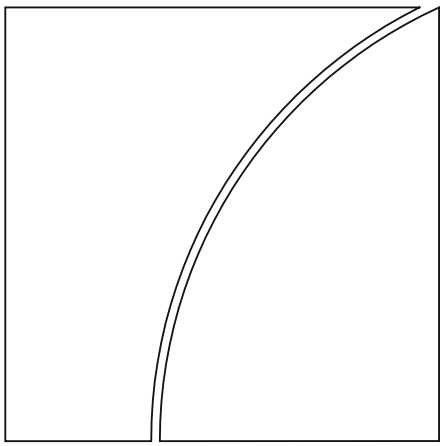
Financial Stability Institute

FSI Insights

on policy implementation

No 23



Policy responses to fintech: a cross-country overview

By Johannes Ehrentraud, Denise Garcia Ocampo, Lorena Garzoni, Mateo Piccolo

January 2020

JEL classification: G18, G21, G22, G23, G28, O30, O38

Keywords: fintech, regulation, digital banking, crowdfunding, fintech credit, robo-advice, e-money, digital payments, insurtech, cryptoassets, cloud, biometrics, distributed ledger technology, machine learning, artificial intelligence, innovation facilitators

BANK FOR INTERNATIONAL SETTLEMENTS

FSI Insights are written by members of the Financial Stability Institute (FSI) of the Bank for International Settlements (BIS), often in collaboration with staff from supervisory agencies and central banks. The papers aim to contribute to international discussions on a range of contemporary regulatory and supervisory policy issues and implementation challenges faced by financial sector authorities. The views expressed in them are solely those of the authors and do not necessarily reflect those of the BIS or the Basel-based committees.

Authorised by the Chairman of the FSI, Fernando Restoy.

This publication is available on the BIS website (www.bis.org). To contact the BIS Media and Public Relations team, please email press@bis.org. You can sign up for email alerts at www.bis.org/emailalerts.htm.

ISSN 2522-2481 (print)
ISBN 978-92-9259-332-2 (print)

ISSN 2522-249X (online)
ISBN 978-92-9259-333-9 (online)

Contents

Policy responses to fintech: a cross-country overview[1]

Executive summary

Technological innovations in financial services (fintech) are increasingly transforming the way financial services are provided. This transformation opens opportunities but comes with potential risks to consumers and investors and, more broadly, to financial stability and integrity, which financial regulation seeks to mitigate. As for opportunities, fintech can support potential growth and poverty reduction by strengthening financial development, inclusion and efficiency. In this context, financial authorities are adjusting their policy frameworks and providing guidance based on their assessments of the implications of emerging technologies for the financial sector.

The challenge for policymakers is to maximise the benefits of fintech while minimising potential risks for the financial system. However, this is easier said than done as regulators face several challenges. Fintech developments present issues that are beyond the traditional scope of financial authorities, and the speed of innovation makes it difficult for regulators to respond in a timely manner. Also, important trade-offs may arise between different policy objectives.

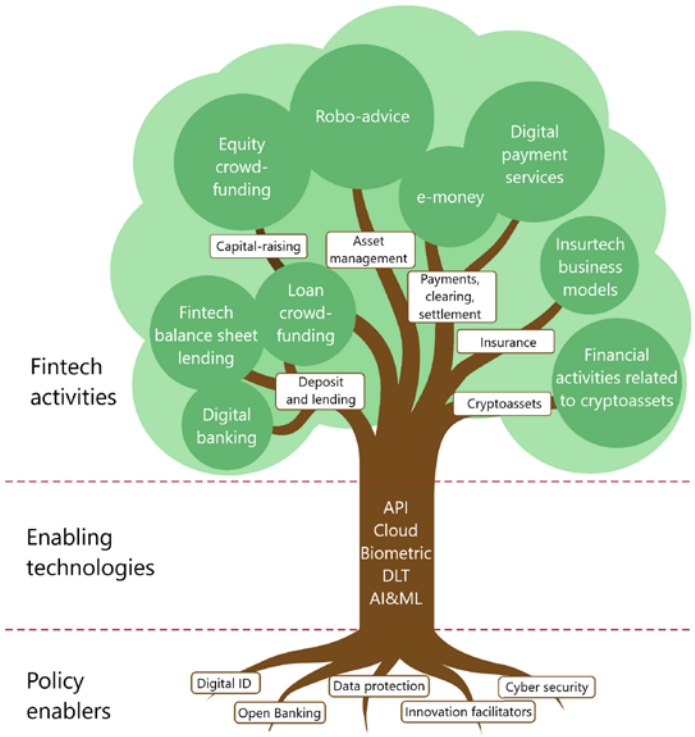
This paper surveys 31 jurisdictions on their policy responses to fintech developments. The key aim of our study is to provide a cross-country overview of the responses that financial authorities have pursued in relation to fintech. The paper is based on responses to a survey conducted in early 2019 by the Financial Stability Institute (FSI), which was supplemented by a comprehensive review of published regulations and documents as well as the authors' own analysis.

Building on the work by global standard-setting bodies and other international organisations, we propose a conceptual framework through which we analyse policy responses to fintech, referred to as the "fintech tree" (see chart on next page). The fintech tree distinguishes three categories: fintech activities, enabling technologies and policy enablers. Fintech activities (eg digital banking or robo-advice) can take various forms and may be performed in different sectors of the financial industry. Enabling technologies (eg cloud computing or artificial intelligence) are those that make innovation possible in the provision of financial services and, as such, form the backbone of fintech activities. Policy enablers refer to public policy measures and initiatives (eg digital ID systems) that support the development of fintech activities and the use of enabling technologies.

[1] By Johannes Ehrentraud (Johannes.Ehrentraud@bis.org) and Denise Garcia Ocampo (Denise.GarciaOcampo@bis.org), Bank for International Settlements; Lorena Garzoni (lorena.garzoni@finma.ch), Swiss Financial Market Supervisory Authority; Mateo Piccolo (mateo.piccolo@bcra.gob.ar), Central Bank of Argentina.

The authors are grateful to the contacts at the central banks and financial authorities from the jurisdictions covered in this paper; to Farzana Badat, Juan Carlos Crisanto, Sebastian Doerr, Conor Donaldson, Jon Frost, Leonardo Gambacorta, Jermy Prenio, Camila Quevedo Vega, Tara Rice, Costas Stephanou, Alexandre Stervinou, Nobu Sugimoto, Greg Sutton, Ken Taniguchi, Mahesh Uttamchandani, Joy Wann and Chris Wilson for their helpful comments; and to Mario Barrantes, Carlos Cantu, Emma Claggett, Quentin Jalla, Mathilde Janfils, Esther Künzi, Christina Paavola, Alan Soughley, Tomas Stastny and Barbara Ulloa for their valuable support with this paper. The views expressed in this paper are those of the authors and not necessarily those of the BIS, the Basel-based standard setters or the surveyed organisations of the jurisdictions listed in Annex 1.

Fintech tree: a taxonomy of the fintech environment



Source: FSI staff.

Policy responses to new fintech activities take various forms. Regulatory authorities may respond to fintech activities in a number of ways. For example, authorities may put in place fintech-specific licensing regimes that require entities to go through an authorisation process before they can offer their fintech services. Alternatively or complementarily, they may issue requirements that are fintech-specific, modify existing ones or even prohibit certain activities. Some authorities may take the path of explaining how the existing regulatory framework is applied to fintech business models and clarify their supervisory expectations.

Authorities pursue a range of approaches when regulating fintech activities. For digital banking, licensing regimes or other specific requirements are the exception. Some jurisdictions, however, have launched initiatives to facilitate the establishment of new banks, including digital banks. In the context of fintech platform financing, while most surveyed jurisdictions do not have a dedicated regulatory regime for fintech balance sheet lending, many have one for both loan and equity crowdfunding. For robo-advice, fintech-specific regulations are not common, but around a third of surveyed jurisdictions published guidance on issues that are unique to robo-advice as compared with traditional financial advice. For digital payment and e-money services, most surveyed jurisdictions have specific regulations. Regarding the former, initiatives put in place often aim at strengthening regulatory requirements for non-banks or facilitating their access to the payments market. For technology-driven business models emerging in the area of insurance distribution and underwriting, existing regulations are generally considered as sufficient to address the features and risks of these innovations. Cryptoassets are subject to a wide array of regulatory responses, with warnings and clarifications of the regulatory treatment as the most common response. New crypto-specific licences or authorisations are emerging in a few jurisdictions.

For enabling technologies, regulators have adjusted their existing regulations to add technology-specific elements in existing laws, regulation or guidelines. As a result of the level of market adoption, some technologies have received more attention than others. Regulators have been particularly active on application programming interfaces (APIs), cloud computing and biometric-based identification and authentication. In contrast, for artificial intelligence, machine learning and, to some

extent, distributed ledger technology, authorities have not gone beyond conducting risk assessments and issuing general guidance.

Public policies that enable the provision of digital services have received much attention. Most jurisdictions have implemented digital ID systems that allow financial institutions to verify the identity of their clients. Data protection laws that allocate rights and responsibilities for accessing and sharing consumers' data have been issued in almost all jurisdictions. Also common are national cybersecurity frameworks, supplemented by cybersecurity regulations and guidance specific for the financial sector. Several jurisdictions have adopted, or are in the process of adopting, open banking initiatives. Last, innovation facilitators have frequently been put in place, with innovation hubs as the most common form.

Policy responses to fintech may need to weigh several policy objectives. Achieving an orderly application of new technologies in the financial system will probably remain a desirable outcome of regulatory actions. At the same time, policy actions need to be consistent with the preservation of financial stability, market and financial integrity, competition and consumer protection. Furthermore, the prevention of regulatory arbitrage and the promotion of a level playing field, where appropriate, may be sought while maintaining adequate control of firms with a larger potential to generate systemic risk.

At the international level, authorities are working to address emerging risks and develop schemes that facilitate a coordinated regulatory response for global challenges. This should be stressed given the wide scope in which technological innovations may be applied to the provision of financial services as well as the potential scale that the provision of these services may take, especially where firms with a large customer base enter the market. This could be the case for proposed global stablecoin arrangements that may affect existing financial, monetary and payment systems or global cloud service providers that occupy a dominant position.

Going forward, financial authorities may face further challenges as technology evolves and is applied to new services. Continuous efforts from authorities will be needed to understand novel business models and their underlying risks, to build or maintain the skills and capacity to adequately assess potential implications on financial markets and to adjust their regulatory responses in an agile manner. Only with sufficient resources and access to timely and reliable information will authorities be able to steer innovation in a desirable direction, while minimising potential risks to the financial system. In this context, cooperation and coordination at the local and international level remain essential.

Section 1 – Introduction

1. **Technological innovations in financial services (fintech) are increasingly transforming the way financial services are provided.** Advances in technology such as computing power, cryptography, big data and artificial intelligence – coupled with easier mobile access and increased internet speed and bandwidth – are giving rise to new applications in different sectors of the financial industry. These include new approaches to how credit is extended, payments are made, investment advice is provided, insurance is priced and, more broadly, the way funds are channelled from savers/investors to borrowers.

2. **Fintech opens opportunities but comes with potential risks.** As noted in the IMF/World Bank Bali Fintech Agenda,[2] fintech can support potential growth and poverty reduction by strengthening financial development, inclusion, and efficiency – but it may pose risks to consumers and investors and, more broadly, to financial stability and integrity (IMF and World Bank (2018)).

3. **The regulatory community is monitoring the situation closely.** The global standard-setting bodies (SSBs) have issued a number of documents in recent years, with the aim to provide insight into fintech developments and, more specifically, to explore the implications for the financial sector. For example, the Financial Stability Board (FSB) has not found evidence of fintech innovations having an adverse systemic impact on the financial system (FSB (2017a, 2019a)). An overview of the work produced by the BIS, its hosted committees and its stakeholders on the implications of emerging technologies for the financial sector and the wider economy can be found on the BIS website.[3]

4. **The challenge for policymakers is to maximise the benefits of fintech while minimising potential risks for the financial system.** Achieving this balance is key for allowing innovation that can provide benefits to society without compromising the soundness of the financial system. In particular, policy interventions aim to mitigate the potential risks fintech entails. Financial regulation aims to address market failures and prevent potential risks from materialising by addressing the vulnerabilities and imperfections in the financial system (IMF (2017)). This objective is the same for traditional financial services and fintech. For example, fintech should not enable or make it easier for criminals and terrorists to abuse the financial system for the purposes of money laundering or terrorism financing. People should be treated fairly when using fintech services, and they should have adequate access to payments, credit, insurance and savings products. As such, adequate and proportional regulation may help to prevent future cases of unwanted incidents, such as fraud in crowdfunding (eg Ezubao in China) or in initial coin offerings (ICOs).[4]

5. **Fintech presents policymakers with trade-offs and other challenges.** First, trade-offs may arise between different policy objectives such as financial stability, market integrity, consumer and investor protection, efficiency and competition, and financial inclusion. Second, fintech developments present issues that are not traditionally within the purview of financial authorities, requiring enhanced cooperation with other public bodies. These may include agencies responsible for consumer protection, fair competition and data protection, each with its own mandate and policy objectives. Third, the speed of innovation makes it difficult for regulators facing resource constraints, at times compounded by a lack of in-house technology experts, to respond in a timely manner to developments in the market – fintech firms are not waiting for the regulator to act. Fourth, technology may lead to more decentralisation in the

[2] In 2018, the IMF and the World Bank approved the Bali Fintech Agenda, a set of 12 policy elements aimed at helping their member jurisdictions to harness the benefits and opportunities of fintech, while managing the inherent risks.

[3] For more information on fintech-related publications by the BIS, its hosted committees (Basel Committee on Banking Supervision (BCBS), Committee on the Global Financial System (CGFS), Committee on Payments and Market infrastructures (CPMI), Markets Committee (MC) and Irving Fisher Committee (IFC)) and hosted associations (FSB, International Association of Insurance Supervisors (IAIS) and International Association of Deposit Insurers (IADI)), see www.bis.org/topic/fintech.htm.

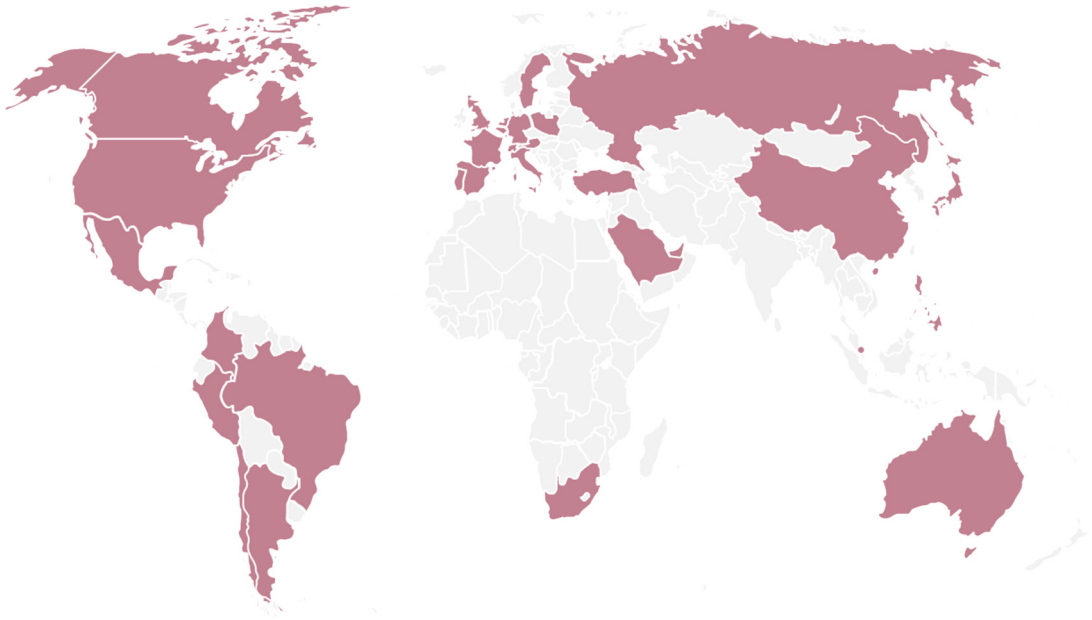
[4] ICO advisory firm Statis Group reported that more than 80% of ICOs conducted in 2017 are thought to have been fraudulent. See research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ.

financial sector, which may pose challenges for financial regulatory and supervisory frameworks (FSB (2019e)).

6. **Financial authorities have resorted to various ways of responding to fintech developments.** For one, regulators may put in place fintech-specific licensing regimes that require entities to go through an authorisation process before they can offer their fintech services. Alternatively or complementarily, they may issue requirements that are fintech-specific, modify existing ones or even prohibit certain activities. Some authorities have taken the path of explaining how the existing regulatory framework is applied to fintech business models and clarifying their supervisory expectations.

7. **This paper provides a cross-country overview of regulatory responses[5] that selected jurisdictions worldwide have taken with respect to fintech developments.** It is based on responses to a survey conducted in early 2019 by the FSI. The survey was supplemented by a desktop review of published documents and the authors' own analysis. The overview is based on a conceptual framework (the fintech tree) that structures the fintech environment in terms of three components: fintech activities, enabling technologies and policy enablers.

Chart 1: jurisdictions covered[6]



Source: FSI survey.

8. **The paper is structured as follows.** Section 2 develops a conceptual framework for categorising different parts of the fintech space in order to allow for a meaningful comparison across jurisdictions. Sections 3 to 5 outline the authorities' approaches in relation to fintech activities, enabling technologies and policy enablers. Sections 6 and 7 outline future challenges and conclude.

[5] Regulatory responses cover policy instruments issued by supervisory authorities to regulate the provision of financial services (eg laws, regulations, guidance) as well as public policy measures (eg national frameworks, initiatives) developed by government bodies (eg competition, consumer protection, cyber security/data protection authorities) to enable innovation in the provision of financial services and adoption of digital services more broadly.

[6] See Annex 1 for a complete list of jurisdictions covered in this paper.

Section 2 – The fintech environment

9. **The devil is in the definitions.** Given fintech is a young area, it is not surprising that the terms used within the fintech space are often not free from ambiguity. Market participants and regulators at times use different terms for the same activity, or the same term for different ones. For example, the terms fintech credit, peer-to-peer lending, crowdlending, lending-based crowdfunding or simply crowdfunding are often used interchangeably.[7] At the international level, acknowledging the need for clear definitions, both FSB (2017a) and BCBS (2018) feature glossaries of fintech terms.[8] Building on these, in Annex 2 we provide a list of terms and their definitions used in this paper. These aim to facilitate the cross-country comparison of regulatory approaches in Section 3.

10. **For the purposes of this paper, we adopt the FSB's working definition for fintech.** The FSB defines fintech as "technologically enabled financial innovation that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services" (FSB (2017a)). Given our focus on regulating fintech, we find this umbrella term helpful in defining the scope of this paper. But its broad nature brings with it the need for more specificity.

Conceptual framework: the fintech tree

11. **At the international level, SSBs and other international organisations have developed categorisations and frameworks through which they analyse fintech.** For example, under the FSB framework, fintech innovations are classified according to the primary economic function they provide.[9] Building on the FSB work, the BCBS developed a categorisation of fintech innovations based on three sectors related to core banking services,[10] supplemented by so-called market support services such as data applications or cloud computing (these are not specific to the financial sector but significant for fintech developments (BCBS (2018)).

12. **Building on this work, we propose a conceptual framework referred to as the "fintech tree" (Chart 2).** To characterise the fintech environment, we distinguish three categories: fintech activities, enabling technologies and policy enablers. Fintech activities, or technologically enabled provision of financial services, can take various forms and encompass the different sectors of the financial industry. Enabling technologies are those that make innovation possible in the provision of financial services and, as such, form the backbone of fintech activities. Policy enablers refer to public policy measures and initiatives that support the development of fintech activities and the use of enabling technologies.

13. **The fintech tree allows us to classify fintech-related regulatory approaches and policy responses in three groups.** These refer to: (i) those that adjust the regulatory perimeter and/or directly target fintech activities; (ii) those that focus on the use of new technologies in the provision of financial

[7] In the United States, crowdfunding is understood as an umbrella term for equity, reward and donation crowdfunding activities, and the term marketplace lending is more common for credit activities intermediated by platforms. (Havrylchyk (2018)).

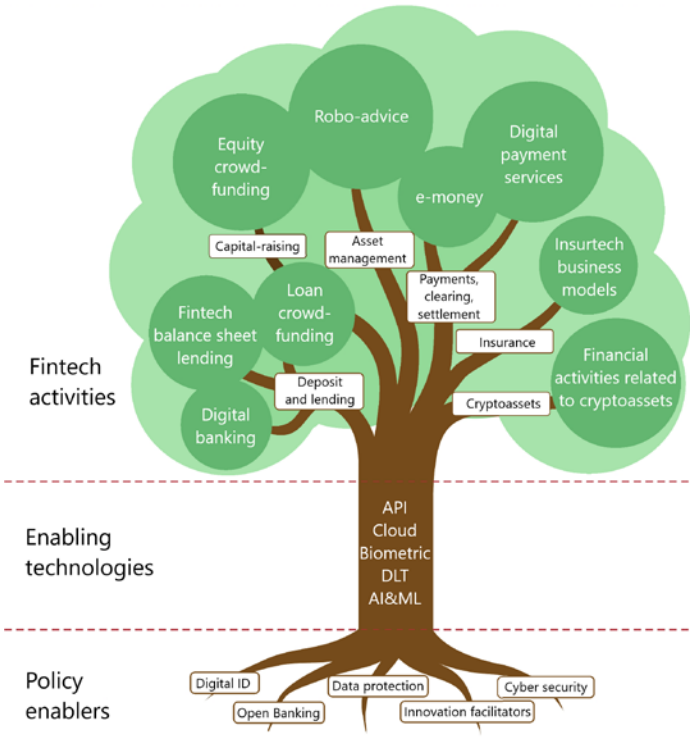
[8] The Committee on Payments and Market Infrastructures (CPMI) provides an online glossary of payments and market infrastructure terminology as a reference to the standard terms and definitions used in connection with payment, clearing, settlement and related arrangements.

[9] Drawing on the categorisation in WEF (2015), the FSB framework classifies fintech activities into five categories of financial services: (i) payments, clearing and settlement; (ii) deposits, lending and capital-raising; (iii) insurance; (iv) investment management; and (v) market support (FSB (2017a)).

[10] The three sectors are: (i) credit, deposit and capital-raising services; (ii) payments, clearing and settlement services; and (iii) investment management services.

services; and (iii) those that facilitate financial innovation or promote digital financial services more broadly.

Chart 2: fintech tree: a taxonomy of the fintech environment



Source: FSI staff.

Fintech activities: the treetop

14. **Fintech activities are performed in different sectors of the financial industry.** In terms of the fintech tree classification, fintech activities can be found in the following financial services categories: (i) deposits and lending; (ii) capital-raising and alternative sources of funding; (iii) asset management, trading and related services; (iv) payments, clearing and settlement services; (v) insurance; and (vi) cryptoassets. These financial services categories build on the FSB categorisation (2017a), with the difference that we have singled out cryptoassets and related financial activities. We acknowledge that most cryptoassets could be classified under the other categories of financial services, depending on their underlying economic function, rights attached and business model features. Yet we decided to keep them separate for the purposes of this paper because crypto-related services involve a range of unique approaches with quickly evolving use cases.

15. **This paper is based on a large but not exhaustive set of specific fintech activities.** Based on the results of our survey, the fintech tree features digital banking, fintech platform financing (crowdfunding and fintech balance sheet lending), robo-advice, e-money, digital payment services, insurtech and financial activities related to cryptoassets. What follows is a brief description of each of these fintech activities.

- **Digital banking.** Differences in regulatory regimes across jurisdictions imply that a type of entity considered to be a bank in one jurisdiction may not be considered to be a bank in another.[11] In

[11] A somewhat narrow definition of a bank includes taking deposits and granting loans (for example, as applied in the Capital Requirements Regulation (CRR) of the European Union). However, authorisation requirements to perform certain activities differ

this paper, we define digital banks (eg KakaoBank and KBank (both Korea), WeBank and MyBank (both China), Monzo (UK), Nubank (Brazil) and N26 (mostly Europe)) as deposit-taking institutions that are members of a deposit insurance scheme[12] and deliver banking services primarily through electronic channels instead of physical branches. This second element, in terms of this definition, implies that the business model of a digital bank relies heavily on technology, and this is what distinguishes it from a traditional bank.

- **Fintech platform financing.** Several fintech activities are facilitated by electronic platforms that provide a mechanism for intermediating financing over the internet.[13] Platforms make extensive use of technology and data. We distinguish the following types:

  - **Fintech balance sheet lending** refers to credit activity facilitated by internet-based platforms (not operated by commercial banks) that use their own balance sheet in the ordinary course of business to intermediate borrowers and lenders. Importantly, balance sheet lenders (eg WeLend in Hong Kong SAR and Quicken Loans in the United States[14]) do not obtain funding from the "crowd" but rely on other sources, such as own capital or debt issuance. Balance sheet lending platforms enter directly into loan contracts with their borrowers and assume credit risk by keeping originated loans on its balance sheet, at least until they are sold to investors.

  - **Crowdfunding.** The term crowdfunding refers to the practice of matching people and companies raising funds with those seeking to invest for a financial return without traditional financial institutions as intermediaries.[15] There are two major types. The first, equity crowdfunding, refers to an activity where investors provide funding to private companies in the form of equity. The fintech platform matches investors with companies they want to invest in, enabling them to participate in the early capital raising activities of startups and other companies. The second, loan crowdfunding, refers to credit activity facilitated by internet-based platforms (not operated by commercial banks) that match borrowers with lenders.[16] Here, individual loan contracts are established between borrowers and lenders, without the platform being engaged in risk transformation. While this definition is in principle consistent with that of fintech credit in Claessens et al (2018) and CGFS-FSB (2017), our definition of loan crowdfunding excludes fintech

across jurisdictions. Regulations in some jurisdictions provide licensing categories for various types of banking business and, for example, require entities to hold a banking licence even if they only engage in granting loans. This is the case, for example, in Austria and Germany.

[12] This defining element of a bank in the narrow sense appears to be consistent with the understanding of a number of regulatory agencies. For example, according to the Australian Prudential Regulation Authority (APRA), "financial institutions that take customer deposits occupy a unique position of trust within the community. The financial safety of these institutions is key to the financial stability and economic well-being of the community and, as a result, these institutions are subject to higher standards than many other sectors of the economy" (APRA (2018a)).

[13] Or some other application or electronic medium.

[14] Quicken Loans is the largest mortgage lender in the United States. While it services almost all the loans it originates until they are paid off, for refinancing purposes, it offers the loans it originates to mortgage investors, often one of the three government-owned or government-sponsored corporations that deal in mortgages (Fannie Mae, Freddie Mac and Ginnie Mae). See the Quicken Loans website.

[15] Crowdfunding as defined in this paper excludes reward and donation crowdfunding because these activities do not entail a financial return for the people giving money and are therefore typically not subject to financial regulation. However, if a reward or donation crowdfunding platform processes or initiates payments related to its activities for its customers, it may be required to obtain a payments licence. In addition, it may be subject to consumer protection regimes and anti-money laundering and combating the financing of terrorism (AML/CFT) requirements.

[16] Fintech platforms facilitate various forms of credit, including consumer and business lending, lending against real estate, and non-loan debt funding such as invoice financing (CGFS-FSB (2017)).

balance sheet lending. This is necessary because regulatory frameworks treat fintech balance sheet lending differently.

- **Robo-advice**, or automated digital advice, refers to financial advice on investment products that is provided with no or limited human intervention and relies on technology to automate the client onboarding process and the generation of advice through algorithm-based tools.
- **Digital payment services.** Digital payment service providers make use of technology to facilitate payment transactions[17] by transferring money, clearing or settling balances digitally, without the use of physical money. As such, they digitally channel funds from payers to payees by either handling payers' money themselves or initiating payment orders on behalf of payers with respect to transaction accounts held at other financial institutions.
- **E-money services** refer to the issuance of debt-like instruments (e-money[18]) for the purpose of facilitating payment transactions. From a balance sheet perspective, e-money represents a fixed value claim on its issuer (e-money provider) that guarantees redemption at a pre-established face value denominated in fiat currency (Adrian and Mancini-Griffoli (2019)). Furthermore, for a claim to be considered e-money, it needs to (i) serve as a multipurpose medium of exchange; (ii) be accepted as a means of payment by parties other than the issuer; and (iii) be issued only on receipt of funds (e-money is prepaid).[19]
- **Insurtech buisness models.** Insurtech refers to the insurance-specific branch of fintech. In the insurance sector, the term insurtech is used to refer both to the use of digital technologies as well as to new business models that have the potential to transform the insurance business (IAIS (2017)). For this paper, we will refer to the latter when analysing insurtech. In this context, insurtech business models refer to technology-driven innovative models that are emerging in two major areas of insurance: (i) distribution, such as comparison portals and digital brokers; and (ii) underwriting, such as mobile, on demand, usage-based or technology-enabled peer-to-peer and parametric insurance.
- **Financial activities related to cryptoassets**. There is no common definition and categorisation of cryptoassets and related financial activities. Rapidly changing technologies and new business models in this area pose a challenge in defining a taxonomy for this type of assets. For this paper, we adopt the FSB definition, which defines a cryptoasset as a type of private asset that depends primarily on cryptography and distributed ledger or similar technology as part of their perceived or inherent value (FSB (2019b)). In general, most of the financial activities related to cryptoassets are similar to existing ones in traditional markets. For this paper, financial activities related to cryptoassets include creating, distributing, storing or exchanging cryptoassets, using them for investment or payment purposes, or as reference in financial products.

Enabling technologies: the trunk

16. **Currently, multiple technologies are enabling innovation in the financial sector.** These include, but are not limited to, application programming interfaces (API), artificial intelligence (AI) and machine learning (ML), biometric-based identification and authentication (biometrics), cloud computing (CC) and distributed ledger technology (DLT).

[17] The CPMI defines a payment as "the payer's transfer of a monetary claim on a party acceptable to the payee. Typically, claims take the form of banknotes or deposit balances held at a financial institution or at a central bank" (CPSS (2004)).

[18] Money may be issued or stored electronically – eg on a device such as a chip card (eg payment cards), a hard drive in a personal computer or a server – with the purpose of replacing physical money in payment transactions.

[19] E-money needs to be distinguished from payment instruments that only allow (remote) access to a customer's account (CPSS (2004)).

17. **These technologies present new opportunities for the financial industry and have a large number of use cases.** APIs have mainly been used to facilitate access to customers' payments and account information by non-bank firms in a regulated and secure way. CC enables the storage, management and processing of large volumes of data under an efficient, scalable and flexible IT scheme. DLT is being applied to raise efficiency, reduce costs and lessen the need for intermediation although the most prominent application are cryptoassets. Biometric data are increasingly employed for the purpose of customer authentication in mobile banking applications. Predominant areas of AI and ML applications have been credit scoring, high-frequency trading and robo-advice.

Policy enablers: the roots

18. **As the roots of the fintech tree, policy enablers are critical to its stability and health.** For digital financial services to develop in a market, government bodies are setting up public policies and initiatives that create the foundations of a digital infastructure required for providing such services. These may include creating a national broadband network, developing digital identities and authentication systems, promoting interoperability of critically important networks and platforms (eg telecoms, banking systems), and establishing overarching frameworks/strategies for data protection and cyber security either at the national level or for the financial industry, amongst others.

19. **In addition, some jurisdictions have also set up initiatives that facilitate the adoption of innovations in their financial systems.** These include innovation hubs, regulatory sandboxes and innovation accelerators. In adition to promoting innovative developments in a safe environment that protects consumers, these initiatives also provide authorities with an understanding of how technology is applied, the rationale behind new business models and the elements to assess whether the regulatory perimeter needs to be adjusted.

Section 3 – Regulatory responses to fintech activities

20. **This section gives an overview of regulatory responses to fintech activities (Table 1).**[20]

Fintech activities — Table 1

Financial services	Deposits and lending	Capital-raising	Asset management	Payments, clearing, settlements	Insurance
Fintech activities	Digital banking	Equity crowdfunding	Robo-advice	E-money services	Insurtech business models
	Fintech balance sheet lending			Digital payment services	
	Loan crowdfunding				
Cryptoasset-related activities					

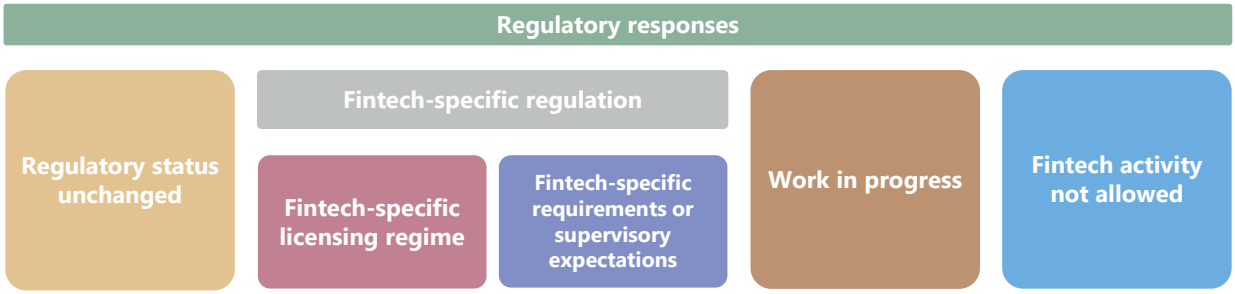
Source: FSI staff.

[20] Complementarily, in 2019, the World Bank and the Cambridge Centre for Alternative Finance presented findings of a global survey on the regulatory treatment of alternative finance activities (WB and CCAF (2019)), and the IMF and the World Bank published a survey-based report on fintech developments around the globe (IMF and WB (2019)).

21. **In order to identify regulatory approaches that are fintech-specific, we need to operationalise the FSB's working definition of fintech.** For this paper, regulatory responses for fintech activities are classified on the basis of the following typology (Chart 3):

- **Regulatory status unchanged:** no change in the exisiting regulatory framework to include fintech activities. In this category, authorities may clarify how existing requirements apply to fintech activities, without introducing any new fintech-specific elements in their regulatory framework.
- **Fintech-specific regulation:** change in the existing regulatory framework to include fintech activities. This category includes cases where regulatory instruments such as laws, regulations or guidelines were issued or amended to regulate fintech activities or otherwise include fintech-specific elements. We do not distinguish between requirements that are legally binding and those that set supervisory expectations.[21] We distinguish, however, between fintech-specific licensing regimes and other requirements or supervisory expectations that are specific to fintech.
- **Work in progress:** work in progress to amend the regulatory framework to include fintech activities.
- **Fintech activity not allowed:** new law or regulation enacted specifically to prohibit a certain fintech activity.

Chart 3: classification of regulatory responses to fintech activities[22]



Source: FSI staff.

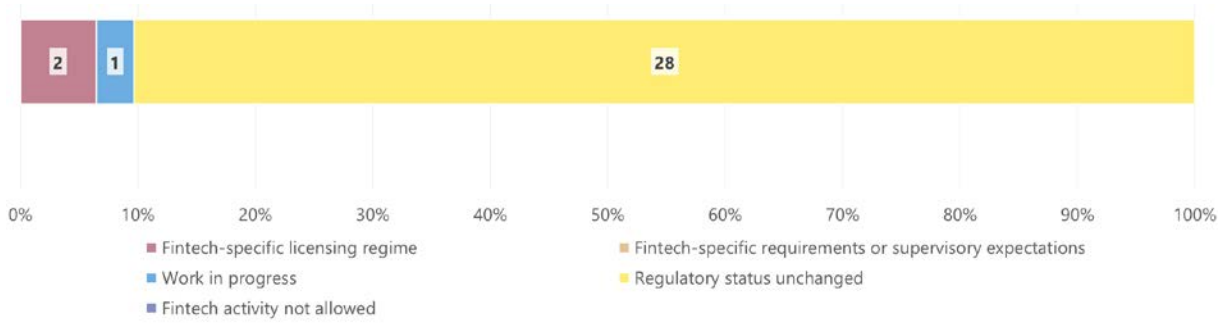
Digital banking

22. **Most jurisdictions apply existing banking laws and regulations to digital banking (Chart 4).** This means that applicants for a banking licence with a fintech business model need to pass through the same licensing process and face the same regulatory requirements as applicants with a traditional business model.

[21] The culture and broader framework for policymaking differ across jurisdictions. In some, to achieve a given objective, authorities often issue rules that create legally binding obligations for regulated entities. In others, they issue guidelines or similar documents that set supervisory expectations. While these policy instruments may not be binding on regulated entities in a legal sense (eg non-compliance does not automatically lead to violation of the law), de facto they are perceived as such by regulated entities. This is because regulators typically have various means to enforce compliance, eg by invoking more general provisions on safety and soundness under the law.

[22] First, EU-wide regulatory regimes are counted at the national level in each surveyed jurisdiction where they apply. Other initiatives by EU institutions are mentioned in the text but are not counted as a separate category in the charts. Second, only initiatives at the federal level are considered so each jurisdiction can only be counted once (eg initiatives at the state level in the US are not considered). For the United Arab Emirates, initiatives in Abu Dhabi and Dubai are considered as well.

Chart 4: regulatory responses for digital banking



Sources: National regulations; FSI survey.

23. **Specific licensing regimes for digital banks were put in place in only a few jurisdictions.** These are Hong Kong SAR and Singapore.[23, 24]

- **Virtual banks in Hong Kong**. In May 2018, the Hong Kong Monetary Authority (HKMA) published a revised "Guideline on authorization of virtual banks",[25] setting out the principles which the HKMA will take into account in deciding whether to authorise "virtual banks"[26] applying to conduct banking business in Hong Kong. For applicants to obtain a licence, the HKMA needs to be satisfied that the minimum criteria for authorisation in the Banking Ordinance are met.[27] This means that a virtual bank needs to operate in the form of a locally incorporated bank, have parent companies that are committed to and capable of supporting the bank; maintain a physical presence in Hong Kong as its principal place of business (but no branches); establish appropriate risk management controls (especially for technology, liquidity, operational and reputation risk); and operate on the basis of a business plan that strikes an appropriate balance between building market share and earning a reasonable rate of return on assets and equity.[28] In terms of consumer protection, virtual banks are expected to treat their customers fairly and adhere to the Treat Customers Fairly Charter.[29]

[23] In the United Arab Emirates, in November 2018, a new law came into effect which defines the provision of virtual banking services as "licensed financial activity" subject to licensing and supervision. There is currently no further guidance, and it remains to be seen whether and how requirements for virtual banking licences differ from those for traditional banks.

[24] Services related to digital banking may also be supported types of licences that enable different fintech activities. Some authorities have introduced licensing regimes that enable fintech companies from various sectors to perform a specific regulated activity, instead of targeting a specific fintech business model. Two examples are the new fintech licence in Switzerland and the planned Special Purpose National Bank Charter for fintech companies by the Office of the Comptroller of the Currency (OCC) in the United States (see Annex 3). However, because these two licences do not allow their holders to have insured deposits, they fall outside our definition of digital banking.

[25] Subsequently, in June 2018, the HKMA updated "Chapter 9: Authorization of virtual banks" of the Guide to Authorization. The Guide sets out the HKMA's interpretation of the minimum authorisation criteria and the procedures for processing applications for authorising banks. In particular, it provides guidance to institutions seeking authorisation under the Banking Ordinance about the scheme of supervision contained in the Ordinance and the policies and approach of the HKMA in implementing it. See HKMA (2018a).

[26] A virtual bank is defined as a bank which primarily delivers retail banking services through the internet or other forms of electronic channels instead of physical branches.

[27] These minimum criteria need to be fulfilled by any applicant and are not specific to fintech. See HKMA (2018b).

[28] Other areas covered are ongoing supervision, technology risk, requirements on the business and exit plan, outsourcing and capital requirements.

[29] In addition, virtual banks should observe the standards contained in the Code of Banking Practice issued by the Hong Kong Association of Banks and the DTC Association.

- **Digital banks in Singapore.** In June 2019, the Monetary Authority of Singapore (MAS) announced a new digital banking framework.[30] It comprises two licences: (i) the digital full bank (DFB) licence, which allows licensees to provide a wide range of financial services and take deposits from retail customers; and (ii) the digital wholesale bank (DWB) licence, which allows licensees to serve small and medium-sized enterprises (SMEs) and other businesses but not accept deposits in Singapore dollars from individuals (except for fixed deposits of at least SGD 250,000). The licensing regime provides a phase-in approach for DFB licences: specifically, a DFB will commence operations as a "restricted DFB" with restricted activities and corresponding lower paid-up capital before progressing to a full functioning DFB with the same scope of activities and requirements as other full banks.[31] For DFB licences, the Monetary Authority of Singapore (MAS) will only consider applicants who are anchored in Singapore, controlled by Singaporeans and headquartered in Singapore. To obtain a digital bank licence, an applicant (or its parent group) must have a track record in operating an existing business in the technology or e-commerce field, provide clear value propositions on how it can serve existing unmet or underserved needs, and demonstrate that it has a sustainable digital banking business model. The digital banks have to be incorporated in Singapore, comply with the same suite of prudential rules as incumbent banks, and provide a viable exit plan to facilitate an orderly wind-up if necessary. In addition, the DFB is required to participate in the deposit insurance scheme provided by the Singapore Deposit Insurance Corporation.

24. **In the euro area, the ECB issued specific guidance on how credit institution authorisation requirements would apply to applicants with new fintech business models.** In 2018, the ECB provided guidance on its supervisory expectations when considering licence applications from fintech companies. As such, the guide – which is technology-neutral – aims to facilitate the application process by increasing the understanding of the procedure and criteria applied by the ECB and therefore fostering a consistent assessment of these new business models within the Single Supervisory Mechanism (SSM) (ECB (2018)). While fintech banks are held to the same authorisation standards as other banks, the guide highlights supervisory considerations with respect to the specific nature of banks with fintech business models, in particular on: (i) suitability of the members of the management body (IT competence, financial competence, fitness and propriety); (ii) suitability of shareholders (reputation and financial soundness of shareholders with a qualifying holding); (iii) structural organisation (credit scoring and governance,[32] IT-related risks, outsourcing, data governance and security); (iv) programme of operations (execution risks arising from the business model, exit plans); and (v) capital, liquidity and solvency assessment.

25. **In the absence of digital banking-specific regulation, some jurisdictions launched initiatives to facilitate the establishment of new banks.** In Australia, APRA, in May 2018, established a new licensing regime, allowing eligible applicants to conduct limited banking business for two years without being subject to the full set of prudential requirements. In the UK, the Prudential Regulation

[30] The MAS internet banking framework introduced in 2000 is not applicable to non-banks, as it was intended to facilitate only Singapore-incorporated banking groups to set up banking subsidiaries with a lower paid-up capital requirement to pursue new business models, including internet-only banking.

[31] Digital full banks commence operations as a Restricted DFB, in which (i) deposits can only be accepted from a limited scope of customers such as business partners, staff and related parties; (ii) aggregate deposits are capped at SGD 50 million and individuals' deposits at SGD 75,000; (iii) only simple credit and investment products can be offered; and (iv) a lower minimum capital requirement at the entry point of SGD 15 million. After the entry phase, the deposit cap and minimum paid-up capital requirement of the Restricted DFB will be progressively increased until it is a fully functioning DFB, ie business and deposit restrictions are lifted but the minimum paid-up capital requirement increases to SGD 1.5 billion.

[32] For example, the ECB will assess how the fintech bank would check customers' repayment capability, given that it may not have the necessary information to build an internal credit scoring model. Moreover, fintech banks intending to operate in more than one jurisdiction are expected to consider jurisdiction-specific credit scoring processes.

Authority (PRA) and the Financial Conduct Authority (FCA) established the New Bank Start-up Unit to provide information and support to potential applicants for a bank licence. While not limited to digital banks or fintech companies in general, both are likely to benefit from initiatives by regulators that aim to lower barriers to entering the banking sector. These initiatives aim to enable potential applicants to understand and navigate the licensing process or to allow them some time before they have to meet the requirements of the prudential framework in full.[33]

- **Restricted authorised deposit-taking institutions (ADIs) licensing framework in Australia.** APRA's new licensing regime for financial entities allows restricted ADIs to conduct a limited amount of low-risk business for up to two years. As such, restricted ADIs are expected to have a balance sheet not greater than AUD 100 million and deposits in protected accounts below AUD 2 million on aggregate. After two years, licence holders must either meet the full prudential framework or wind up their banking business. The framework is not introducing a new licence with relaxed requirements but aims to assist potential new entrants to the banking industry.[34] While the restricted ADI licence is not limited to applications from entities with fintech business models, the first such licence was granted to a digital bank.[35]
- **New Bank Start-up Unit in the United Kingdom.** In January 2016, the PRA launched the New Bank Start-up Unit and published a guide to help firms, including fintech companies, understand the regulatory requirements of being a bank, and provide practical information on the application process. The New Bank Start-up Unit Guide (PRA and FCA (2018)) is updated frequently to ensure firms have the most up to date information on regulatory requirements. It also holds frequent seminars to help firms understand regulatory expectations.

Fintech platform financing

26. **Fintech platforms perform several financial activities.** Some fintech platforms may accept money from investors on their balance sheet, which is then lent out to borrowers or used to buy securities. Others may act exclusively as brokers between investors and those seeking funding. Some platforms that intermediate lending may use their own balance sheet to retain some of the credit risks ("skin in the game"); others may pass the entirety of credit risks on to investors.[36] In addition, platforms are often issuers of securities or of interests in collective investment schemes, or they offer or deal in securities (IOSCO (2017)).

27. **Without a fintech-specific regulatory regime in place, the business model of a fintech platform determines its regulatory treatment.** In broad terms, the requirements for platform financing depend on: what types of activities are performed; what types of entities/parties are involved; who performs which activity; and who bears the risk (Chart 5).

- **Banking regulation.** A platform whose business model involves taking deposits from the public and holding these together with own funds typically need some form of banking licence. In some countries, a bank licence is also required for granting loans, even if the platform does not take

[33] In other jurisdictions, regulatory sandboxes may be established to pursue similar objectives.

[34] The framework establishes the eligibility criteria, minimum initial and ongoing requirements and application of the prudential and reporting standards during the restricted phase of operation. It also acts as a guide to help restricted ADI applicants navigate the licensing process.

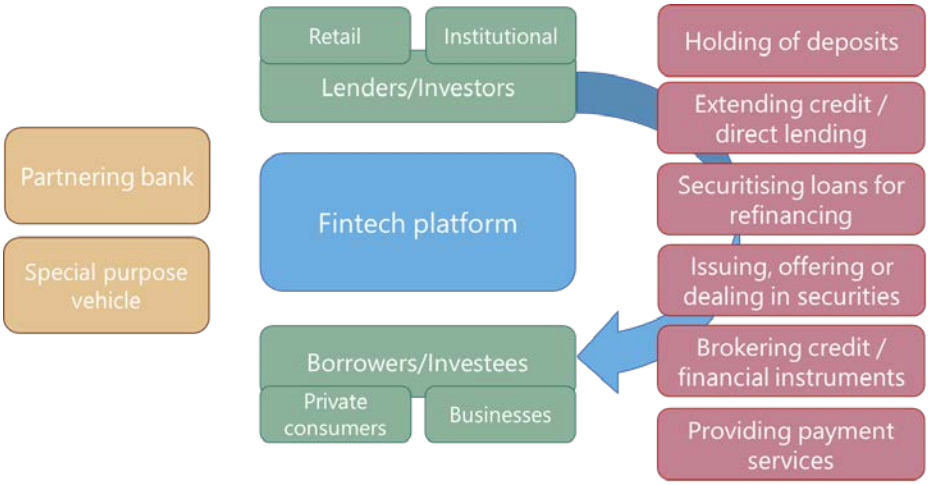
[35] In May 2018, APRA authorised Volt Bank Limited as a restricted ADI under the Australian Banking Act. The conditions attached to its authorisation followed the new framework and were publicly available on APRA's website. In January 2019, APRA granted Volt Bank Limited a licence to operate as ADI without any restrictions.

[36] See CGFS and FSB (2017) for a discussion of different models for loan crowdfunding.

deposits. To avoid this, fintech platforms may involve third-party banks that originate the loans, which are then assigned to investors (CGFS and FSB (2017)). If the third-party bank does not retain the loans, it may sell them to the platform or other investors by making use of a special purpose vehicle.

- **Securities regulation.** If a platform issues and sells securities (eg to finance the purchase of loans), provides related investment advice or establishes secondary markets for the loans or investments it intermediates, it is typically subject to licensing or registration requirements under securities regulation. In case a platform acts as an intermediary by transmitting buy or sell orders in relation to financial instruments, it may provide a regulated investment service (brokerage of financial instruments). Moreover, offering securities to the broad general public typically requires the publication of a prospectus, which needs to be approved by the securities regulator.[37]
- **Payments regulation.** A platform may not only intermediate financing but also provide payment services (eg initiation of payments on behalf of the customer), in which case licensing and oversight requirements in the payments space apply. For example, a platform may operate payment accounts which it uses to channel payments between its clients. Or it may initiate payments on behalf of clients from clients' payment accounts held elsewhere.

Chart 5: activities involved in fintech platform financing

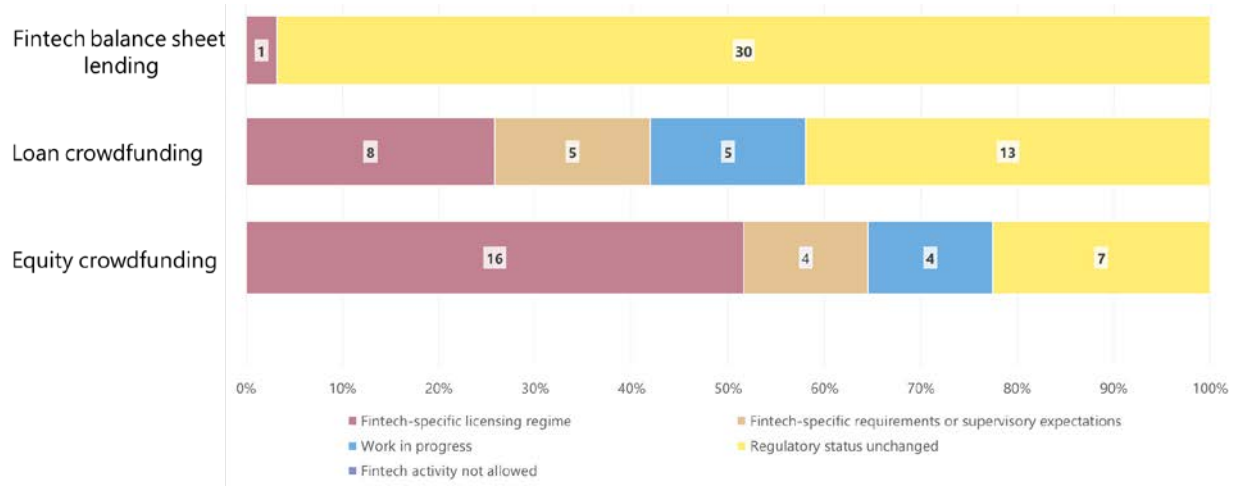


Source: FSI staff.

28. **Dedicated regulatory regimes for platform financing typically target a specific business model.** Building on the definitions in Section 2, in what follows we differentiate between fintech balance sheet lending, loan crowdfunding and equity crowdfunding, because we found that regulatory requirements distinguish between these three platform financing models (Chart 6).

[37] See ESMA (2019) for an overview of thresholds below which the obligation to publish a prospectus does not apply in the European Union.

Chart 6: regulatory responses for fintech platform financing



Sources: National regulations; FSI survey.

Fintech balance sheet lending

29. **Most jurisdictions do not have regulations that are specific to fintech balance sheet lending (Chart 6).** Therefore, it is subject to a variety of regulatory approaches that in most cases centre on the extension of credit as a regulated activity. In a few jurisdictions, the business of making loans requires a banking licence (eg Austria and Germany). In others, specific licensing regimes exist for non-banks that are in the business of granting loans without taking deposits. For example, in Hong Kong any person (or corporation) who carries on business as a money lender (eg making loans) must obtain a money lender's licence.[38] In both cases, under existing regulation, it is irrelevant whether a customer obtains a loan through an online platform's website or a physical signature in a brick-and-mortar branch.

30. **Only one of the surveyed jurisdictions has introduced a dedicated licensing regime for fintech balance sheet lending.** In Brazil, in April 2018 the National Monetary Council issued a new resolution that introduced direct credit companies (sociedades de crédito direto, SCD) as a new type of financial institution, whose operation requires a licence by the Central Bank of Brazil. The resolution defines SCDs as financial institutions that: (i) provide loans and financing and acquire collection rights;[39] (ii) operate exclusively on the basis of an electronic platform; and (iii) are funded exclusively through equity capital. SCDs are not allowed to raise capital from the public, except by means of issuing shares, and may sell or assign the originated loans only to financial institutions, specific investment funds or securitisation vehicles.[40] SCDs are subject to minimum capital requirements (BRL 1,000,000) and prudential supervision.

Loan and equity crowdfunding

31. **Loan and equity crowdfunding involve similar underlying activities.** Crowdfunding platforms connect those who can lend or invest money directly with those who need financing for a specific project. As such, both loan and equity crowdfunding platforms broker financial products whose financial returns depend on their future cash flows.[41] Both target the general public (the "crowd") over the internet and

[38] Money lenders are licensed in Hong Kong. Applications for money lender licences are subject to approval by the Licensing Court; the Hong Kong Police Force is responsible for enforcement; and the Registrar of Money Lenders (RML) is responsible for handling administrative matters.

[39] SCDs may also provide additional services such as credit analysis, loan collection, distribution of insurance products and electronic money issuance.

[40] The latter two investment possibilities are restricted to qualified investors.

[41] See definition of crowdfunding by European Commission.

match buyers and sellers in a manner comparable with a marketplace like a stock exchange. Both do not engage in risk transformation and balance sheet intermediation – losses are born by lenders or investors – and earn their profits from fees rather than carrying risks.

32. **These similarities give rise to similar risks.** Despite differences in the type of financial products, crowdfunding platforms give rise to comparable risks. The first is investor/consumer protection. A platform may unexpectedly fail, engage in fraudulent behaviour or enable parties seeking funding to commit fraud. Moreover, lenders or investors have to rely on the platform for accurate information. They do not know the quality of borrowers or investment projects and may have to rely on the platform for sound due diligence and risk assessment.[42] Second, both platform types are subject to operational risks, such as the risk that identity, payments or other data could be stolen through cyber attacks.

33. **Many surveyed jurisdictions introduced fintech-specific regulations that apply to both loan and equity crowdfunding (Table 2).** Most of these regulations were put in place in 2018. In terms of policy objectives, customer protection has been the most cited by authorities, followed by level playing field issues and financial stability. Often, crowdfunding platforms need to be licensed or registered before they can perform crowdfunding activities, and satisfy certain conditions. Although there may be only one type of licence for both activities, the regulatory framework typically includes requirements that apply to both activities and requirements that apply to either loan or equity crowdfunding.

Fintech-specific regulations for crowdfunding Table 2

Equity crowdfunding		Equity and loan crowdfunding		Loan crowdfunding
Argentina	Colombia	Belgium	Peru*	Australia
Australia	Italy	Canada	Philippines	Brazil
Austria	Japan	Chile*	Singapore	China
Brazil	Turkey	European Union**	Spain	Italy
China	United States	France	Sweden*	United Arab Emirates***
		Mexico	United Arab Emirates***	
		Netherlands	United Kingdom	

(*) Work in progress. In Peru, crowdfunding through issuance of securities (debt or equity) is currently not being authorised, but work is under way to introduce a new framework for different types of crowdfunding.

(**) Proposal by European Commission. Once adopted at the EU level, the new regulation will allow platforms to apply for an EU passport based on a single set of rules. See EC (2018a).

(***) Dubai and Abu Dhabi have the same regulatory framework for both ECF and LCF. At the UAE level, the central bank issued a draft regulation on LCF.

LCF=loan crowdfunding. ECF=equity crowdfunding. The Swiss fintech licence and, once implemented, the OCC fintech charter may also enable fintech platform financing activities.

Sources: FSI survey; desktop research.

[42] Investors are compensated for bearing the risk that the issuer or borrower may default. The higher this risk, the higher the compensation should be.

34. **Around a third of surveyed jurisdictions have fintech-specific regulations exclusively for equity crowdfunding[43] (Chart 6).** When issuing fintech-specific regulations, most authorities seek not only to enhance investor protection, but also to expand the direct financing channels for SMEs.

35. **Only a few jurisdictions have a dedicated licensing regime exclusively for loan crowdfunding (Chart 6).** In Brazil, in April 2018 the National Monetary Council issued a new resolution that introduced peer-to-peer loan companies (sociedade entre pessoas, SEP) as a new type of financial institution, whose operation requires a licence by the Central Bank of Brazil.[44] In China, loan crowdfunding is regulated under the regulatory framework for internet finance. Under Chinese regulation, loan crowdfunding platforms are treated as information intermediaries that act as brokers between lenders and borrowers.[45] In Australia, although there is no fintech-specific licensing regime, so-called marketplace lending providers (MLPs) can use existing regimes linked together with a tailored Australian Financial Services (AFS) Licence granted by the Australian Securities and Investments Commission (ASIC) in order to provide crowdfunding services and/or an Australian Credit Licence if the platform is extending consumer loans.

36. **In most cases, regulatory requirements focus on consumer and investor protection, anti-money laundering (AML) and combating the financing of terrorism (CFT) and on operational resilience.** Depending on the jurisdiction, crowdfunding platforms also face requirements, inter alia, on transparency, risk management, governance and business continuity (see Table 1 in Annex 4). Nevertheless, the details of requirements vary (see Table 2 in Annex 4).

Robo-advice

37. **In principle, robo- and traditional advisers receive the same regulatory treatment.**[46] Robo-advisers are typically classified as providers of financial advice under securities regulation and need to be authorised by the securities regulator, irrespective of whether the advice is provided digitally, face to face or a mix of both. In that sense, regulatory regimes for financial advice are technology-neutral. This follows from the idea that clients of robo-advisers should enjoy the same level of protection and quality of advice as those of traditional advisers.

38. **Consequently, the majority of surveyed jurisdictions do not have fintech-specific regulations for providers of robo-advice (Chart 7).** In the absence of a fintech-specific licensing regime or other specific requirements, robo- and traditional advisers need to go through the same licensing process and are in principle subject to the same regulatory requirements. These requirements depend on a variety of factors,[47] such as the:

- *type of advice*. In many jurisdictions, only the provision of personalised advice (in contrast to factual or general advice) falls within the regulatory ambit. Within personalised advice, less

[43] In some jurisdictions, dedicated regulatory regimes for equity crowdfunding also allow the intermediation of debt securities.

[44] The resolution defines SEPs as financial institutions that: (i) direct funds collected from creditors to debtors; (ii) operate exclusively on the basis of an electronic platform; and (iii) are prohibited from using own capital to fund loans and from retaining any credit risk. SEPs may also provide additional services such as credit analysis, loan collection, distribution of insurance products and issuance of electronic money. For non-sophisticated investors, a maximum limit of BRL 15,000 applies per debtor in a given SEP. SEPs are subject to comprehensive disclosure requirements and minimum capital requirements (BRL 1,000,000).

[45] Among other things, platforms are required to: (i) register with the local financial regulatory department; (ii) disclose relevant information on the basis of "authenticity, accuracy, completeness and timeliness"; and (iii) deposit clients' funds in commercial banks. See Yu and Shen (2019) for more details; their Table 2, they provide a list of major regulations on loan crowdfunding in China.

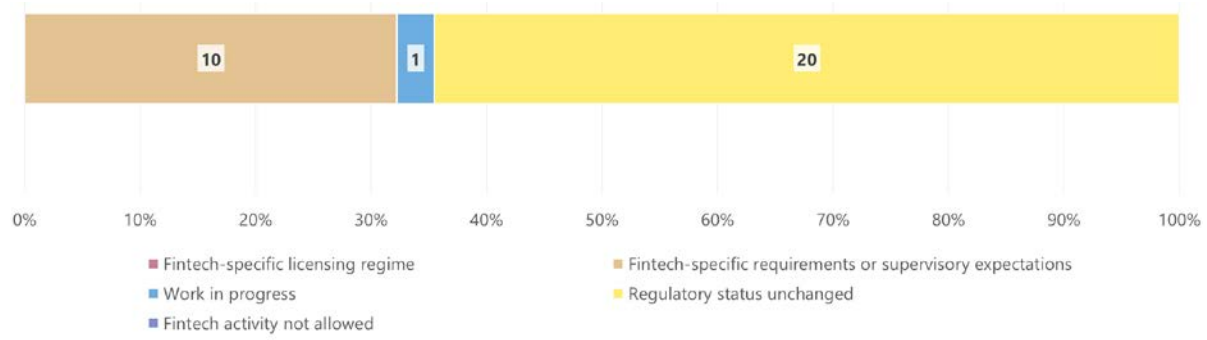
[46] Based on the results of our survey, this section covers the regulatory approach of robo-advice on investment products (as defined in Section 2), ie robo-advice on insurance products is not considered.

[47] For more details, see IOSCO (2017), EBA (2016, 2018), ESA (2018) and OECD (2016, 2017).

stringent requirements typically apply for advice which is limited in scope and does not involve a comprehensive analysis of a client's circumstances (eg simplified or streamlined advice).

- *type of adviser*. Different requirements may apply if the adviser is restricted (eg advice is based on a limited universe of products or providers) and not independent.
- *type of client*. Customer protection afforded to retail clients is typically more stringent than that for other investors.
- *purpose of investment*. Requirements may differ depending on the purpose of the investment. For example, under the conflicts of interest rule in the US, more stringent duty of care standards apply to broker-dealers for advice on retirement plans than for other types of investments.
- *type of product*. The applicability of regulations may depend on the type of product (securities, insurance and banking products) or its complexity. For example, in the European Union, depending on the type of product, relevant regulations include MIFID2, the Mortgage Credit Directive (MCD), the Consumer Credit Directive (CCD) and the Insurance Distribution Directive (IDD).
- *type of activities performed*. Licensing requirements often depend on the extent of the adviser's activities. The robo-adviser may generate advice, it may pass clients' orders on to brokers, it may execute clients' orders on its own platform, it may regularly rebalance clients' portfolios in line with the advice given, or it may even have discretion over managing clients' portfolios beyond rebalancing.

Chart 7: regulatory responses for robo-advice



Sources: National regulations; FSI survey.

39. **Around a third of surveyed jurisdictions have published guidance and set supervisory expectations on issues that are unique to robo-advice as compared to traditional financial advice.** With most guidelines issued between 2016 and 2018, regulators' responses to our survey indicated that they acted mainly because of customer protection and level playing field issues. In the guidance provided, we identified five common elements (Table 3). These are:

- *How to get licensed and what types of licences are available.*[48] For example, in Singapore, providers of financial investment advice need to hold a financial adviser's licence. If the robo-adviser also offers a platform for the execution of capital market products, it needs to hold a Capital Markets Services (CMS) licence for dealing in capital market products. If the robo-adviser has discretion over the management of clients' investment portfolios beyond portfolio rebalancing, it needs to hold a CMS licence in fund management.
- *How to meet the obligation to act in the best interest of clients and provide only suitable investment advice in the face of limited, if any, human interaction*. Robo-advisers are expected to collect

[48] While not strictly fintech-specific, regulatory guidance documents for providers of robo-advice often elaborate on the licensing requirements.

sufficient and reliable information before recommending any investment product. Information will only be reliable if the tool used to collect client information (eg an online questionnaire) is clear and self-explanatory, has a mechanism to resolve inconsistent client responses and incorporates a mechanism to identify clients for whom robo-advice is not appropriate. Given the challenges for fully automated models, some regulators are of the view that suitability of advice is very hard to achieve without human advisers involved.[49]

- *How to ensure that the algorithm used to generate advice is doing what it is supposed to do.* At the core of a robo-adviser's business model is an algorithm that translates a client's information into actionable advice. A coding error or bias in the algorithm may harm many clients as it could result in systematic mis-selling of financial products and unexpected losses. To mitigate this risk, some regulators require robo-advisers to put in place governance and oversight arrangements for algorithms (with the ultimate responsibility assigned eg to the board or senior management). Aspects considered in these arrangements are the availability of sufficiently qualified staff involved in developing and running the algorithm, regular review of the algorithm's methodology against best market practice, monitoring of the quality of advice generated, and internal processes and procedures, eg for approving changes in methodology or suspending the algorithm if errors are detected.
- *What to consider when providing streamlined/scaled advice.*[50] Advice provided by robo-advisers is often limited in scope and does not consider all aspects of a client's financial situation. In this case, robo-advisers may be expected to communicate the limited nature of the advice and the potential consequences of the scope of the advice. This could be by issuing a risk disclosure statement. Because robo-advisers that provide streamlined advice do not collect full information on a client's financial circumstances, some regulators provide guidance on what sort of information is needed to establish suitability in different scenarios.
- *What information needs to be disclosed and how it should be presented.* Robo-advisers are expected to provide sufficient information to their clients to allow them to make informed decisions. Information should be simple, easily understandable, clear and not misleading. Disclosure of information may also be required on the business model, scope of advisory services and potential conflicts of interest.

[49] For example, securities regulators in Canada expect clients to be contacted by advisers in the onboarding process and to always have the option to initiate contact with an adviser. In Massachusetts (US), "fully automated robo-advisers, as currently structured, may be inherently unable to carry out the fiduciary obligations of a state-registered investment adviser" (Massachusetts Securities Division (2016)).

[50] The UK FCA defines streamlined advice as: "A term used to collectively describe advisory services (such as focused and simplified advice) that provide a personal recommendation that is limited to one or more of a client's specific needs. The service does not involve analysis of the client's circumstances that are not directly relevant to those needs."

Robo-advice: elements of regulatory guidance Table 3

	Licensing/authorisation requirements (types of licences, licensing process)	Best interests duty/provision of suitable advice/ collection of customer information	Use of algorithms	Provision of scaled/streamlined advice vs comprehensive advice	Required or expected disclosures to clients
AU	✓	✓	✓	✓	✓
CA	✓	✓			
CN	✓	✓	✓		✓
CO*	✓	✓			✓
GB	✓	✓	✓	✓	✓
HK	✓	✓	✓		✓
NL	✓	✓	✓		✓
SE	✓	✓	✓		✓
SG	✓	✓	✓	✓	✓
US		✓			✓
ZA		✓			
Total	9	11	7	3	9

* Introduced under the Decree 661 of 2018, secondary regulation is under consideration.

Sources: National regulations; FSI survey.

40. **In the absence of robo-specific regulations, several authorities provide somewhat more general information on existing regulatory requirements.** In particular, guidance focuses on what financial advisers need to do to be compliant and meet their obligations under applicable securities laws (eg Markets in Financial Instruments Directive (MIFID2) in the European Union). In doing so, they factually explain how the existing regulatory framework applies to financial advisers, without setting any specific supervisory expectations or adding any new requirements that are specific to robo-advice (eg Austria, Germany, Luxembourg, Poland and Spain).

Digital payment services and e-money

41. **Digital payment services are provided by banks and non-banks on the basis of different transaction accounts.** While banks have historically dominated the payments market, non-bank fintech companies have become increasingly involved. This means that users now have various options to make payments digitally. To transfer money, they may use payment services that operate on the basis of a traditional bank account, or they may use a prefunded e-money account or a payment account operated by a non-bank payment service provider (PSP).[51] As Table 4 shows, these accounts are different in nature. Whereas e-money accounts are similar to bank accounts and permit the indefinite storage of money, payment accounts are closer to flow-through accounts for future payment transactions.

[51] See CPMI (2014, 2018) for a categorisation of different types of non-bank PSPs.

Differences in transaction accounts Table 4

	Bank account	E-money account	Non-bank PSP payment account
Restrictions on holding of funds in account	No	No	Yes, only funds in relation to payment transactions
Time limit on storage of funds in account	No	No	Yes, no longer than is necessary for executing payment*
Regulatory classification	Bank deposit	E-money	Neither bank deposit nor e-money
Deposit insurance	Covered	Not covered	Not covered

* The features of payment accounts vary across jurisdictions and there may not be a specified time limit on the storage of funds.

Source: FSI staff.

42. **Non-bank providers of digital payment services are in the business of enabling the flow of money in an economy.** More specifically, they use technology to facilitate payment transactions by transferring money, clearing or settling balances digitally, without the use of physical money. But they are difficult to categorise because they have different business models and offer services at different stages of the payment process.[52] One categorisation distinguishes between those that execute payment transactions by transferring funds from payers to payees, and those that initiate payment transactions from the payer's account to the payee's account without handling any money themselves.[53] Another categorisation distinguishes between those that offer their payment services by placing an overlay on existing payment infrastructures, while others use their own proprietary standalone systems (CPMI and IMF (2019)).[54] Prominent examples include Alipay (standalone), WeChat Pay (standalone), PayPal (overlay) and Calibra[55] (overlay).

43. **E-money is an electronic store of monetary value on a technical device.** Depending on the type of e-money, the purchasing power resides in a personal physical device or specialised software, such as e-wallets.[56] For issuers, e-money represents a "prepaid" debt-like instrument that is issued on receipt of funds for the sole purpose of facilitating payment transactions. More specifically, e-money is a claim against the issuer that is typically denominated in the same currency as central bank or commercial bank

[52] In CPMI (2014), non-banks are classified into four categories: front-end providers, back-end providers, operators of retail payment infrastructure and end-to-end providers. See Annex A in CPMI (2014) for a description of the five stages involved in a retail payment process.

[53] Examples for providers executing transactions through payment accounts are GoCardless and WePay; and for those initiating payment transactions Apple Pay and Google Pay (digital wallets that tokenise credit/debit cards), Facebook messenger (IT solution for making payments on the basis of credit/debit cards), and iDEAL and Sofort (service connecting transaction accounts through overlay IT solutions that act like a "software bridge" between accounts).

[54] In CPMI and IMF (2019), overlay and standalone systems are defined as follows. Overlay systems build an innovative customer interface that improves the ease with which customers can instruct and receive payments. These systems then use existing payment infrastructure, such as correspondent banking, credit card or retail payment systems, to process and settle payments. Standalone systems are "closed-loop" payment systems and do not interact with or depend on existing payment infrastructure. In these systems, payments are processed, cleared and settled by the platform provider independently of any other system.

[55] Calibra is the mobile wallet that Facebook intends to run on top of the Libra network (CPMI and IMF (2019)).

[56] See www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html.

money[57] and is usually redeemable in fiat currency[58] at face value upon demand.[59] For users, e-money is an alternative means of payment that makes it convenient to pay for goods or services, or to settle a debt. For them, it is as a form of purchasing power bought for future transactions.

44. **Because of the risks involved, e-money is typically regulated separately from other payment services.**[60] For example, in the European Union payment service providers are regulated as payment institutions under the Payment Services Directive 2 (PSD2) and e-money providers are regulated as e-money institutions under the Electronic Money Directive 2 (EMD2).[61] While the latter can also provide payment services, they are the only non-banks allowed to issue e-money. E-money institutions are subject to more stringent and additional requirements than institutions providing only payment services (Table 5).

Overview of the regulatory regime for payments in the EU — Table 5

		Allowed activities			Regulatory requirements	
		Deposits and lending	Issuance of e-money	Provision of payment services	Initial minimum capital (EUR)	Applicable regulation
Banks	Credit institution	✓	✓	✓	5,000,000	CRR/CRD4*
Non-banks	E-money institution		✓	✓	350,000	EMD2
	Payment institution			✓	Up to 125,000 (depending on service)	PSD2

CRR=Capital Requirements Regulation; CRD4=Capital Requirements Directive; PSD2 = Payment Services Directive; EMD2=Electronic Money Directive.

* CRR and CRD4 are being revised with a view to continuing implementation of Basel III in the EU and will be replaced by CRR2 and CRD5.

Digital payment services

45. **Most surveyed jurisdictions have fintech-specific regulations for digital payment services.** However, the regulatory frameworks vary depending on the objective and according to the role and type of service provided by non-banks. In general, institutions with activities that involve customers' funds are regulated differently than those that do not.

[57] See www.bis.org/cpmi/publ/d137.pdf.

[58] An exception is Singapore, where the Payment Services Act explicitly prohibits that users withdraw e-money from a payment account and exchange the e-money withdrawn for Singapore currency. This is only allowed upon termination of the payment account.

[59] As pointed out in IMF (2019), the redemption guarantees for e-money are not backstopped by governments (unlike other claim-based money such as commercial bank deposits) but rely on private safeguarding measures such as prudent management and legal protection of assets available for redemption.

[60] For a detailed description of the risks involved in e-money, see IMF (2019).

[61] Many big techs now have companies in their group that are authorised as payment or e-money institutions in the EU. Examples for e-money institutions are: Airbnb (licence granted by UK FCA), Alipay (CSSF), Amazon (CSSF), Facebook (Central Bank of Ireland), Google (UK FCA, Bank of Lithuania) and Uber (Dutch National Bank).

46. **Some jurisdictions aim at facilitating the access of non-banks to the payments market.** For example:

- In the EU, PSD2 introduced two new categories of regulated payment service providers, referred to collectively as third-party payment services providers (TPPs): payment initiation service providers (PISPs) and account information service providers (AISPs). TPPs do not operate payment accounts themselves but, once authorised by their clients, have access to their clients' payment accounts held by other financial institutions. Specifically, PISPs enable consumers to make online payments while informing merchants that the payment has been made. As such, they represent an alternative to online credit card payments. AISPs provide users with aggregate information on their accounts, irrespective of where they are being held.
- In South Africa, non-banks are currently required to partner with a bank to offer payment services. In order to relax this constraint and open the market to broader competition, giving non-banks the power to clear and settle certain transactions is currently under consideration.
- In Japan, the Payment Services Act of 2009 allowed non-bank firms to perform fund transfers, which previously were the exclusive domain of banks. However, unlike bank transfers, these non-bank transfers are subject to a cap of JPY 1 million.[62]
- In Chile, in 2017 non-banks were allowed to issue prepaid cards, subject to certain conditions. Nevertheless, there always needs to be a bank in the background that operates these cards.

47. **Some jurisdictions have put in place regulatory initiatives to strengthen requirements for non-banks.** For example:

- In Canada, the Department of Finance is working on extending the regulatory perimeter to include the retail payment system by appointing the Bank of Canada as oversight authority (it already oversees systemically important payment systems), ensuring that non-banks put in place sound risk management policies. These include operational risk mitigation frameworks and safeguarding requirements for money held by payment service providers. In Turkey, a new framework was implemented in 2013 that introduced licensing requirements for non-bank payments.
- In Singapore, the pre-2019 framework was fragmented in two pieces of legislation that regulated payment systems, stored value facilities, money-changing and remittance businesses separately. The Payment Services Bill was passed in Parliament in January 2019 and became an Act in February 2019. The Act is modular and encompasses seven types of services[63] within the same framework, offering different types of licences depending on the regulated activities performed and related business volumes.

E-money services

48. **Most surveyed jurisdictions have a dedicated regulatory framework for e-money services.** This is in the form of either a specific licensing regime or other requirements, or supervisory expectations that are specific to e-money. In South Africa, work on an e-money regime is in progress. In Canada, work is under way on a retail payments oversight structure that includes e-money services. At present, it appears that only one jurisdiction, Argentina, does not have specific requirements for e-money, though e-money services are permitted under its payments framework.

[62] Japanese authorities have publicly stated their intention to adopt a more risk-based licensing approach by softening the cliff effect related to the cap on non-bank permitted transfers, so as to facilitate competition from non-bank operators.

[63] Those seven types of services are: account issuance, domestic and cross-border money transfer, merchant acquisition, e-money issuance, digital payment token dealing and exchanges and money-changing services.

49. **There are two broad types of e-money licensing regime**. Under the first, e-money services are considered a banking business and subject to bank-like prudential regulation. While in some jurisdictions a bank licence is required (eg South Africa[64]), in others e-money providers form a special class of bank that is licensed to provide a limited range of banking activities (eg Colombia). In all these jurisdictions, customer balances ("float") are covered by the deposit insurance scheme. Under the second type, non-bank e-money service providers are required to obtain a dedicated licence from the authority, subject to specific regulatory requirements.

50. **Non-bank e-money providers are typically restricted from engaging in financial intermediation or other banking activities.** E-money service providers are often not allowed to use the funds received in exchange for e-money to make loans.[65] Also, e-money is often prohibited from earning interest, or this is allowed only in narrowly defined circumstances.

51. **Requirements for the amount and type of assets in which the float can be held are common.** Most jurisdictions require that clients' funds held at least match the outstanding e-money.[66] This 100% reserve requirement is meant to ensure that all redemption requests can be met at all times and that there are sufficient assets available to satisfy e-money holders' claims in case of insolvency of the e-money provider. Also, all jurisdictions require in some form that clients' funds be held in safe and liquid assets, such as bank deposits[67] or short-term government paper.

52. **Requirements on how customers' funds need to be protected are commonplace.** Customers may lose their funds in the case of bankruptcy of the e-money provider or some other party involved in the safekeeping of the float. To protect against this risk, regulatory frameworks often require that customers' funds be insulated and ring-fenced from the issuer's assets as to ensure that e-money funds cannot be seized by creditors other than e-money holders. There are various means to achieve this, and the approach chosen often depends on the legal tradition. E-money service providers may be required to hold clients' funds in a separate account at a licensed bank[68] (eg Turkey) or the central bank (eg China), in a trust[69] (eg Hong Kong SAR, Peru), or to take out an insurance policy (eg EU[70]).

Insurtech business models

53. **There are no licensing regimes or other requirements that are specific to insurtech business models in surveyed jurisdictions.** Existing licensing regimes and regulatory requirements are considered

64 As stated above, non-banks are currently required to partner with a bank to offer payment services.

65 Nevertheless, several jurisdictions allow e-money providers to give credit under restricted conditions. For example, under EMD2 in the EU, e-money institutions may grant credit only if it is ancillary and directly related to payment services and granted exclusively in connection with the execution of a payment transaction (eg negative balances). Such credit cannot be granted from the funds received or held for the purpose of executing a payment transaction and needs to be repaid within a short period of time (maximum 12 months).

66 For example, China and Brazil recently raised their reserve requirement for outstanding client balances to 100%.

67 The coverage by deposit insurance schemes of a bank account that holds e-money funds varies across jurisdictions. For example, in some, the funds are guaranteed up to the respective limit (eg EUR 100,000) like any other bank account. In others, this limit does not apply at the account level but at the level of individual e-money holders (BBVA Research (2016)).

68 The bank would be bound by a fiduciary contract, or other legally effective arrangements, that protects e-money funds from the claims of other creditors of the bank or the e-money provider in the case of bankruptcy of either party.

69 In the case of bankruptcy of the e-money provider, funds placed in a trust cannot be used to meet obligations of the provider that are not related to the e-money issued (BBVA Research (2016)).

70 Safeguarding measures under EMD2 include private insurance.

sufficient to address the features and risks of innovative business models that are emerging in the provision of insurance.

54. **Entities offering mobile, on-demand, usage-based or technology-enabled peer-to-peer and parametric insurance are licensed under the existing regimes.** Authorities consider that existing regulations cover adequately the underlying risks of these innovative products. Technology-enabled peer-to-peer insurance is the only business model for which some authorities are currently assessing whether to issue new requirements in order to address the potential risks when it is scaled up to a certain number of customers and policy premium size.

55. **The absence of insurtech-specific requirements does not mean that authorities are not responding to the increasing digitalisation of the insurance business.** All areas of the insurance value chain are being transformed by emerging technologies, presenting potential benefits and risks to consumers and markets.[71] Many authorities are responding by issuing new, or modifying existing, requirements concerning the use of digital technologies by market participants (ie modifying outsourcing regulations to include specific requirements for the use of cloud computing) or by conducting exploratory analysis and formulating general principles related to the use of such technologies (ie principles for the use of AI in financial services).[72] Based on the conceptual framework of this paper, such regulatory responses are analysed under the fintech tree category of enabling technologies.

Financial services related to cryptoassets

56. **The lack of a common categorisation of cryptoassets is one of the most important challenges when considering a regulatory approach.** Terms and classifications used by regulators have evolved over time as rapidly changing technologies and new business models emerge and transform in an ongoing basis. Since Bitcoin's creation, some of the terms that have been used are virtual/crypto-/digital currency and virtual/crypto-/digital asset. As analysed by Blandin et al (2019), regulators' definitions of these terms usually share a common set of distinctive elements. There are the: (i) form of the asset – it is a digital or electronic representation of value; (ii) properties of the asset – it may be transferred, stored and traded electronically; and (iii) function of the asset – it may be used as a means of payment or exchange, store value or unit of account. Only a few of the definitions offered by regulators explicitly mention the underlying technology that enables the creation of this new type of asset.

57. **There are a number of different criteria for classifying cryptoassets.** From survey responses, jurisdictions currently classify cryptoassets according to:

- Nature of the issuer: cryptoassets may be issued by non-regulated entities (eg Tether), regulated financial entities (eg JPM Coin) or the public sector (eg central bank digital currency).
- Underlying economic function: cryptoassets may be used as means of payment or exchange ("payment tokens"); be used as a source of investment, giving holders rights and obligations ("security tokens"); and can also grant holders access to a current or future service ("utility tokens").
- Underlying assets: cryptoassets may be backed by assets such as currencies (fiat or crypto), commodities (eg precious metal), real estate or securities.

58. **In general, the underlying economic function is the criterion regulators use to classify cryptoassets and determine whether they fall within the regulatory perimeter and, if so, which regulation applies.** This approach follows the basic principle of "same risks, same rules". If the economic

[71] See IAIS (2017).

[72] For a more detailed analysis of supervisory considerations over the impact of digital technologies in the insurance industry, see IAIS (2018a, 2018b).

function and purpose of a cryptoasset are the same as a regulated asset class, then they are, in general, subject to the same financial rules on anti-money laundering, securities trading, banking, fund management or financial infrastructure regulation. Similarly, if an entity or intermediary is engaging in activities with cryptoassets that are by nature similar to those performed by regulated financial entities or intermediaries, then such activities fall into the perimeter and should be subject to financial regulation.

59. **With the emergence of stablecoins, the underlying assets criterion is also being considered to determine regulatory requirements.** Such is the case of Switzerland, which has published an indicative classification of stablecoins in eight categories according to the underlying asset to which they are linked.[73] FINMA uses this classification to assess stablecoin projects and determine on an individual basis the regulatory requirements applying under the Swiss financial market regulation. For example, in applying this classification, FINMA indicated that the planned Libra project would initially fall under the financial market infrastructure regulation and would require a payment system licence and, due to the issuance of Libra payment tokens, the services planned by the Libra project would be subject to additional requirements.[74]

60. **Regulatory attention has mostly focused on cryptoassets issued by non-regulated entities.** Cryptoassets present a number of risks for investors including liquidity risk, credit risk, market risk, operational risk (including fraud and cyber risks), money laundering and terrorist financing risk, and legal and reputational risks.[75] Given that these risks may increase when the issuer is not subject to prudential regulatory requirements, it is no surprise that most of regulators' attention is targeted on cryptoassets issued by non-regulated entities.

61. **Regulatory and policy responses to cryptoassets vary widely among surveyed jurisdictions.** These may vary depending on the level of development of the market, nature of the legislative process, number of authorities involved in the legal and regulatory framework, and financial authorities' mandates and architecture, among other factors. Likewise, responses have varied over time in terms of the type and scope of the approach as regulators are constantly working to address emerging risks from this new asset class.[76]

62. **In the light of the wide diversity of policy responses, the regulatory approaches to cryptoassets and related activities[77] are only classified in this section according to the nature of the policy response.** Regulatory approaches are classified in seven categories, shown in Table 6. These categories are not mutually exclusive since a jurisdiction's approach may cover regulations and other policy instruments from various authorities to different type of cryptoassets and related activities.

[73] See FINMA (2019a, 2019b).

[74] Under the Financial Market Infrastructure Act (FMIA), all additional services that increase the risks of a payment system must be subject to corresponding additional requirements. This means that all the potential risks of a Swiss payment system, including bank-like risks, can be addressed by imposing appropriate requirements in line with "same risks, same rules". Due to the issuance of Libra payment tokens, the services planned by the Libra project would clearly go beyond those of a pure payment system and therefore be subject to such additional requirements. These would relate in particular to capital allocation (for credit, market and operational risks), risk concentration and liquidity as well as the management of the Libra reserve. See FINMA (2019a, 2019b).

[75] See BCBS (2019a).

[76] Some jurisdictions' regulatory responses have been to restrict cryptoassets or specific crypto-related activities in a first stage and then to adopt a more permissive regulatory approach at a later stage. Likewise, the initial scope of a policy initiative may evolve over time as regulators define the regulatory treatment of new business models.

[77] For this paper, these activities may include creating, distributing, storing or exchanging cryptoassets, using them for investment or payment purposes, or as reference in financial products.

Regulatory and policy responses to cryptoassets and related activities

Table 6

	Introduction of crypto-specific licence, authorisation or registry	Clarification on applicable regulation to ICOs	Clarification on applicable regulation to crypto-related activities/ providers	Clarification on tax treatment	Amendment of AML framework	Publication of warnings	Ban on certain crypto-related activities
AE	L						
AR							
AU							
AT							
BE							
BR							
CA							
CH							
CL							
CN							
CO							
DE	L						
ES							
FR	L+R						
GB							
HK							
IT							
JP	L						
LU							
MX	A						
NL	R						
PE							
PH	R						
PL							
RU							
SA							
SE							
SG	L						
TR							
US*	L						
ZA							

Regulatory response has been approved
Regulatory response in progress
Regulatory prohibition

L = licence; A = authorisation; R = registration; * = state level

Sources: National regulations; FSI survey.

63. **In general, publication of warnings is the first and most common response of jurisdictions to cryptoassets.** Since December 2013, 27 surveyed jurisdictions have published warnings alerting consumers and investors to the various risks associated with using cryptoassets as means of payment or exchange (eg cryptocurrencies) or for investment purposes (eg initial coin offerings (ICOs)).

64. **A number of jurisdictions have published statements and issued different policy instruments[78] to clarify the regulatory treatment of cryptoassets and related activities.** These clarifications usually include the criteria to assess whether cryptoassets and related services fall within the regulatory perimeter and the applicability of existing licensing or authorisation regimes as well as other regulatory requirements. From our survey, 16 jurisdictions have clarified the applicability of tax regulations to income generated from transactions with cryptoassets, 15 have clarified the applicability of financial regulations to ICOs and 14 have clarified the applicability of financial regulations to crypto-related activities or providers. The latter include issuing, marketing, trading or providing other intermediary service, or holding, storing, exchanging and advising on cryptoassets. In general, clarifications focus on due diligence, governance, risk management and disclosure applicable requirements.

65. **Given the threat of criminal and terrorist misuse of cryptoassets, jurisdictions are amending their respective frameworks to incorporate international AML/CFT guidance.** From our survey, 11 jurisdictions have already amended, and seven more will amend, their AML framework. In the European Union, national authorities are introducing the requirements established in the Fifth Anti-Money Laundering Directive (AMLD5). Similarly, other jurisdictions are planning to amend their frameworks to incorporate the recommendations issued in this area by the Financial Action Task Force (FATF) in June 2019.[79]

66. **New crypto-specific licensing, authorisation and registration regimes are emerging in a few jurisdictions.** Six jurisdictions have introduced specific licensing regimes related to crypto-assets: Abu Dhabi Global Market contemplates a financial services permission to carry on the regulated activity of operating a cryptoasset business; the Autorité des Marchés Financiers in France introduced a new optional status for digital asset service providers along with mandatory registration for some of the services and optional visa regime for ICOs; the Deutsche Bundesbank requires a specific license for custodian wallet providers; in Japan, a license for exchanging cryptoassets was introduced under the Payment Services Act; in Singapore, digital payment token dealing or exchange is subject to the licensing regime established by the new Payment Services Act 2019; and the US state of New York introduced BitLicense, which is a business licence issued for cryptocurrency operations in that state. Other jurisdictions have implemented authorisation regimes, as in Mexico, where the central bank requires credit institutions and financial technology institutions to hold a virtual asset authorisation to perform internal operations with cryptoassets. Another two jurisdictions reported that they have a registration regime for virtual currency exchanges and/or crypto-wallet providers (ie the Netherlands and the Philippines). See Table 7 for more information on selected crypto-specific licensing regimes.

67. **The type of prohibitions on crypto-related activities varies widely among surveyed jurisdictions.** Partial approaches are implemented in four jurisdictions. Belgium forbids the marketing to retail clients of financial products for which the return depends, directly or indirectly, on virtual currencies. Colombia does not allow financial institutions to invest or offer investment services in cryptoassets. Mexico does not allow financial institutions to use virtual assets in products offered to their clients, and ICOs are prohibited. In Saudi Arabia, trading of cryptocurrencies is not allowed.[80] In the case of China, any crypto-related activity is considered illegal.

[78] These may include laws, secondary regulations, guidance and guidelines.

[79] See FATF (2019a).

[80] Previously, a warning was issued to investors for such investment. However, the regulators will continue to monitor and assess cryptoassets.

Description of selected crypto-specific licensing regimes Table 7

Name	Jurisdiction	Content
Operating a Crypto Asset Business	Abu Dhabi	The Financial Services Regulatory Authority (FSRA) of Abu Dhabi Global Market (ADGM) issued a Spot Crypto Asset Framework composed of guidance that regulates initial coin/token offerings and other cryptoasset activities. The framework contemplates a financial services permission to carry on the regulated activity of operating a cryptoasset business. The framework is designed to address the full range of risks associated with cryptoasset activities, including risks relating to money laundering and financial crime, consumer protection, technology governance, custody and exchange operations. The new ADGM crypto framework instils proper governance, oversight and transparency over cryptoasset activities.
Digital Asset Service Providers and ICO visa approval	France	The Autorité des Marchés Financiers (AMF) regulates digital asset services providers (DASPs) and grants optional approval to ICOs through the Law "Action Plan for Business Growth and Transformation" (PACTE) and Decree No. 2019-1213. The licence for DASPs is a new optional status that covers a wide range of activities: custody of digital assets for third parties; purchase or sale of digital assets against legal tender or other digital assets (broker/dealer); operation of a digital asset trading platform; other digital asset services such as the reception and transmission of third-party orders, third-party portfolio management, advice, underwriting and placing on or without a firm commitment basis. Even though the licensing regime is optional, custody or exchange services are subject to mandatory registration with the AMF upon the assent of the Autorité de Contrôle Prudentiel et de Résolution (ACPR).
BitLicense	New York, US	In June 2015, the New York State Financial Services Department (NYSFSD) published the Virtual Currency Business Activity (BitLicense) rules that apply to a wide range of activities involving virtual currencies such as their transmission, storage, holding, maintaining custody or control, buying, selling, performing exchange services, controlling administering or issuing this type of currencies. These rules include both prudential and market conduct requirements.

Sources: FSI Survey; FSI research.

Section 4 – Policy responses for enabling technologies

68. **While enabling technologies present opportunities, their application in financial services may also pose new risks or increase existing ones.** For financial institutions, these may include data privacy, cyber security, third-party dependency and concentration risks. In addition, there are significant challenges that institutions face regarding the explainability of predictive models used in ML and AI applications related to issues of bias, ethics and fairness.

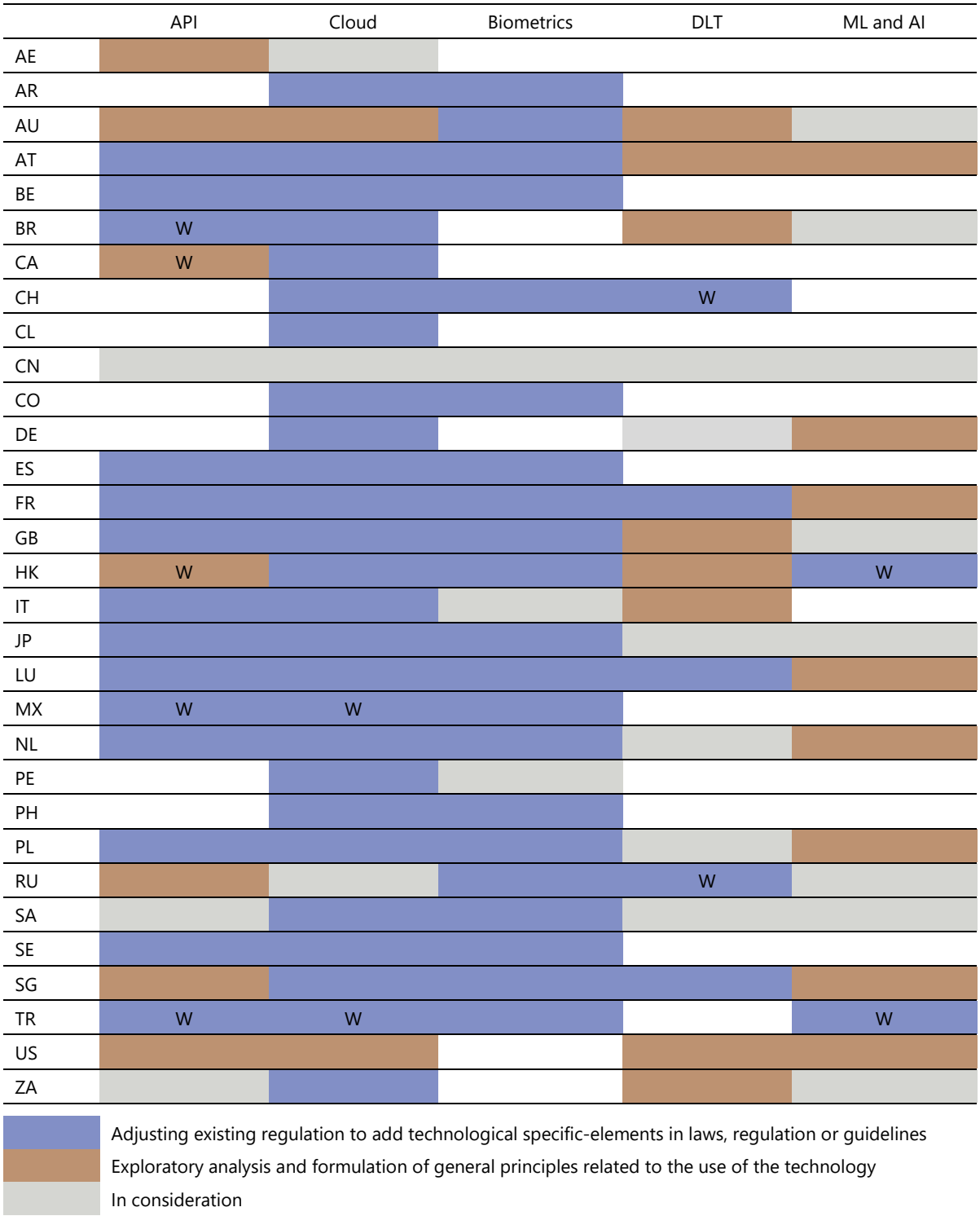
69. **Regulatory and policy responses rely mainly on adjusting existing regulations to add technology-specific elements in existing laws, regulations or guidelines.** Authorities have also been active in conducting exploratory analysis and establishing general principles related to the use of such technologies. These initiatives tend to take the form of research and discussion papers, with the aim of providing a general assessment of the regulatory implications related to the use of a certain technologies in the context of a supervised financial activity.

70. **As a result of the level of market adoption, some technologies have received more attention than others.** Regulators have been particularly active with regard to APIs, cloud computing[81] and biometric-based identification and authentication as a result of a higher level of adoption of these technologies in the provision of financial services. In contrast, AI and ML and, to some extent, DLT have been subject to risk assessments and issuance of general principles by the authorities. Several jurisdictions are still investigating concrete actions to be taken in terms of enabling technologies. In most cases, authorities are applying a technology-neutral approach. See Table 8.

[81] See FSB (2019c) for a discussion on financial stability implications of third-party dependencies in cloud services.

Policy responses to enabling technologies

Table 8



W = Work in progress

As EU directives and/or regulations are counted for each jurisdiction that applies such directive/regulation (either directly or via transposition mechanism) and EU jurisdictions are highly represented in our sample, this might lead to conclusions which are not necessarily representative of world tendencies.

Source: FSI survey.

Application programming interfaces

71. **Current regulatory responses to APIs are usually part of open banking initiatives.** APIs have been used for decades to facilitate data flows between systems. However, in recent years authorities have focused their attention on APIs since they provide a means of interaction between banks and third parties for sharing customer-permissioned bank-held data, which is a key element of open banking frameworks.

72. **A number of jurisdictions have required banks to create mechanisms to give third parties access to their data.** Such is the case of jurisdictions within the EU, where PSD2 and the supplementing Regulatory Technical Standards on strong customer authentication and common and secure communication (RTS SCA and CSC) mandate specific requirements for account information service providers, payment initiation service providers and payment service providers on interfaces (EBA (2019a, b, c)). Likewise, in Mexico the Fintech Law will require in 2020 that fintech institutions, clearing houses, traditional financial institutions and credit bureaus develop APIs that allow connectivity between them.

73. **Other jurisdictions have provided guidance to encourage and facilitate API adoption to enable innovation in financial services.** In Singapore, MAS, together with the Association of Banks in Singapore, published an API Playbook which presents high-level guidelines for API design and usage aimed at stakeholders intending to use the APIs, including providers, consumers, fintechs and the developer community. These guidelines include best practices for the design, implementation and usage of the selected APIs. Likewise, the HKMA is in the process of implementing an open API framework in Hong Kong following a public consultation which aims to facilitate the development and adoption of APIs by the banking sector.

Cloud computing

74. **Almost all surveyed jurisdictions have either modified their existing regulatory frameworks or clarified their regulatory expectations on the use of CC by financial institutions.** Authorities have included specific requirements or published their expectations on outsourcing, governance, risk management and cyber security frameworks concerning arrangements between financial institutions and cloud service providers on the provision of material or critical services.

75. **Requirements and clarifications are intended to ensure adequate management of the risks associated with the use of CC by financial institutions.** Besides the operational risks of any outsourcing activity, CC may pose additional risks to the financial sector, given: (i) shared computing resources in some cloud deployment models; (ii) the type of information that is stored and processed; (iii) the different geographical location of computing resources and providers; and (iv) the small number of global cloud providers, resulting in market concentration that could have systemic implications. The cross-border nature of cloud services complicates the effective oversight of all these risks.[82]

76. **Regulatory frameworks have a number of common requirements and expectations for CC.** Authorities generally focus on: (i) the adequacy of information security, data confidentiality and availability;[83] (ii) the strength of IT and cyber security capabilities at cloud service providers; (iii) the effectiveness of recovery and resumption capabilities; and (iv) the adequacy of audit rights (ie the supervisory authority's access to documentation and information, and ability to conduct on-site inspections at the provider).

[82] See Crisanto et al (2018).

[83] Including for some jurisdictions data residency requirements. See Crisanto et al (2018).

Biometrics

77. **Regulatory responses to the use of biometric data usually aim to facilitate non-face to face customer identification and remote authentication by financial institutions.** In jurisdictions where remote authentication is allowed, financial authorities have issued or modified their existing regulatory frameworks to allow the use of biometric data for onboarding and account opening processes.

78. **In jurisdictions where requirements related to the collection, use and storage of biometric data have been set, these are mostly focused on addressing data privacy, cyber security and money laundering risks.** Such is the case of EU member jurisdictions, where PSD2, GDPR and AML5 require payment service providers to have strong security requirements regarding consumers' biometric authentication.

Distributed ledger technology

79. **Currently, only a few jurisdictions have issued specific DLT regulations.** Application of this technology is mostly related to the creation of cryptoassets. However, DLT may also be used in foreign exchange remittance payments, securities settlement systems, debt issuance programmes, parametric insurance and digital identity initiatives. On a global scale, DLT is also being applied to support private securities transactions, interbank payments and netting services for repo and foreign currency markets. Given its wide range of applications and the early adoption in the financial industry, most jurisdictions are still exploring potential policy responses through exploratory analysis and discussion papers that analyse its unique features, opportunities and risks, different use cases, potential implications for financial markets and regulatory considerations.

80. **Depending on its application, the use of DLT by financial institutions or intermediaries may be subject to various regulations.** For example, civil law governs basic ownership and intellectual property rights as well as the validity of smart contracts, whereas financial laws dictate how the industry processes securities transactions, payments, client data transmitted through this technology, and how it ensures cyber resilience, data privacy and security.

81. **Even though DLT is in an early stage of adoption, a number of jurisdictions have included specific DLT provisions in their legal frameworks.** Such is the case of France, where the notion of a distributed ledger was first introduced in French law allowing the use of DLT for the purpose of recording the issuance and sale of minibons,[84] afterwards extended to recording issuance and sale of unlisted financial securities. Likewise, the Luxembourg parliament approved a bill of law inserting a new article regarding the circulation of securities. The purpose of this amendment was to provide additional legal certainty by expressly allowing securities to be registered and held via secure electronic registration devices, including distributed electronic registers or databases.

82. **Issuing a specific DLT legal framework is not common.** Switzerland is the only jurisdiction from our survey that is working on a specific framework for DLT and blockchain applications in the financial sector. On March 2019, the Swiss Federal Council presented a preliminary draft of a new Federal Act on the amendment of Federal Laws in the light of the developments regarding DLT. The proposal is expected to be examined in Parliament in early 2020. The draft aims to further improve the regulatory framework for DLT in Switzerland by increasing legal certainty, removing hurdles for DLT-based applications and limiting risks of misuse. In Russia, a DLT regulatory framework applicable to all economic sectors is currently under discussion.

[84] A class of short-term debt instrument dedicated to the financing of SMEs.

Machine learning and artificial intelligence

83. **In the surveyed jurisdictions, to date there are no specific regulatory requirements for financial institutions' use of ML and AI.** Given that ML and AI applications in the financial sector are in a nascent phase, authorities' responses focused on analysing their implications for consumers and financial markets. Some authorities have published exploratory reports, while others are in the process of drafting consultation papers that serve as a basis to discuss potential regulation with the industry.

84. **A few jurisdictions have issued non-binding principles to encourage ethical and responsible use of AI by financial institutions.** Such is the case of Singapore, which issued principles to promote fairness, ethics, accountability and transparency (FEAT) in the use of AI;[85] the Netherlands, which issued general principles on soundness, accountability, fairness, ethics, skills and transparency (SAFEST) for the use of AI in the financial sector;[86] and Hong Kong, which issued high-level principles on the use of AI by banks.[87] Table 9 gives examples.

Examples of principles for the use of AI — Table 9

Singapore (2018)	Netherlands (2019)	Hong Kong SAR (2019)
Fairness: • justifiability • accuracy • bias	Fairness	Governance: • board and senior management accountable for the outcome of AI application
Ethics	Ethics	Application design and development: • possessing sufficient expertise • ensuring an appropriate level of explainability of AI applications • using good-quality data • conducting rigorous model validation • ensuring auditability of AI applications • implementing effective management oversight of third-party vendors • being ethical, fair, transparent
Accountability • internal • external	Accountability	Ongoing monitoring and maintenance: • conducting periodic reviews and ongoing monitoring • complying with data protection requirements • implementing effective cyber security measures • risk mitigation and contingency plan
Transparency	Transparency Soundness Skills	Consumer protection: • governance and accountability • fairness, transparency and disclosure • data privacy and protection

Sources: Jurisdictions' public information; FSI research.

[85] See MAS (2018).

[86] See Netherlands Bank (2019).

[87] See HKMA (2019).

Section 5 – Policy enablers

85. **To take advantage of the economic and social opportunities that a digital economy might bring, public authorities are seeking ways to increase or improve the provision of public and private digital services in their jurisdictions.** Besides building a digital infrasctructure that allows greater connectivity between people and businesses, multiple authorities (eg financial supervisors and competition, consumer protection and data privacy authorities) are implementing public policies to enable the provision of digital services, such as:

- digital identity systems that enable citizens to have access to public, commercial and financial digital services;
- data protection regimes that allocate rights and responsabilities for accessing and sharing consumer data;
- cyber security strategies that facilitate both public and private institutions' mitigation of cyber risk and their effective response to, and recovery from, cyber attacks;
- open banking initiatives that allow banks to share consumer data, provided consent, with third parties; and
- innovation facilitator initiatives that enable innovations in digital financial services that provide benefits to the market.

See Table 10 for a comprehensive comparison across jurisdictions.

Public policies that enable the provision of digital services

Table 10

	Digital ID (eID)		Data protection	Cyber security		Open banking	Innovation facilitator
	Framework for eID systems' use in financial services	National eID system	National framework	Financial sector framework	National strategy	Type of approach	Type of facilitator
AE	✓		✓	✓	✓		
AR	✓	✓	✓	✓			IH
AU	✓	✓	✓	✓	✓	P	IH, RS
AT	✓	✓	✓	✓	✓	P	IH
BE	✓	✓	✓	✓	✓	P	IH
BR	✓		✓	✓	✓	P*	IH, RS*, A
CA	✓		✓	✓	✓		IH, RS, A
CH	✓		✓	✓	✓	P	RS
CL			✓	*	*		
CN	✓	✓	✓	✓	✓		RS
CO			✓	✓			IH, RS
DE			✓	✓	✓	P	IH
ES	✓		✓	✓	✓	P	IH
FR	✓	✓*	✓	✓	✓	P	IH, A
GB	✓		✓	✓	✓	P	IH, RS
HK	✓	✓	✓	✓	✓	F	IH, RS, A
IT		✓	✓	✓	✓	P	IH
JP	✓		✓	✓	✓	P, F	IH, RS
LU	✓	✓	✓	✓	✓	P	IH
MX	✓		✓	✓	✓	P	RS
NL	✓	✓	✓	✓	✓	P	IH, RS
PE	✓		✓	*	*		
PH			✓	✓	✓		RS
PL	✓		✓	✓	✓	P	IH
RU	✓		✓	✓	✓		RS
SA	✓			✓	✓		IH*, RS, A*
SE	✓	✓	✓	✓	✓	P	IH
SG	✓	✓	✓	✓	✓	F	IH, RS, A
TR	✓		✓	✓	✓	P	
US	✓s			✓s	✓		IHs, RSs
ZA	✓		✓	✓	✓		

P = prescriptive; F = facilitative; IH = innovation hub; RS = regulatory sandbox; A = accelerator; * = in progress; s = state level.

Sources: BCBS (2019d); FAFT (2019b); FSB (2017b); WB-GPFI (2018); FSI survey.

Digital ID systems

86. **Digital IDs enable governments and businesses to deliver digital services which may increase financial inclusion and allow efficiency gains and improvements in service provision.** By secure remote identification and authentication of a person's identity via a digital channel, digital ID gives people access to online and mobile digital services, including bank accounts, digital payments, insurance and credit. For governments and businesses, digital ID may offer economic and non-economic benefits, such as increasing efficiencies in registration processes, reducing onboarding costs and strengthening mechanisms against fraud.

87. **Digital ID systems vary widely among jurisdictions.** They may be implemented by different entities (eg national government, consortium of private or nonprofit organisations or individual entities) and may be develped using different technologies to perform digital authentication (eg biometric data, passwords, smart devices or security tokens). For example, digital IDs may rely on a permissioned DLT shared by institutions or on a centralised data platform held by authorities.

88. **Most jurisdictions allow institutions to use digital ID systems for customers verification and authentication for certain government, commercial and/or financial digital services.** In these jurisdictions, financial authorities have included regulatory provisions in their frameworks that clarify how these systems can be used. These may include requirements on assurance levels and technical standards that must be met for identification/verification at onboarding (account opening) and for ongoing support for customers' due diligence (including transaction monitoring).

89. **Some jurisdictions are also implementing national digital identity systems which are part of a broader innovation and digital strategy in their jurisdictions.** For example, in Sweden citizens can use their BankID, which was developed by a number of large banks, for identification purposes concerning online transactions with banks, organisations and government agencies (eg it works as an identity document like passports, driver's licences and other physical identity documents).

90. **Some jurisdictions are enhancing their frameworks to facilitate consent management and control of citizen's data when accessing digital services.** These frameworks allow digital ID systems that allow citizens to store personal data in a secure database or platform which enables sharing of such data, for multiple purposes, only with their consent.[88] In Australia, for example, the government is implementing a digital ID ecosystem made up of agencies, private sector businesses and systems working together to deliver a secure way to prove a person's identity online to access services. Likewise, Singapore is implementing a National Digital Identity as a key element of the Smart Nation strategy, with the aim to allow residents and businesses to securely and conveniently transact digitally with the government and private sector.

Data protection frameworks

91. **Given the increasing value that data bring to the digital economy in terms of obtaining detailed insights into people's economic, social and political profile, the right to privacy of personal data has gained more attention in recent years.** Data protection regimes have been in place for many years. However, given the increasing digitalisation transforming economies worldwide, public authorities in most jurisdictions have issued new or enhanced existing regulations concerning the collection, use and protection of customer information.

92. **Almost all surveyed jurisdictions have issued data protection laws where the most common requirement is to ask citizens for consent before data about them may be collected, used or shared.**

[88] For an example of how other jurisdictions not covered in the survey are enhancing their frameworks to facilitate consent management and control of citizen's data when accessing digital services, review the case of India. See D' Silva et al (2019).

The definition of what constitutes a customer's personal or sensitive data varies among jurisdictions, where some include in this definition elements such as location, financial or health information (eg Mexico). In all jurisdictions with a data protection regime, the purpose of data collection and use should be explicitly specified.

93. **More comprehensive frameworks also establish new rights for individuals, like data portability, the right not to be profiled or the right to be forgotten.** Such is the case of the GDPR in the EU, where citizens have the right to receive their personal data from an organisation in a commonly used form so that they can easily share it with another (portability), have the right for decisions affecting not to be made on the sole basis of automated processing unless it is necessary by law or a contract, and have the power to have their personal data erased when they are no longer necessary for the purpose they were collected.

94. **Appointment of a Data Protection Officer (DPO) is not a common requirement.** Only two surveyed jurisdictions required the designation of individual(s) responsible for the institution's compliance with data protection regulation. EU law requires companies over a certain size which regularly and systematically monitor or process data on a large scale to employ a DPO. The purpose of this position is to ensure, in an independent manner, that the company is compliant with the applicable data protection rules and to act as point of contact for employees and customers for data protection issues. Singapore's Personal Data Protection Act (PDPA) requires all organisations to designate one or more individuals to be responsible for the organisation's compliance with the PDPA. Business contact information of one of these individuals should be provided for the purpose of responding to access and correction requests.

Cyber security frameworks

95. **Cyber risk is a growing global challenge, and one that governments are addressing with a number of regulatory initiatives.** These include issuing national and/or sectoral regulations, guidance and supervisory practices, where the common objective is to set up a cyber security framework that facilitates entities' mitigation of cyber risk and effective response to and recovery from cyber attacks. Other initiatives include setting up a national cyber security centre (eg France, the UK, the US and Singapore), conducting sector simulation cyber resilience exercises (eg UK) or simulating a cross-border attack on the financial sector (eg G7 cyber attack simulation exercise coordinated by the Bank of France).

96. **In many surveyed jurisdictions, a national cyber security framework is already in place.** Governments are aiming to strengthen the cyber security of critical sectors and infrastructure. These frameworks apply to financial firms, as they are not only part of a critical sector but also are more exposed to cyber risk than other sectors given that they are IT-intensive and highly dependent on information as a key input.

97. **Given its critical role in the economy, almost all jurisdictions have put in place cyber security regulations and guidance specific for the financial sector.** Most of these have been drawn from different cyber security frameworks and guidance developed by international, national and industry organisations, both public and private sector.[89] In particular, they build on the G7 Fundamental Elements of Cybersecurity for the Financial Sector (G7FE), the Committee on Payments and Market Infrastructures-Technical Committee of the International Organization of Securities Commissions (CPMI-IOSCO) *Guidance on cyber resilience for financial market infrastructures* and the G7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector (G7FEA).

[89] See FSB (2017b).

98. **Even though cyber security frameworks for financial institutions vary among jurisdictions, there are some common elements.**[90] The usual starting point for a cyber security regulatory setup is to require financial institutions to have a documented cyber security programme or policy. Institutions are expected to identify critical information assets that need to be protected. Testing institutions' vulnerability and resilience to cyber risk (such as through penetration testing)[91] is a common requirement, as well as the reporting of cyber events. Other common requirements relate to having clear responsibilities and accountabilities at financial institutions and ensuring the capabilities of third-party providers as key components of their cyber security framework. Less common regulatory requirements include cyber threat intelligence-sharing (although it is generally encouraged).

Open banking initiatives

99. **A number of jurisdictions have adopted, or are in the process of adopting, open banking initiatives.** These cover the requirements that apply for accessing and sharing customer information from banks with third-party firms to build innovative applications and services for customers. Most initiatives seek to increase competition in the banking sector and to foster innovation in the provision of digital financial services. Thus, these initiatives may be promoted by competition or financial authorities depending on the ultimate policy objective.

100. **Open banking initiatives vary among surveyed jurisdictions.** According to the classification introduced by the BCBS on regulatory approaches to open banking,[92] Table 10 shows the jurisdictions that follow a prescriptive approach by mandating banks to share customer-permissioned data with registered third parties, and those that follow a facilitative approach by issuing guidance that includes recommended designs and technical specifications to encourage API adoption as an innovation enabler in financial services.

101. **For prescriptive frameworks, there is a wide range of requirements focused mostly on data privacy and security as well as on third-party risk management.** For example, the BCBS identified that regulatory frameworks in its member jurisdictions cover requirements on: licensing of third parties; restrictions around screen scraping practices; data privacy and disclosure/consent requirements; conditions with which third parties should comply for sharing and/or reselling data onward to "fourth parties" or using the data for purposes beyond the customer's original consent; and expectations or requirements for data storage and security.[93]

Innovation facilitators

102. **The three main types of facilitators are innovation hubs, regulatory sandboxes and accelerators.** Hubs are set up by supervisory agencies and provide support, advice or guidance to regulated or unregulated firms in navigating the regulatory framework or identifying supervisory policy or legal issues and concerns. A regulatory sandbox is a controlled testing environment, sometimes featuring regulatory forbearance and alleviation through the use of legally provided discretions by the supervisory agency. Accelerators refer to a partnership arrangement between fintech providers and central banks/supervisory agencies to develop use cases that may involve funding support and/or authorities'

90 See Crisanto and Prenio (2017).

91 See Kleijmeer et al (2019).

92 See BCBS (2019d).

93 See BCBS (2019d).

endorsement/approval for future use in central banking operations or in the conduct of supervisory tasks.[94] These initiatives are not mutually exclusive, as seven jurisdictions responded that they currently have in place both an innovation hub and a regulatory sandbox, while only three have three initiatives in operation (Canada, Hong Kong and Singapore).

103. **Among jurisdictions that have innovation facilitators in operation, innovation hubs are the most common.** Even though the name may vary among the 21 jurisdictions that responded that they have implemented an innovation hub, they have similar objectives: (i) to provide support and guidance on regulatory requirements applying to innovations to be developed; and (ii) to serve as a communication channel with the fintech sector. In some jurisdictions, innovation hubs serve as a prior step for applying to the regulatory sandbox.

104. **Innovation hubs may be established as part of supranational collaboration initiatives.** This is the case for the Bank for International Settlements (BIS) Innovation Hub scheme, which was established by 60 central banks with the aim to identify and develop in-depth insights into critical trends in financial technology of relevance to central banks, to explore the development of public goods to enhance the functioning of the global financial system, and to serve as a focal point for a network of central bank experts on innovation.

105. **Regulatory sandboxes are also a common innovation facilitator.** Similar objectives are followed by the 15 jurisdictions that have a regulatory sandbox in operation, such as: (i) reducing the time and cost of introducing innovative products or services to consumers; (ii) analysing the risks of new business models and underlying technologies; and (iii) assessing if the regulatory approach is balanced for mitigating those risks while enabling innovation in their markets.

106. **There are various operating schemes for regulatory sandboxes.** Schemes differ in terms of targeted participants, eligibility criteria for accepting projects, testing parameters, application process and exit strategy. For example, in Australia the ASIC regulatory sandbox is targeted towards only new unregulated entrants that do not hold a licence to carry out a regulated financial service, while in most jurisdictions these initiatives are also open to regulated institutions and technology providers. In some jurisdictions (Abu Dhabi, Japan and the UK), participants are accepted under a cohort scheme, while in other jurisdictions participants are accepted in an ongoing basis.

107. **In general, most sandboxes are open to any innovative project that benefits consumers.** Only a few surveyed jurisdictions are narrowing their attention to certain topics or technologies (commonly referred as "thematic sandboxes"). Such is the case of Japan's FSA, which tested a small cohort of projects focused on customer identity verification, or Abu Dhabi Global Markets RegLab, which completed a cohort focused on SME finance.

108. **Depending on the supervisory architecture, regulatory sandboxes may be established by different financial authorities**. Such is the case in Hong Kong, where the Insurance Authority, the Monetary Authority and the Securities and Futures Commission have launched their respective sandboxes. In this scheme, if a firm intends to conduct a pilot trial of a cross-sector fintech product, it may apply for access to the sandbox it considers most relevant. The regulator will act as the primary point of contact and assist in liaising with the other regulators.

109. **Some jurisdictions with a regulatory sandbox have implemented a "fast track" approach for the adoption of specific fintech innovations in their markets.** For example, Singapore has created a Sandbox Express to enable firms that intend to conduct certain activities regulated by MAS (eg conducting business as an insurance broker, establishing or operating an organised market and remittance business) to quickly start experimenting with their innovations within pre-determined boundaries, without having to go through the existing sandbox application. Similarly, the Insurance Authority of Hong Kong

[94] See definitions in BCBS (2018).

has introduced a fast track to expedite applications for new authorisation to carry on insurance business in or from Hong Kong using solely digital distribution channels.

110. **Regulatory sandboxes may be established at an international level by financial authorities from multiple jurisdictions.** For example, the Global Financial Innovation Network is an international alliance of government regulators led by UK's FCA seeking, among other objectives, to provide firms with an environment to trial cross-border solutions. To date, this global sandbox scheme is composed of 50 financial authorities, central banks and international organisations.

111. **Innovation accelerators have also been established in a few jurisdictions.** From the survey responses, the following five jurisdictions have an accelerator in operation: Brazil, Canada, France, Hong Kong and Singapore. In general, under these schemes the central bank supports the development and/or funding of projects that use innovative technologies for specific use cases in central banking operations or in the conduct of supervisory activities. For example, in France the ACPR has set up an "intrapreneurship" programme, relying on the Bank of France innovation accelerator, in order to develop dedicated supervisory tools (suptech).

Section 6 – Further considerations for financial sector authorities

112. **A key challenge of any regulatory approach to fintech activities will be to continue to prevent regulatory arbitrage.** Authorities may need to assess whether regulation establishes unwarranted differences in the requirements that incumbents or new entrants in specific markets must satisfy. They would need to assess the extent to which those discrepancies can be justified on the basis of the comparison of the risks that different types of institutions can generate when performing the same activity.[95]

113. **With the entrance of big tech firms as direct competitors of traditional financial institutions in the financial system, authorities will face new challenges at both a national and international level.** Given their wide customer base, high capitalisation, expertise in innovative technologies and ability to use customer-permissioned non-financial data, big tech firms may have some competitive advantages.[96] This might reduce the resilience of financial institutions, either by affecting their profitability or by reducing the stability of their funding, with the potential to change the competitive dynamics in financial services.[97] In this case, the challenge for authoritites will be to design an adequate policy framework that addresses the risks on fair competition and financial stability on both a domestic and an international level.

114. **Likewise, the emergence of global stablecoins poses new risks that will require authorities to coordinate at both the national and international level.** Global stablecoins refer to stablecoin initiatives sponsored by big tech firms or large financial firms that have the potential to scale rapidly to achieve a global or other substantial footprint. The G7 Working Group on Stablecoins has identified that this type of stablecoins may pose challenges and risks to fair competition, financial stability, monetary policy and, in the extreme, the international monetary system (Box 1). Thus, cross-sectoral and cross-border coordination will be essential to ensure a globally consistent response to mitigating risks.

95 See Restoy (2019).

96 See FSB (2019a).

97 See FSB (2019d).

115. **A major challenge for authorities will be overcoming the lack of harmonised standards and interoperability in some enabling technologies.** For example, the lack of commonly accepted API standards is a challenge in some jurisdictions, posing potential inefficiencies for third parties or fragmentation of the digital financial ecosystem.[98] Similarly, there is a worldwide need to develop international standards that will allow for interoperability and compatibility among multiple DLT protocols.

116. **For AI and ML applications, fairness, accountability and transparency will be key elements on which supervisors may need to focus their regulatory attention.** Different algorithms on the same raw data may result in very different outcomes, posing questions about how data are processed, and the potential for discrimination, financial exclusion and even exploitation.[99] Thus, authorities may need to refine governance and risk management frameworks generally considered to apply to AI and ML models to address the unique risks posed by AI and ML in terms of ethics and bias, as well as to build internal capacity or hire experts needed to assess AI and ML models.[100]

117. **Institutions' increasing reliance on third-parties in services with a high concentration of providers may pose new risks and challenges for the financial system.** Application of digital technologies to financial services may increase institutions' reliance on IT and third-party data providers. If third-party dependencies increase in critical services with a high degree of concentration among service providers, an operational failure, cyber incident or insolvency could disrupt the activities of multiple financial market participants. Systemic operational and cyber security risks may arise if systemically important institutions do not appropriately manage risks associated with outsourcing critical services to third parties.[101] Such could be the case of cloud or AI and ML providers.[102]

118. **For a digital strategy to succeed in harnessing the benefits of a digital economy, authorities may need to design a digital infrastructure and harmonised public policies on digital ID and data privacy, security and sharing regimes.** This may require strong coordination among multiple authorities (eg financial, competition, consumer protection) as well as involvement with industry, academia and the community.

119. **Implementation of digital ID systems may bring economic value and social benefits for economies but also comes with relevant challenges that authorities may need to assess.** Digital IDs support the development of inclusive digital financial services. In the process of designing and implementing digital ID schemes, authorities may need to assess potential risks and misuses by the public (eg for political manipulation) or private sector (eg for commercial gain).[103]

120. **As the economic value of personal data increases, data protection frameworks may need to be updated.** In some jurisdictions, data ownership is not clearly defined and controls over such data are not explicit. Given the economic benefits from the use of such data, authorities may need to enhance their frameworks to introduce customer rights to own and control their data. In addition, they may need to enhance their coordination with competition and data protection authorities at a national and international level concerning the definition of regulatory approaches on issues of personal data usage in financial services. Distribution of economic gains from the use of data among customers, financial

98 See BCBS (2019c).

99 See Carstens (2019).

100 See BCBS (2019b).

101 See FSB (2019a).

102 See FSB (2017c and 2019a,c).

103 See McKinsey (2019).

institutions, big techs and others, and about the impact on competition, will also be one of the most important challenges that authorities will face going forward.[104]

121. **As cyber attacks continue to be a major risk for financial institutions, increasing cyber resilience in the financial sector will remain a priority for supervisory authorities.** This may require implementing or strengthening existing cyber security frameworks with new measures. For example, some authorities might introduce red team testing requirements to identify potential weaknesses in financial institutions' cyber protection, detection and response capabilities in order to establish an effective remediation plan.[105] Other approaches might entail performing a sector-wide simulation exercise to assess the financial sector's ability to respond to a cyber attack scenario (eg Bank of England cyber simulation exercise).

122. **While innovation facilitators may bring several benefits to the market, authorities may need to address potential risks.** In particular, experiences reviewed for the purpose of this paper showed that consumers interpret that being in a sandbox or accelerator is a stamp of quality/approval from the regulator. Thus, a key challenge for authorities will be to highlight to customers that the financial product that they are acquiring is in a testing phase.

[104] See Carstens (2019).

[105] For a detailed analysis of red team testing, see Kleijmeer et al (2019).

Box 1

Global stablecoins

G7 Working Group on Stablecoins report: investigating the impact of global stablecoins

This report is born from the initiative of the French G7 presidency which, due to the recent increased innovation in payment services, considered stablecoins a crucial topic to research. The general consensus is that while national payments have improved a lot over the last decade, cross-border payments, especially in retail, remain a challenge. Cryptoassets remain too volatile to serve as a trustworthy alternative to remedy those problems. Stablecoins, however, intend to overcome these shortcomings.

Stablecoins have been designed so that the value of the coin is pegged to an underlying basket of assets or currencies to stabilise its value. This characteristic, it is argued, makes them more suitable as a means of payment or store of value. Retail stablecoins could overcome frictions in payment markets and make them more efficient and inclusive. These advantages, however, come with risks. The G7 report explores the new challenges linked to stablecoins and focuses more specifically on those arising from stablecoins initiatives with a *global* reach. These may be launched by large technology or financial firms with a vast user base. For these reasons and due to their size and potential reach, they create unique risks. The principal risks linked to (global) stablecoins are

- Legal certainty
- Sound governance, including investment rules of the stability mechanism
- AML, CFT and other forms of illicit finance
- Safety, efficiency and integrity of payment systems
- Cyber security and operational resilience
- Market integrity
- Data privacy, protection and portability
- Consumer and investor protection
- Tax compliance

Stablecoins with a global reach could pose additional challenges to:

- Monetary policy and sovereignty
- Financial stability
- The international monetary system
- Fair competition

The G7 report argues that no global stablecoin project should be undertaken until the necessary legal, regulatory and oversight challenges have been correctly addressed. Public authorities should adapt their regulatory frameworks in a way that is technology-neutral and does not hinder innovation, as long as it does not conflict with other public policy goals.

Source: G7 Working Group on Stablecoins (2019). For more information regarding the work of the G7 on stablecoins, please see the section of the Bank of France's website on the G7 and speeches of B Cœuré.

Section 7 – Concluding remarks

123. **Fintech has not changed the core mission of financial regulators.** Their main objective is to keep the financial system safe and sound. The financial system relies on trust – losing sight of risks to the stability and integrity of the financial system could jeopardise that trust. Without it, the potential benefits of fintech are unlikely to materialise. Moreover, to date, technological developments have not yet resulted in any major changes in the structure of financial regulation. In their core content, the rulebooks on prudential safeguards, consumer protection and market integrity remain broadly unaffected.[106] However, when regulating fintech, authorities are seeking to find a balance that encourages innovation while minimising potential risks to the financial system. In the quest for this balance, authorities face important policy trade-offs. For example, because novel fintech activities carry unknown risks, regulators may feel compelled to impose stringent prudential or conduct requirements. While these may be intended to ensure financial stability and consumer protection, they may be detrimental to competition and innovation more generally.

124. **Most fintech activities covered in this paper are regulated in one form or another.** Depending on the activity, several authorities have put in place dedicated regulatory regimes.[107] When this is not the case, fintech activities are normally subject to existing regulations. For example, taking deposits and providing financial advice are typically regulated activities. Hence, any firm that performs any of these activities is regulated. In such a case, an authority may decide not to create a bespoke fintech regime for a given fintech activity if it deems the existing requirements to be sufficient.

125. **Cooperation and coordination at the local and international level remain crucial.** At the local level, financial authorities are engaging with other public agencies responsible for data privacy, consumer protection, competition, digitalisation, financial inclusion, cyber security and market integrity. The challenge here is that the more authorities are tasked with these objectives, the more coordination within a jurisdiction is needed. At the international level, financial authorities benefit from sharing information on their regulatory approaches and supervisory practices with each other. Based on this exchange of information, authorities may also choose to agree on best practices or international standards.

126. **Authorities may need to adjust their supervisory architecture and practices to fintech activities.** While most surveyed authorities supervise fintech activities as part of the ongoing supervisory process within their existing organisational structure, a few introduced visible changes to their organigram. For example, some authorities have established a general dedicated fintech unit (eg the Fintech Department at the Polish KNF) while others have established a fintech unit specialised in the supervision of a certain activity (eg the Supervisory Direction for Crowdfunding and E-money Institutions at the Mexican CNBV). In case fintech is dealt with by existing supervisory units, these may be supported by a dedicated unit. For example, the Bank of Italy created a specific unit, the Fintech Sector, within its Supervision Department, to support other units on how to approach fintech matters. In Austria, the FMA established the Fintech Point of Contact to coordinate fintech-related matters between different departments.

127. **Having adequate expertise and resources will be critical components for the supervision of fintech developments.** One of the main challenges for authorities is to have sufficient resources and expertise to keep up with the speed of technological change, to understand novel business models and develop adequate policy responses.

[106] See Restoy (2019).

[107] The regulatory approach taken for fintech activities is influenced by the supervisory architecture. A case in point is platform financing in Brazil, where equity crowdfunding platforms need to be licensed by the Securities and Exchange Commission, and loan crowdfunding platforms and fintech balance sheet lenders by the Central Bank of Brazil.

128. **In a similar way, collecting data related to fintech developments and adjusting regulatory reporting requirements will be a common challenge in most jurisdictions.** Wherever licensed, authorities are obtaining information from regulated entities, including new entrants offering fintech services, through regulatory reporting. Other sources include information obtained through innovation facilitators or through the research of other public and private organisations. However, a survey conducted in 2019 by the Irving Fisher Committee found that fintech developments present various challenges to statisticians in a number of central banks.[108] Some of these challenges are related to the granularity of data required to identify fintech firms and the integration of fintech activitites in business classifications.

[108] See IFC (2020).

References

Adrian, T and T Mancini-Griffoli (2019): "The rise of digital money", International Monetary Fund, *FinTech Notes,* Note/19/01.

Australian Prudential Regulation Authority (2018a): "ADI licensing: restricted ADI framework", *Information Paper*.

——— (2018b): "Authority to carry on banking business".

Basel Committee on Banking Supervision (2018): "Implications of fintech developments for banks and bank supervisors", *Sound practices*, February.

——— (2019a): "*Statement on crypto-assets*", March.

——— (2019b): "High-level summary: BCBS SIG industry workshop on the governance and oversight of artificial intelligence and machine learning in financial services", Supervision and Implementation Group, October.

——— (2019c): "Basel Committee discusses policy and supervisory initiatives and approves implementation reports", October.

——— (2019d): *Report on open banking and application programming interfaces (APIs)*, November.

Bank for International Settlements (2019): "Big tech in finance: opportunities and risks", *Annual Economic Report 2019,* June, pp 55–79.

BBVA Research (2016): "Protection of customers' funds in electronic money: a myriad of regulatory approaches".

Blandin A, A Cloots, H Hussain, M Rauchs, R Saleuddin, J Grant Allen, B Zhang and K Cloud (2019): "Global cryptoasset regulatory landscape study", *Cambridge Centre for Alternative Finance*.

Carstens, A (2019): "Data, technology and policy coordination", keynote speech at the 55th SEACEN Governors' Conference and High-level Seminar on "Data and technology: embracing innovation", Singapore, 14 November 2019.

Claessens, S, J Frost, G Turner and F Zhu (2018): "Fintech credit markets around the world: size, drivers and policy issues", *BIS Quarterly Review,* September, pp 29–49.

Committee on Payment and Settlement Systems (2004): *Survey of developments in electronic money and internet and mobile payments*, March.

Committee on Payments and Market Infrastructures (2014): *Non-banks in retail payments*, September.

——— (2016): *A glossary of terms used in payments and settlement systems*.

——— (2018): *Cross-border retail payments*, February.

Committee on Payment and Market Infrastructures and International Monetary Fund (2019): "Investigating the impact of global stablecoins", *G7 Working Group on Stablecoins*, October.

Committee on the Global Financial System and the Financial Stability Board (2017): *Fintech credit: market structure, business models and financial stability implications*, May.

Crisanto, J and J Prenio (2017): "Regulatory approaches to enhance bank's cyber-security frameworks", *FSI Insights on policy implementation*, no 2, August.

Crisanto, J, C Donaldson, D Garcia Ocampo and J Prenio (2018), "Regulating and supervising the clouds: emerging prudential approaches for insurance companies", *FSI Insights on policy implementation*, no 13, December.

D'Silva, D, Z Filkova, F Packer and S Tiwari (2019), "The design of digital financial infrastructure: lessons from India", *BIS Papers*, no 106, December.

European Banking Authority: *Glossary for financial innovation*.

——— (2018): *EBA Report on the prudential risks and opportunities arising for institutions from fintech*, July.

——— (2019a): "EBA clarification to issues I to III raised by participants of the EBA Working Group on APIs under PSD2", 11 March.

——— (2019b): "EBA responses to issues IV to VII raised by participants of the EBA Working Group on APIs under PSD2", 1 April.

——— (2019c): "EBA responses to issues VIII to XIII raised by participants of the EBA Working Group on APIs under PSD2", 26 April.

European Central Bank (2018): *Guide to assessment of fintech credit institution licence applications*, March.

European Commission (2018a): "Crowdfunding".

——— (2018b): "Commission proposal for a regulation on European crowdfunding services providers", March.

European Securities and Markets Authority (2019): "National thresholds below which the obligation to publish a prospectus does not apply", February.

European Securities and Markets Authority, European Banking Authority and European Insurance and Occupational Pensions Authority (2018): "FinTech: regulatory sandboxes and innovation hubs", *Joint Report*.

Financial Action Task Force (2019a): "Public Statement on Virtual Assets and Related Providers", 21 June.

——— (2019b): *Draft Guidance on Digital Identity*, 21 November.

Financial Stability Board (2017a): *Financial stability implications from FinTech: supervisory and regulatory issues that merit authorities' attention*, 27 June.

——— (2017b): *Stocktake of publicly released cybersecurity regulations, guidance and supervisory practices*, 13 October.

——— (2017c): *AI and ML in financial services: market developments and financial stability implications*.

——— (2019a): "FinTech and market structure in financial services: market developments and potential financial stability implications", 14 February.

——— (2019b): "Crypto-assets: work underway, regulatory approaches and potential gaps", 31 May.

——— (2019c): "Third-party dependencies in cloud services: considerations on financial stability implications", 9 December.

——— (2019d): "Big tech in finance: market developments and potential stability implications", 9 December.

——— (2019e): "Decentralised financial technologies: Report on financial stability, regulatory and governance implications", 6 June.

FINMA (2019a): "FINMA publishes 'stable coin' guidelines".

——— (2019b): "Supplement to the guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)", September.

Havrylchyk, O (2018): "Regulatory framework for the loan-based crowdfunding platforms", *OECD Economics Department Working Papers*, no 1513.

Hong Kong Monetary Authority (2018a): "Authorization of virtual banks", *Guide to Authorization*, Chapter 9.

——— (2018b): "Guideline on minimum criteria for authorization".

——— (2019): *High-level principles on artificial intelligence*.

International Association of Insurance Supervisors (2017): *Report on fintech developments in the insurance industry*, 21 February.

——— (2018a): *Application Paper on the Use of Digital Technology in Inclusive Insurance*, November.

——— (2018b): *Issues Paper on Increasing Digitalisation in Insurance and its Potential Impact on Consumer Outcomes*, November.

International Monetary Fund (2017): "Fintech and financial services: initial considerations", *Staff Discussion Notes*, no 17/05.

International Monetary Fund and the World Bank Group (2018): *The Bali Fintech Agenda: a blueprint for successfully harnessing fintech's opportunities*.

——— (2019): *Fintech: the experience so far*.

International Organization of Securities Commissions (2017): *IOSCO research report on financial technologies (Fintech)*.

Irvin Fisher Committee on Central Bank Statistics (2020*): 2019 IFC Annual Report*, January.

Joint Committee of the European Supervisory Authorities (ESA) (2016): "Report on automation in financial advice".

——— (2018): "Joint committee report on the results of the monitoring exercise on 'automation in financial advice'".

Kleijmeer, R, J Prenio and J Yong (2019): "Varying shades of red: how red team testing frameworks can enhance the cyber resilience of financial institutions", *FSI Insights on policy implementation*, no 21.

Massachusetts Securities Division (2016): "Policy statement: robo-advisers and state investment adviser registration".

Mayer Brown Perspective (2019): "Federal court allows New York Department of Financial Services to proceed with lawsuit challenging proposed OCC fintech charter".

McKinsey Global Institute (2019): *Digital identification: a key to inclusive growth*.

Monetary Authority of Singapore (2018): *Principles to promote fairness, ethics, accountability and transparency (FEAT) in the use of artificial intelligence and data analytics in Singapore's financial sector*.

——— (2019): *Digital full bank framework*.

Netherlands Bank (2019): *General principles for the use of Artificial Intelligence in the financial sector*.

Organisation for Economic Co-operation and Development (2016): "Policy measures to improve the quality of financial advice for retirement", *OECD Pensions Outlook 2016*.

——— (2017): *Robo-advice for pensions*.

Prudential Regulation Authority and Financial Conduct Authority (2018): "New bank start-up unit: what you need to know from the UK's financial regulators".

Restoy, F (2019): "Regulating fintech: what is going on, and where are the challenges?", speech at the ASBA-BID-FELABAN XVI Banking public-private sector regional policy dialogue "Challenges and opportunities in the new financial ecosystem", Washington DC, 16 October.

Schweizerische Eidgenossenschaft (2018): *Revision der Bankenverordnung (BankV) «Fintech-Bewilligung»*, November.

World Economic Forum (2015): *The future of financial services*.

World Bank Group and Cambridge Centre for Alternative Finance (2019): *Regulating alternative finance: results from a global regulator survey*.

World Bank Group and Global Partnership for Financial Inclusion (2018): *G20 Digital Identity Onboarding*.

Yu, T and W Shen (2019): "Funds sharing regulation in the context of the sharing economy: Understanding the logic of China's P2P lending regulation", *Computer Law and Security Review,* vol 35, pp 42–58.

Annex 1 – List of jurisdictions

1. Argentina (AR)
2. Australia (AU)
3. Austria (AT)
4. Belgium (BE)
5. Brazil (BR)
6. Canada (CA)
7. Chile (CL)
8. China (CN)
9. Colombia (CO)
10. Europe (EU/ECB)
11. France (FR)
12. Germany (DE)
13. Hong Kong SAR (HK)
14. Italy (IT)
15. Japan (JP)
16. Luxembourg (LU)
17. Mexico (MX)
18. Netherlands (NL)
19. Peru (PE)
20. Philippines (PH)
21. Poland (PL)
22. Russia (RU)
23. Saudi Arabia (SA)
24. Singapore (SG)
25. South Africa (ZA)
26. Spain (ES)
27. Sweden (SE)
28. Switzerland (CH)
29. Turkey (TR)
30. United Arab Emirates (AE)
31. United Kingdom (GB)
32. United States (US)

Annex 2 – Glossary of terms

Fintech activities

Cryptoassets: a type of private asset that depends primarily on cryptography and distributed ledger or similar technology as part of its perceived or inherent value. (FSB)

Digital banks: deposit-taking institutions that are members of a deposit insurance scheme and deliver banking services primarily through electronic channels instead of physical branches.

Digital payment services: digital payment service providers make use of technology to facilitate payment transactions by transferring money, clearing or settling balances digitally, without the use of physical money.

E-money services: issuance of debt-like instruments (e-money[109]) for the purpose of facilitating payment transactions.

Equity crowdfunding: an activity where investors provide funding to private companies in the form of equity. The fintech platform matches investors with companies they want to invest in, enabling them to participate in the early capital-raising activities of startups and other companies.

Financial activities related to cryptoassets: include creating, distributing, storing or exchanging cryptoassets, using them for investment or payment purposes, or as reference in financial products.

Fintech balance sheet lending: a credit activity facilitated by internet-based platforms (not operated by commercial banks) that use their own balance sheet in the ordinary course of business to intermediate borrowers and lenders.

Fintech platform financing: a funding activity facilitated by internet-based platforms (not operated by commercial banks). Fintech platform financing includes balance sheet lending, loan crowdfunding or equity crowdfunding.

Insurtech business models: technology-driven innovative business models that are emerging in two major areas of insurance: (i) distribution, such as comparison portals and digital brokers; and (ii) underwriting, such as mobile, on-demand, usage-based or technology-enabled peer-to-peer and parametric insurance.

Loan crowdfunding: a credit activity facilitated by internet-based platforms (not operated by commercial banks) that match borrowers with lenders. Individual loan contracts are established between borrowers and lenders, without the platform being engaged in risk transformation.

Robo-advice: financial advice on investment products that is provided with no or limited human intervention and relies on technology to automate the client onboarding process and the generation of advice through algorithm-based tools.

Enabling technologies

Application programing interfaces (APIs): a set of rules and specifications followed by software programs to communicate with each other, forming an interface between different software programs that facilitates their interaction. (BCBS)

[109] Money may be issued or stored electronically – eg on a device such as a chip card (eg payment cards), a hard drive in a personal computer or a server – with the purpose of replacing physical money in payment transactions.

Artificial intelligence (AI): information technology (IT) systems that perform functions requiring human capabilities. AI can ask questions, discover and test hypotheses, and make decisions automatically based on advanced analytics operating on extensive data sets. (BCBS)

Biometrics: automated recognition of individuals based on their biological and behavioural characteristics.[110] It covers a variety of technologies in which unique identifiable attributes of people are used for identification and authentication. These include (but are not limited to) a person's fingerprint, iris print, hand, face, voice, gait or signature, which can be used to validate the identity of individuals.

Cloud computing: the use of an online network ("cloud") of hosting processors to increase the scale and flexibility of computing capacity. This model enables convenient on-demand network access to a shared pool of configurable computing resources (for example networks, servers, storage facilities, applications and services) that can be rapidly released with minimal management effort or service provider interaction. (BCBS)

Distributed ledger technology (DLT): a means of recording information through a distributed ledger, that is, a repeated digital copy of data at multiple locations. This technology enables nodes in a network to securely propose, validate and record state changes (or updates) to a synchronised ledger that is distributed across the network's nodes. (BCBS)

Machine learning (ML): a method of designing problem-solving rules that improve automatically through experience. ML algorithms give computers the ability to learn without specifying all the knowledge a computer would need to perform the desired task. The technology also allows computers to study and build algorithms that they can learn from and make predictions based on data and experience. ML is a subcategory of AI. (BCBS)

Policy enablers

Cyber crime: when a computer system or component is the object of a crime (hacking, phishing, spamming) or is the facilitator of a crime (such as theft of information or money). (BCBS)

Cyber resilience: a financial market infrastructure's ability to anticipate, withstand, contain and rapidly recover from a cyber attack (CPMI-IOSCO)

Cyber risk: the combination of the probability of an event occurring within the realm of an organisation's information assets, computer and communication resources and the consequences of that event for the organisation. (CPMI-IOSCO, BCBS)

Digital ID system: a system that covers the process of identity proofing/enrolment and authentication. Identity proofing and enrolment can be either digital or physical (documentary), or a combination, but binding, credentialing, authentication, and portability/federation must be digital. (FATF)

Innovation accelerator: a partnership arrangement between fintech providers and central banks/supervisory agencies to develop use cases that may involve funding support and/or authorities' endorsement/approval for future use in central banking operations or in the conduct of supervisory tasks. (BCBS)

Innovation hub: an innovation facilitator set up by supervisory agencies that provides support, advice or guidance to regulated or unregulated firms in navigating the regulatory framework or identifying supervisory policy or legal issues and concerns. (BCBS)

Open banking: the sharing and leveraging of customer-permissioned data from banks with third-party developers and firms to build applications and services that provide real-time payments, greater financial transparency options for account holders, marketing, etc. (BCBS (2019d))

[110] See definition of the Biometrics Institute: www.biometricsinstitute.org/definition-of-biometrics.

Regulatory sandbox: a controlled testing environment, sometimes featuring regulatory forbearance and alleviation through the use of legally provided discretions by the supervisory agency. The testing environment may involve limits or parameters within which the firms must operate (eg restrictions on the time a firm may operate in the sandbox). (BCBS)

Annex 3 – Horizontal regulatory schemes

Among surveyed jurisdictions, there are two distinct approaches for regulating fintech activities. Under the most common, the regulatory framework is designed to target a specific fintech activity (eg loan crowdfunding), ie the approach is business model-centric or vertical. In contrast, under the second approach, the regulatory framework is designed to enable more than one fintech activity, ie the approach is horizontal (Box 2).

Box 2

Horizontal regulatory approach: the cases of Switzerland and the United States

Some authorities have introduced licence regimes that do not target a specific fintech business model but enable fintech companies from various sectors to perform a specific regulated activity. A prominent example is the Swiss fintech licence. Instead of being required to obtain a full banking licence, fintech licence holders may accept a limited amount of deposits from the public as long as they do not use these funds to lend or invest. Another example is the Special Purpose National Bank Charter for fintech companies planned by the Office of the Comptroller of the Currency (OCC) in the United States.

Fintech licence in Switzerland. Amendments to the Banking Act that entered into force on 1 January 2019, creating a new authorisation category that allows licence holders to accept public deposits of up to CHF 100 million. Deposits need to be transferred, repaid or kept segregated and liquid, and must not be invested, and licence holders cannot pay interest on them as deposit-based lending business remains reserved for banks. Further, deposits are not covered by the Swiss deposit insurance scheme and customers need to be informed as such (Schweizerische Eidgenossenschaft (2018)).①

Special purpose national banks (SPNBs) in the United States. In July 2018, the OCC issued a Supplement to the Comptroller's Licensing Manual to clarify how the OCC would evaluate applications for an SPNB charter from fintech companies that would engage in lending money or paying checks, but would not take deposits.②③ While SPNBs would be subject to the same laws and regulations that apply to all federally chartered banks, irrespective of whether new delivery channels or technology is used, the OCC may tailor its standards based on a bank's business model and activities. As such, the OCC expects fintech SPNBs to establish a contingency plan that includes options to sell, wind down or merge with a non-bank affiliate, and demonstrate an ongoing commitment to financial inclusion.

① While the fintech licence enables more than one fintech activity, it may be of particular use for fintech companies involved in crowdfunding, e-money or payments. ② An SPNB, according to OCC definition, is a national bank that engages in a limited range of banking or fiduciary activities, targets a limited customer base, incorporates non-traditional elements or has a narrowly targeted business plan. ③ In response, the New York Department of Financial Services (DFS) filed a lawsuit in federal court against the OCC, claiming that issuing SPNB charters to non-depository institutions exceeded the OCC's authority under the National Bank Act. In May 2019, the US District Court for the Southern District of New York found in favour of the DFS, arguing that the National Banking Act permits the OCC to charter firms that engage in the "business of banking," which, as used in the National Bank Act, "unambiguously requires receiving deposits as an aspect of the business." (Mayer Brown Perspectives (2019)).

Annex 4 – Fintech-specific regulations for loan and equity crowdfunding

Selected regulatory requirements for crowdfunding platforms

Annex Table 1

Areas	**Examples**
Transparency	Disclosure of information about risks, the platform itself, conflicts of interest
Know your customer and AML/CFT	Need to establish identity of investors and borrowers/issuers
Safekeeping of clients' money	Mandated use of a licensed bank or trust account that is separated from own funds
Risk management	Internal procedures for conducting due diligence on fundraisers, minimum standards for credit risk analysis if loans are priced by the platform
Thresholds and eligibility	Caps on amounts per issue or loan, maximum amount an investor can invest,* restrictions on certain investor types such as qualified investors
Governance, fitness and proprietary	Requirement to have a risk, compliance and internal audit function, sufficient professional qualifications of managers and directors
Risk retention	Requirement to retain or not to retain any part of the credit risk
Business continuity	Wind-down plans and resolution procedures
Prudential requirements	Minimum capital or the requirement to take out a professional liability insurance policy that covers certain amounts**

* For example, less experienced investors in the UK can invest no more than 10% of net investable assets. This limit is removed once an investor has made two or more investments in the past two years and is therefore reclassified as a sophisticated investor.

** Minimum capital or insured amounts may be expressed either as fixed minimum amounts or a percentage of loaned funds.

Sources: EC (2018b); OECD (2018); national rules and regulations; FSI survey.

Regulations for loan and equity crowdfunding – selected features

Annex Table 2

	Maximum amount per project or loan	Maximum amount per investor	Minimum capital requirements	Risk retention
France	LCF: €1 million per project ECF: €8 million per year and project	LCF: €2,000 per loan if interest-paying; €5,000 for interest-free loan ECF: No limit	No, but professional insurance policy required, covering: LCF: €250,000 per event, €500,000 per year ECF: €400,000 per event, €800,000 per year	Forbidden
Spain	€2 million per year and project (qualified investors: €5 million)	€3,000 per project and €10,000 per year No limit for qualified investors	€60,000 or professional insurance policy or combination of both*	Up to 10% of project
United Kingdom	No restriction (but prospectus required for ECF above €8 million)	10% of net investable assets for less experienced investors (no limit for other investors)	ECF: €50,000 BCF: €50,000 or a percentage of loaned funds (whichever is higher)	No restriction

* If funds raised exceed €2 million in a yearly period, minimum capital requirements increase to €120,000 (in addition, own resources required increase further (up to €2 million) in proportion to the funds raised in said period when above €5 million).

ECF=equity crowdfunding; LCF=loan crowdfunding.

Sources: EC (2018b); OECD (2018); national rules and regulations; FSI survey.