialisation of certain financial products and services may have to comply with other relevant legal requirements, if applicable, concerning:

- consumer protection (Law No 19,496, which applies to some extend to SMEs);
- data protection (Law 19,628); and
- anti-money laundering/combatting the financing of terrorism (AML/CFT) (Law No 19,913).

These provisions were not tailored for, nor mention specifically, fintech companies or businesses related to financial innovation, and thus compliance with them is usually a relevant area of expert legal advice.

The lack of a proper legal and regulatory environment for fintech companies and other businesses related to financial innovation has been a relevant concern for Chilean authorities in recent years. In February 2019, the Chilean Financial Market Commission (Comisión para el Mercado Financiero or CMF) issued a white paper with general guidelines for the regulation of crowdfunding and other related financial services, later followed with a draft proposal for the then-Fintech Bill (the Bill), which was broadly viewed as a clear push from the financial regulator to gain momentum for a widescale legal reform.

Given the shared interest from the financial regulator and the private sector to enact specific legal provisions that cover different aspects of financial innovation, in September 2021, President Sebastián Piñera formally introduced to Chilean Congress the Bill (Bulletin No 14,570-05), which was approved by Congress on 12 October 2022. The Fintech Law was published on 4 January 2023.

Article 1 of the Fintech Law states that the new legislation aims to establish a general framework to incentivise the provision of financial services through technological means carried out by providers governed by it.

Moreover, it seeks to regulate, among other things, the provision of certain technology-based financial services that must be registered with the CMF, which therefore will be subject to its supervision. Among these services are crowdfunding platforms, alternative transaction systems (ATS), credit and investment advisory services, custody of financial instruments, order routing and intermediation of financial instruments.

The Fintech Law also contains provisions regulating a system of open finance, in which the exchange of information between different institutions is allowed by means of remote and automated access interfaces that allow interconnection and direct communication between the institutions participating in this system. This will allow the provision of new financial services.

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

Until recently, there was no specific regulation governing crypto assets in Chile. However, different public authorities have issued legal statements concerning several relevant aspects related to them, ranging from their legal status as either currency or foreign currency, if they can be deemed as securities, and the fiscal implications arising from their commercialisation.

Notwithstanding the above, the Fintech Law can now regulate many aspects relating to crypto assets:

- it defines them in broad terms and considers them a type of 'financial instrument' under the Bill, thus linking them to the several fintech activities that will now be under the CMF's regulatory perimeter;
- it considers some stablecoins (that comply with the requirements to be set forth by the Central Bank of Chile) as 'means of payment', which can even be stored in prepaid cards and that can be part of payment systems regulated by the Central Bank; and
- it deems some stablecoins (that comply with the requirements to be set forth by the Central Bank of Chile) as foreign currency, for all applicable legal purposes.

Regarding their status as a means of payment, the Central Bank of Chile (Banco Central de Chile), by General Notice No 219, of 2019, characterised crypto assets as 'digital representations of value susceptible of being traded or transferred, and used for investment or payment purposes, only to the extent that the intervening people consent to it'.

Previously, in its General Notice No 2518, of 2018, it had concluded that cryptocurrencies or digital assets are not Chilean legal tender or currency, as they are not issued nor minted by the Central Bank of Chile, and that they also do not constitute a form of foreign currency, as they are not issued nor minted by any foreign state via its monetary policy authorities.

In this latter General Notice, it also stated that crypto assets are not means of payment regulated by Law No 20,950, which authorises the issuance of payment cards with provision of funds to non-banking entities. Finally, from a regulatory perspective, the Central Bank of Chile argued that purchase, selling and/or intermediation of virtual currencies does not constitute an activity subject to its regulatory powers.

Concerning their status as a security (*valor de oferta pública*), which would entail the application of the Securities Market Law, the CMF in several statements (General Notices Nos 20,088 and 20,089 of 2016; 3,517 of 2019; and 34,091 of 2022) has deemed that crypto assets cannot be considered as such. From a regulatory perspective, this means that the entities involved in their offering and intermediation are not under its perimeter of control.

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 Bitcoin 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 under No 4 of Article 20 of the Income Tax Law, and that the commission received by the intermediary is subject to VAT.

Finally, as previously explained, with the Fintech Law now in force, crypto assets have proper legal recognition, as the Law defines them as 'digital representations of units of value, goods or services, other than money, whether in local or foreign currency, which can be transferred, stored or exchanged digitally'. Likewise, these digital representations will now be considered as means of payment and as foreign currency.

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

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), mentions payment processing service providers (PSP), but only to exempt such companies from said regulation when they 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.

The chapter also 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 to 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 operator, in which it is expressly stated that any of the latter has assumed or shall assume the corresponding payment responsibility before the affiliated entities, without prejudice that the respective PSP shall make the settlements and/or payments that may be applicable; and
- that the settlement and/or payments made by said PSP, during the previous 12 months, on behalf of each of the issuers or operators with which it has a contract or agreement in force for this purpose, is less than 1 per cent of the total amount of payments to affiliated entities made by all the operators governed by these regulations, during the same period.

As regards digital wallets, until the recent entry of the Fintech Law into force, Law No 20,950 (in force since 2016) authorised 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 digital wallets that is used for similar purposes: the prepaid funds accounts (*cuentas de provisión de fondos*), which are 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 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.

Finally, it is worth mentioning that, with the enactment and entry into force of the Fintech Law, the commercialisation of the custody of financial instruments (such as crypto assets) will be regulated as a fintech service in Chile. In this respect, Article 2 defines financial instruments as any security, contract, document or incorporeal good, designed, used or structured for the purpose of producing monetary income, or representing an outstanding debt or a virtual financial asset (also called crypto assets in the Law). Accordingly, the fintech service concerning the custody of virtual financial assets or crypto assets will be 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 sandbox programme or innovation hub promoted by any regulatory entity that promotes innovations in the fintech ecosystem. However, as mentioned above, pursuant to the constitutional right to freedom in economic matters, any person or entity may undertake and develop new businesses without the need to have a specific regulation that authorises it; thus, the Chilean Constitution itself promotes the start and development of any kind of business or enterprise that is not contrary to morality, public order or national security and abides with the applicable laws that govern them.

However, we can mention several state initiatives that aim to promote different types of enterprises, such as:

- the entrepreneurship programmes of the Corporation for the Promotion of Production (CORFO);
- a public business accelerator called Start-up Chile, which promotes technological ventures and that is under the umbrella of CORFO and the Chilean Government; and

- several 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.

The Association of Fintech Companies of Chile (FinteChile), a private association, aims to represent and promote the growth of the fintech industry in Chile, and for this purpose, they have 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 AG (*Asociación de Bancos e Instituciones Financieras* or ABIF) and Banco Estado, for the purpose of establishing standards of responsibility and mechanisms for capturing customer data from the institutions that adhere to this 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.

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

There is currently no specific regulation governing open banking. However, general data protection legislation applies when due (Law No 19,628), as do the provisions stated in Law No 20,575, of 2012 concerning credit scoring and credit rating agencies.

Moreover, 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 ensures the standards of responsibility and the mechanisms for capturing data from the clients of the institutions adhere to certain legal and best-practice standards. It should be noted that this Framework Agreement must be complemented with bilateral contracts entered into by the interested parties, which specify the conditions under which the data capture would operate.

It is also worth mentioning Law No 21,236, which aims to promote financial portability, making it easier for individuals and businesses to switch financial service providers, if they deem it convenient.

Finally, as previously mentioned, Title III of the Fintech Law will regulate an open finance system that should allow for the exchange of information between different institutions, via remote and automated access interfaces that enable an interconnection and direct communication between the institutions participating in this system, thus allowing the provision of new financial services.

Colombia

Natalia Escobar*
Posse Herrera Ruiz, Bogotá
natalia.escobar@phrlegal.com

Julián Aguirre†
Posse Herrera Ruiz, Bogotá
julian.aguirre@phrlegal.com

Introduction

The development of fintech in Colombia has been guided by a public policy objective of increasing access to financial services through the adoption of innovative technologies.

During the past two decades, Colombian governments have established public policies and issued decrees and regulations covering the provision of payment, deposit and lending services by financial institutions[1] and non-regulated entities, while aiming to maintain financial stability and a level playing field.

Under that approach, Colombia has refrained from creating a comprehensive regulation for fintech; instead choosing to provide mechanisms and incentives through regulation for the orderly integration of financial innovations into the Colombian financial system.

This report surveys the regulations that have enabled the adoption of digital technology in financial services, as well as those addressed to product, services and activities generally recognised as falling under fintech.

Colombian financial system regulators have yet to issue comprehensive regulation addressing virtual assets, including those based in crypto technology. Colombian regulators have approached cryptocurrencies and digital assets with a coherent risk approach, as described in Question 2.

It is worth mentioning that this regulatory effort has been guided by key public policies established by the National Council for Economic and Social Policy (CONPES), under different governments, including:

- The 2006 Bank of Opportunities: 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.

---

* Natalia Escobar has been a partner of Posse Herrera Ruiz since 2022, in the Financial Law & Capital Markets department. She has over 15 years of experience in local and international financial regulation matters, and in lending and capital market transactions. Natalia advises local and foreign financial institutions and securities issuers in regulatory matters related to banking, asset management, pension, insurance, securities, and fintech. She also represents regulated and non-regulated entities on a broad range of matters before the Colombian Financial Superintendency and other authorities. Her practice includes advising innovative ventures and projects related to the financial system, with high social impact or focused on sustainability.

† Julián Aguirre is an associate at Posse Herrera Ruíz. His practice focuses on corporate and financial matters. Julián advises local and foreign innovative ventures, financial institutions and projects related to business models focused on fintech.

1 The terms 'financial institutions' and 'SFC-supervised entities' are used throughout this text interchangeably to encapsulate the diverse types of institutions that operate in the financial, securities, insurance, and investment markets in Colombia under the licence and supervision of the Colombian financial services regulatory agency, Superintendencia Financiera de Colombia.

- The 2019 National Policy for Digital Transformation and Artificial Intelligence: a policy that guided regulatory changes required to enhance the efficiency and competitiveness of the low-value payment ecosystem.
- The 2020 National Policy for Inclusion and Economic and Financial Education: a policy that sought to foster citizens' digital interactions with the government and financial institutions, including laying the groundwork for tools such as 'digital citizenship' and open finance.

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

Colombia has not adopted a specific regulatory framework for fintech. However, there are laws and regulations currently in place that enable innovation technology in the financial services industry. These: may be classified into four groups:

- e-commerce;
- personal data;
- digitalisation of financial products; and
- regulatory financial innovation tools.

E-commerce, digital contracting and technological infrastructure for providing financial services

Decree 410 of 1971 (Code of Commerce)

Provides merchants with the possibility of executing agreements by any unequivocal means.

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 documents. Recognises the validity and enforceability of data messages.

Law 1735 of 2014

Sociedades especializadas en depósitos y pagos electrónicos (electronic payment and deposit companies or SEDPEs) are financial institutions that may:

- receive deposits through simplified savings accounts;
- make payments and transfers and act as acquirers;
- take loans locally or internationally to finance their operation;
- send and receive money transfers.

SEDPEs may not provide credit. This law also enables financial institutions and financial services operators to access personal and biometrical identification data held by the National Government when required to gain effective access to financial services (ie, for know your customer procedures).

Law 1273 of 2009

This amends the Criminal Code to include criminal offences against the confidentiality, integrity and availability of data and information systems. These enhanced protections served as an enabling factor for the development of technological innovations, including fintech.

External Circular 029 of 2014

Issued by the *Superintendencia Financiera de Colombia* (the Colombian Financial Superintendence or SFC) and known as the Basic Legal Circular (BLC), this is a compilation of mandatory regulations issued by the SFC to govern the products, services, and entities that comprise the Colombian financial system. Two chapters are noteworthy for this report:

- SFC's BLC, Part I, Title II, Chapter I: instructs financial institutions and other regulated entities on digital transaction security and quality requirements and standards for customer attention through electronic channels.
- 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.

Decree 1074 of 2015

Codified several decrees regarding the commercial, industrial and tourism sectors, includes regulations on e-commerce and electronic signatures.

Decree 620 of 2020

Provides guidelines to foster the access of Colombian citizens to private and public digital services, including financial services.

Decree 338 of 2022

Strengthens digital security governance.

Personal data and consumer protection

Statutory Law 1266 of 2008

Governs writ 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.

Law 1581 of 2012

Personal data protection law.

Decree 1074 of 2015

Codified several decrees regarding the commercial, industrial and tourism sectors, including authorised financing activities developed by non-regulated persons, such as lending with own funds and factoring. Many fintech business models are based on these types of activities.

External Circular 10 of 2001

Issued by the Superintendent of Industry and Commerce (SIC) and also referred to as the Unique External Circular (UEC), it compiles all mandatory regulations issued by the SIC. It is important to highlight two titles:

- SIC's UEC, Title V: provides instructions on data protection and data treatment activities applicable to all economic sectors in Colombia.
- SIC's UEC, Title VIII: It provides instructions on lending activities by unregulated persons, including buy-now-pay-latter business models.

Law 1328 of 2009

Financial consumer protection law.

Law 1480 of 2014

Consumer protection law including rules on ecommerce platforms, electronic payments reversion, and on-line shopping withdrawal rights.

Digitalisation of financial products

Decree 661 of 2018 (compiled on Decree 2555 of 2010[2])

Authorises financial entities to use technological tools to provide advisory and product recommendations using technological means (eg, robo-advisors).

Decree 1357 of 2018 (compiled on Decree 2555 of 2010)

Governs collaborative financing (crowdfunding) instruments (both equity and debt) based on electronic infrastructure, which may include interfaces, platforms, internet pages or other means of electronic communication, to match contributors and recipients to finance a business initiative.

2 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.

Decree 222 of 2020 (compiled on Decree 2555 of 2010)

Regulates simplified savings accounts, electronic savings accounts and low-amount credit facilities, for which it enables virtual opening, onboarding and disbursement processes. It also authorises financial institutions and other regulated entities to contract with unregulated persons (ie, correspondents) to provide services to their clients through the correspondent's brick-and-mortar facilities and digital channels.

Decree 1692 of 2020 (compiled on Decree 2555 of 2010)

Governs low-value payment ecosystems, including acquiring and payment services providers activities, such as processing, aggregation and access technologies.

Decree 1297 of 2022 (compiled on Decree 2555 of 2010)

Regulates payment initiation services, open banking, financial services ecosystems (both embedded and third-party prompted), open financial architecture, and technology infrastructure services provided by financial entities to third parties.

Decree 2443 of 2018 (compiled on Decree 2555 of 2010)

Enables certain financial institutions to invest directly in financial technology innovation companies (FTIC), provided that the FTIC does not conduct any other main activities and refrains from investing in equity in other entities. Colombian law and regulations severely limit local financial institutions' capacity to invest in equity.

Regulatory financial innovation tools

Law 1955 of 2019, National Development Plan, Article 166

Authorises the SFC to issue temporary financial services licences (for up to two years) in a controlled environment for innovative technological developments related to activities reserved for financial institutions and other regulated entities. It also authorises all SFC-supervised entities to develop and test innovative technological activities under similar temporary conditions.

Decree 1234 of 2020 (compiled on 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 governmental authorities.

External Circular 16 of 2021 (compiled on the SFC's BLC)

Provides further instructions regarding access to the SFC's sandbox.

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

Colombia has yet to issue comprehensive regulations on crypto assets. Primary efforts 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 provisions have been implemented to address the higher anti-money laundering (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 take 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 cryptocurrencies. No private or governmental guarantee, or deposit insurance scheme is available for investment in 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 guest), have concluded that under Colombian law and regulation cryptocurrencies:

- may not be considered as legal tender. Only the currency issued by *Banco de la República* is legal tender in Colombia.[3] As a result, it is not mandatory to receive cryptocurrencies as means of payment;
- if issued abroad, cryptocurrencies may not be considered foreign currency because they are not recognised by any international financial authority or backed by any central bank;
- are not considered securities under Colombian securities law and regulations, therefore may not be referred to or advertised as such; and
- may not be considered financial assts or investment assets in accounting terms.

Following these conclusions, in Colombia cryptocurrencies are treated as intangible assets that may be traded and acquired by the public. 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 (STRs). 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 finalisation of a pilot project on the SFC's sandbox on cash-in cash-out transactions on virtual

3 Banco de la República is planning to issue a digital currency.

assets exchanges operated by fintechs in alliance with financial institutions. The draft regulation is expected to be issued in 2023 and covers the following issues:

- the main elements financial institutions must consider when evaluating a VASP as a client;
- consumer protection measures when financial institutions enter into alliances with VASPs; and
- clarifies that the following financial institutions may enter into the following operations involving VASPs or virtual assets:
    - managing companies of investment funds and private equity funds may include in the fund's portfolio investments in foreign investment funds with virtual assets as underlying assets;
    - trust companies may enter into trust agreements over virtual assets, directly or indirectly;
    - Colombian financial institutions may act as distributors or sub-distributors of foreign funds invested directly or indirectly invested in virtual assets; and
    - representative offices of foreign financial or securities market institutions, and local correspondents of foreign securities brokers, may promote and advertise financial products structured with virtual assets

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

Payment service providers

Colombia has regulated the payment services industry under the legal definition of '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, a LVPS requires: (1) a low-value payment system managing company (LVPSMC) and (2) that at least three or more SFC-supervised institutions, and certain cooperatives (subject to requirements) act as participants. Access to the LVPS is considered acquiring activity, and as such may include:

1. Connecting merchants to the LVPS.
2. Providing the merchants with access technologies that allow the use of means of payment (eg, debit and credit cards, QR, contactless instrument of payments, cash transfers, etc).
3. Processing payment orders or transfer of funds initiated through access technologies.
4. Aggregating merchants before LVPS.
5. Receiving the proceedings 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 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 (PSP). Acquiring activity may be carried out by credit establishments (including banks) and, SEDPEs (known in this capacity as acquirers), and by commercial companies not supervised by the SFC subject to certain 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:

- Aggregator: an acquirer payment service provider that connects merchants to the LVPS. It provides access to technologies that allow the use of payment instruments and collects on their behalf the proceeds resulting from the orders payment or transfer of funds in the merchant's favour.
- 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 present and non-present environments.
- Acquirer processor: payment service provider of the acquirer that routes orders for payment or transfer of funds to the managing entity of the low value payment.
- Issuer processor: provider of payment services of the issuing entity of a payment that 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 its owner to extinguish a monetary obligation, transfer funds, or make withdrawals through physical or virtual means.

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 maximum balance and on the aggregated value of transactions per month.

While soliciting funds from the public is an activity 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, it is not possible to offer digital wallets in which a fintech aggregates depositors for a financial institution.

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.

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 innovation applied to financial services, the stock market or insurance services, in a controlled and supervised space. 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 new market dynamics and promote safe and sustained financial innovation. In this space, innovative companies that intend to implement innovative technological developments to carry out activities reserved for SFC-supervised entities may request a temporary operation certificate valid for up to two years. Once the temporary certificate lapses, the participant may opt for obtaining a full licence or to wind down its operation under close oversight by the SFC.

5. Open banking: a summary of regulations regarding open banking and direct or indirect regulations that affect 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' personal data subject to compliance with Colombia data protection law and regulations.

It also regulated payment initiation activities, setting ground rules for LVPSAC neutrality, removing barriers to access by payment initiators and managing conflicts of interest, and providing a mandate for the SFC to develop applicable security requirements. It also regulated digital ecosystems, including the offering of third-party services through the financial institutions' distribution channels, and the offering of financial institutions products and services through the technological platforms of third-party providers.

Colombia opted for a regulated standard for the development of open financial architecture, and the SFC will act as its regulatory body. The SFC is expected to issue the required regulation before August 2023.

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: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

In Paraguay there is no 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 regarding financial innovation and indirectly addressing technology applied in finance:

- Regulations on Electronic Transactions:
  - Law 6822/2021 on Electronic Transactions Services and Electronic documents;
  - Regulatory Decree 7576/2022 of Law 6822/2021 (adopted on 3 August 2022).
- Regulations on the Paraguayan Payment System (SIPAP):
  - Law 4595/2012 on Payment and Securities Settlement Systems;
  - Rules on the Paraguayan Payment System (adopted by Resolution 1 of the Central Bank on 17 May 2022).
- Other Regulations with impact on financial technology:
  - Law 6534/2020 on Credit Data Protection Regulation;
  - Rules on Cloud Computing Services (approved by Resolution 10, on 28 July 2022).

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

In Paraguay's legal order, there is no current legal definition of digital assets (including crypto assets such as crypto currencies or non-fungible tokens (NFTs).

However, there is a bill under consideration in Parliament[1] which aims to regulate crypto mining activities and crypto assets-based activities. It has been already vetoed by the Executive Branch on 29 August 2022 and was rejected by the Senate on the same day.

---

* Martín is the Head of BKM/Berkemeyer's Project Finance, Infrastructure and PPP practice. He advises local and international companies and banks in major infrastructure projects and local business financial regulation.

† Pedro is an associate in BKM/Berkemeyer's Project Finance, Public Procurement and PPP practice. He advises local and international companies on local financial regulation and public procurement issues.

1 By the Chamber of Deputies for discussion.

Regardless, Paraguayan authorities have issued certain specific regulations concerning crypto asset activities:

- Secretariat for the Prevention of Money or Property Laundering (SEPRELAD):
    - Resolution 314 of 1 September 2021, which approves the Rules on domestic anti-money laundering (AML) and combatting the financing of terrorism (CFT) for Legal and Natural Persons established or domiciliated in Paraguay that perform activities related to virtual assets.
    - Resolution 008 of 15 January 2020, which determines that legal and natural people 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).
    - Resolution 009 of 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.
- Paraguayan Central Bank:
    - Statement on virtual currencies of 31 May 2019[2] and of 19 September 2020.[3]

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

In Paraguay, there are no specific regulations on payment service providers but there are many regulations on digital wallet.

Regulations on e-wallets[4] (*billeteras electrónicas*)

- Guidelines on Electronic Means of Payment, adopted by Resolution 6 of the Central Bank on 13 March 2014, as modified by Resolution 6 of the Central Bank on 16 April 2020.
- Guidelines on Information Provided by Electronic Payment Entities adopted by Resolution 10 of the Central Bank on 31 January 2019.
- Anti-Money Laundering/Combating the Financing of Terrorism Guidelines for Electronic Payment Entities adopted by Resolution 77 of SEPRELAD[5] on 6 March 2020.

2 '*Comunicado del BCP sobre monedas virtuales o criptomonedas*' (BCP, 31 May 2019), see www.bcp.gov.py/comunicado-del-bcp-sobre-monedas-virtuales-o-criptomonedas-n1153.

3 '*Comunicado sobre monedas virtuales o criptomonedas*' (BCP, 19 September 2020), see www.bcp.gov.py/comunicado-sobre-monedas-virtuales-o-criptomonedas-n1381.

4 In Paraguay, the term 'electronic money' is legally defined in Resolution 6 of the Central Bank (13 March 2014) and the term 'electronic money account' is legally defined in Resolution 6 of the Central Bank (16 April 2020). Therefore, it would be more accurate under Paraguayan law to refer to such wallets as electronic wallets or e-wallets.

5 Secretariat for the Prevention of Money or Property Laundering.

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 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 the digitalisation within the member countries of the Southern Common Market (MERCOSUR), through the Digital Agenda Group (DAG).[6]

At a purely domestic level, the national government is focused on the Digital Agenda Programme, which aims to improve digital connectivity in order to strengthen the national digital economy.[7]

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*)[8] 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 central bank digital currencies (CBDC).

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

In Paraguay there are no specific regulations on open banking. However, certain financial institutions are starting to use third-party services to analyse their consumer databases via software as a service (SaaS) businesses through APIs.

6 Established in December 2017 (see www.mercosur.int/temas/agenda-digital/).

7 '*Agenda Digital*' (Gobierno Nacional), see www.mitic.gov.py/agenda-digital/portada, accessed 23 January 2023.

8 See www.bcp.gov.py/ibcp/inicio.

Peru

Nydia Guevara Villavicencio*
Rodrigo, Elías & Medrano, Lima
nguevara@estudiorodrigo.com

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

In Peru, currently, there are 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, 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 recently 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.

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.

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.

* Nydia is a partner in the Finance and M&A practice. She specialises on 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.

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.

In addition, there have been recent initiatives by Peruvian congressmen to regulate the marketing and commercialisation of crypto assets; however, these initiatives (consolidated in a single proposal) are still under review by a specialised commission in Congress. No certainty exists whether they will be approved or not.

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).[1]

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.

By means of the foregoing regulations, 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 delivered 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; as well as remitting 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

1 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.

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,[2] 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;
- 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 abovementioned, 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

2 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.

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.
- 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 taking 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 an authorisation before the SBS complying 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) in order 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 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,[3] 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.

Finally, as mentioned in Question 3, the only specific piece of regulation related directly to open banking is the 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.

3 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: a summary of the most relevant laws and regulations concerning fintech and financial innovation.

Within the fintech regulatory framework in Uruguay, our country has encouraged a series of acts willing to adjust current regulation to a proper legal ecosystem that safeguards the guaranties of all the parties. We consider the following to be the most relevant regulations and foreseen regulations.

Current regulations

Act No 20,038 modified Uruguayan Check's Act No 14,412 and established new regulation of electronic and digital cheques. By virtue of this law, cheques may now be card, digital or electronic, including:

- traditional physical cheques, which have a handwritten signature of their issuer or endorser;
- card cheques that have been received by a bank and have been digitalised for the purpose of electronic clearing of cheques; and
- electronic documents with a digital signature. In order to issue an electronic cheque, the digital signature must be 'advanced' according to Uruguayan regulations.

The Central Bank's regulation No 2.307 incorporated the figure of peer-to-peer lending companies. These companies are legally defined as legal entities that manage web applications or other electronic media designed to mediate between suppliers and borrowers of money loans.

Their activity is strictly limited to mediation between parties, and are controlled by the regulations of the Superintendency of Financial Services. In addition, these types of companies are legally prohibited from acting as agents, offerors, demanders and operating payments and collections, among others.

The Central Bank's regulation Nbr. 2377 informed the incorporation of 'company managers of crowdfunding platforms' to the regulatory compendium of the securities market. By virtue of this,

* Jean Jacques is the founder of Bragard. He has more than 30 years of legal experience. He has focused his practice in the banking and capital markets areas. He has been recognised by international publications such as *Chambers and Partners, International Financial Law Review, LACCA, Leaders League, Legal 500 and Latin Lawyer* as a leading lawyer in Uruguay in financial and capital markets matters.

† Sofía is an associate in Bragard's legal corporate department. She provides legal advice to companies in the financial sector, including portfolio managers, stockbrokers, investment advisors and electronic money issuers. She has also started a technical specialisation in the area of legal tech, which enhances the value of the projects she is involved in.

regulation referring to public offering of securities was reformed, adding the possibility of such dynamics being carried out through these platforms. The Central Bank also provided that these companies must be subject to the supervision and control of the Superintendency of Financial Services, requiring prior authorisation from this body in order to operate.

Future regulation

In May 2022, the Uruguayan Central Bank announced to financial institutions and the general public a preliminary future amendment to the compilation of securities market regulations, which could incorporate the definition of credit-granting institutions as those natural and legal people who, without being credit management companies or financial services companies, habitually and professionally grant loans with their own resources or with loans granted by certain third parties. There is also a digital onboarding approach being promoted by the Superintendency of Financial Services that is applicable to financial institutions in general, which seeks to provide certain security guarantees regarding the authenticity of the user. Among the proposed modifications, the following stand out:

- The use of a process that allows remote verification of the customer's identity, which complies with recognised standards.
- Validation of the customer's digital identity or advanced electronic signature provided by suppliers. Regarding the advanced electronic signature, the one based on certificates issued by providers accredited before the Electronic Certification Unit or that are recognised as equivalent when issued by entities not established in the national territory will be accepted.

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

As a general conclusion, crypto assets are not yet regulated in the Uruguayan jurisdiction.

However, at the end of 2021 the technological innovation department of the Central Bank of Uruguay, issued a paper entitled *Conceptual framework for the regulatory treatment of Virtual Assets in Uruguay* in which terms related to the taxonomy of tokens and other related references were conceptualised (such as utility tokens or stablecoins).

The regulatory framework established the scope of Central Bank's competence as a regulator, which includes only those crypto assets linked to fintech. The content of the paper included the future regulation of two new types of business conducted by companies: (1) issuers of virtual assets and (2) virtual asset service providers. Any company carrying out activities that fall within the spectrum delimited by the conceptual framework must first apply for a licence to operate before the Central Bank, and act under the supervision and oversight of said authority.

Subsequently, in 2022, the Central Bank submitted a preliminary bill to the legislative branch which contained these terms and definitions[1] by introducing amendments to local regulations in force.

1 See www.bcu.gub.uy/Acerca-de-BCU/Resoluciones per cent20de per cent20Directorio/RD_99_2022.pdf.

The spirit of the regulator was not to create a new law but to adapt current regulation to this new reality in terms of technology. For example, the bill seeks to amend Article 14 of the Securities Market Law to include virtual assets within the definition of book-entry securities, which are characterised by the fact that they exist under a decentralised registry.

Likewise, given the disruptive nature and the speed at which these new technologies move forward, the Uruguayan Central Bank always placed great emphasis on the aspects that will be regulated, in the event that the draft bill is approved by legislative authorities.

Currently, it is under discussion before the Chamber of Representatives of the legislative authority alongside two other bills related to crypto assets; 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.

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

The payment system in Uruguay is regulated by Law No 19,210 (the Financial Inclusion Law) and its subsequent amendments and regulatory decrees. The law states in its first article that electronic means of payment shall be understood as 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.

Payments made through electronic means have a full cancellation effect on the obligations in compliance with which they are made. In the case of electronic fund transfers, the full cancellation effect will be produced at the moment of crediting the amount transferred in the destination account.

In addition, the regulation states that automatic debit payment services may be provided by (1) financial intermediaries and (2) electronic money issuing institutions (known in Uruguay as *instituciones emisoras de dinero electrónico* or IEDEs).

Likewise, the Central Bank, in its capacity as controlling entity of the payment system in Uruguay, has issued a compilation of rules regarding the payment and collection system, and the providers of such services.[2] In this sense, Article 82 of Book VII of Circular No 2353 provides that institutions issuing electronic money must obtain authorisation from the Central Bank of Uruguay prior to carrying out this activity, without prejudice, to start issuing special, general, mixed or feed electronic money, they must also have the authorisation of the Management of Economic Policy and Markets.

2 See www.bcu.gub.uy/Acerca-de-BCU/Normativa/Documents/Recopilacion-de-Normas/Sistema-de-Pagos/LIBRO per cent20VII.pdf.

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.

Although Uruguay does not yet have regulations that provide for the promotion of fintechs, the Uruguayan Fintech Chamber (CUF) is an association that brings together Uruguayan startups in the financial ecosystem. It emerged in 2017, with the intention of energising the atmosphere of those companies working in the financial sector and fostering their growth.

Among the aims of this organisation are to increase the visibility of Uruguay and its fintech market abroad, and to promote and encourage open banking in Uruguay.

Notwithstanding the above, our current regulation offers a variety of advantages created with the aim of fostering entrepreneurship and they have led to the development of several startups in Uruguay that have had a significant impact at regional and global level, albeit not strictly linked to financial technology.

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

Although Uruguay does not have yet a regulation regarding this matter, Open Banking is foreseen in the 2020–2022 agenda published by the Central Bank of Uruguay.

In its roadmap for the modernisation of the payment system,[3] it plans to promote the appropriate regulatory framework for the operation of the open banking system in the country.

Regulation, together with the high degree of formal banking in Uruguay and the exponential increase in the use of electronic money, may facilitate the implementation of these new business models in the near future.

Within its objectives, the Central Bank, specifically its innovation department, seeks to promote and encourage, together with market agents, the appropriate regulatory framework for the operation of an open banking system. The Central Bank considers that this will allow the exchange of data between financial institutions, with high standards of digital security, guarantees for all participants and a fair distribution of operating costs.

3 *Sólido, innovador y accesible*, (BCU), see www.bcu.gub.uy/Sistema-de-Pagos/Documents/Sistema per cent20de per cent20Pagos-hoja-de-ruta.pdf, accessed 23 January 2023.

the global voice of
the legal profession®

International Bar Association

5 Chancery Lane
London WC2A 1LG, United Kingdom
Tel: +44 (0)20 7842 0090
Website: www.ibanet.org