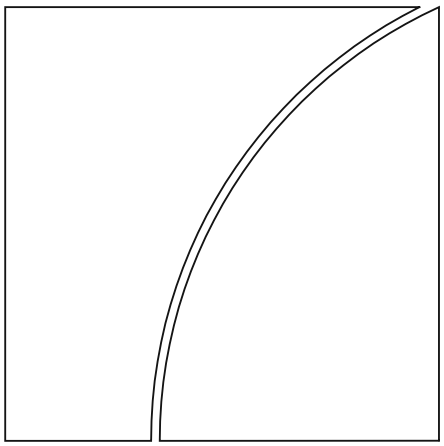
Basel Committee
on Banking Supervision

Consultative Document



Sound Practices: Implications of fintech developments for banks and bank supervisors

Issued for comment by 31 October 2017

August 2017

BANK FOR INTERNATIONAL SETTLEMENTS

This publication is available on the BIS website (www.bis.org).

ISBN 978-92-9259-087-1 (online)

Contents

Executive summary

Interest is growing in financial technology, or "fintech". In recent years, sizeable investments have been made by both banks and venture capital funds, indicating the expectations for substantial change. Against this backdrop, the Basel Committee on Banking Supervision (BCBS) has set up a task force to provide insight into this development, and more specifically to explore the implications for supervisors and banks' business models. This consultative document summarises the BCBS's main findings and conclusions.

As fintech developments remain fluid, the impact on banks and their business models is uncertain. While some market observers estimate that between 10–40% of revenues and 20–60% of retail banking profits are at risk over the next 10 years,[1] others claim that banks will be able to absorb the new competitors, thereby improving their own efficiency and capabilities.

The analysis presented in this paper considered several scenarios and assessed their potential future impact on the banking industry. A common theme across the various scenarios is that banks will find it increasingly difficult to maintain their current operating models, given technological change and customer expectations. Industry experts opine that the future of banking will increasingly involve a battle for the customer relationship.[2] To what extent banks or new fintech entrants will own the customer relationship varies across each scenario. However, the current position of incumbent banks will be challenged in almost every scenario.

The BCBS recognises that the emergence of fintech is only the latest wave of innovation to affect the banking industry. Banks have undergone various technology-enabled innovation phases before. However, the rapid adoption of new technologies along with their effect in lowering barriers to entry in the financial services market has fostered the emergence of new business models and many new fintech entrants. These factors may prove to be more disruptive than previous changes in the banking industry, although as with any forecast, this is in no way certain.

This Sound Practices paper combines historical research, analysis of current media and industry periodicals, surveys on BCBS members' activities, fintech product analysis, and scenario analysis to provide a forward-looking perspective on fintech and its potential impact on the banking industry. Based on this work, the BCBS has identified 10 key observations and related recommendations on supervisory issues for consideration by banks and bank supervisors.

[1] See McKinsey & Co, *Global Banking Annual Review*, 2015.

[2] Ibid.

Observations and recommendations

Observation 1: The nature and the scope of banking risks as traditionally understood may significantly change over time with the growing adoption of fintech, in the form of both new technologies and business models. While these changes may result in new risks, they can also open up new opportunities for consumers, banks, the banking system and bank supervisors.

Recommendation 1: Banks and bank supervisors should consider how they balance ensuring the safety and soundness of the banking system with minimising the risk of inadvertently inhibiting beneficial innovation in the financial sector. Such a balanced approach would promote the safety and soundness of banks, financial stability, consumer protection and compliance with applicable laws and regulations, including anti-money laundering and countering financing of terrorism (AML/CFT) regulations, without unnecessarily hampering beneficial innovations in financial services, including those aimed at financial inclusion.

Observation 2: For banks, the key risks associated with the emergence of fintech include strategic risk, operational risk, cyber-risk and compliance risk. These risks were identified for both incumbent banks and new fintech entrants into the financial industry.

Recommendation 2: Banks should ensure that they have effective governance structures and risk management processes in order to identify, manage and monitor risks associated with the use of enabling technologies and the emergence of new business models and entrants into the banking system brought about by fintech developments. These structures and processes should include:

- robust strategic and business planning processes that allow banks to adapt revenue and profitability plans in view of the potential impact of new technologies and market entrants;
- sound new product approval and change management processes to appropriately address changes not only in technology, but also in business processes;
- implementation of the Basel Committee's *Principles for sound management of operational risk* (PSMOR) with due consideration to fintech developments; and
- monitoring and reviewing of compliance with applicable regulatory requirements, including those related to consumer protection, data protection and AML/CFT when introducing new products, services or channels.

Observation 3: Banks, service providers and fintech firms are increasingly adopting and leveraging advanced technologies to deliver innovative financial products and services. These enabling technologies, such as artificial intelligence (AI)/machine learning (ML)/advanced data analytics, distributed ledger technology (DLT), cloud computing and application programming interfaces (APIs), present opportunities, but also pose their own inherent risks.

Recommendation 3: Banks should ensure they have effective IT and other risk management processes that address the risks of the new technologies and implement the effective control environments needed to properly support key innovations.

Observation 4: Banks are increasingly partnering with and/or outsourcing operational support for technology-based financial services to third-party service providers, including fintech firms, causing the delivery of financial services to become more modular and commoditised. While these partnerships can

arise for a multitude of reasons, outsourcing typically occurs for reasons of cost-reduction, operational flexibility and/or increased security and operational resilience. While operations can be outsourced, the associated risks and liabilities for those operations and delivery of the financial services remain with the banks.

Recommendation 4: Banks should ensure they have appropriate processes for due diligence, risk management and ongoing monitoring of any operation outsourced to a third party, including fintech firms. Contracts should outline the responsibilities of each party, agreed service levels and audit rights. Banks should maintain controls for outsourced services to the same standard as the operations conducted within the bank itself.

Observation 5: Fintech developments are expected to raise issues that go beyond the scope of prudential supervision, as other public policy objectives may also be at stake, such as safeguarding data privacy, data and IT security, consumer protection, fostering competition and compliance with AML/CFT.

Recommendation 5: Bank supervisors should cooperate with other public authorities responsible for oversight of regulatory functions related to fintech, such as conduct authorities, data protection authorities, competition authorities and financial intelligence units, with the objective of, where appropriate, developing standards and regulatory oversight of the provision of banking services, whether or not the service is provided by a bank or fintech firms.

Observation 6: While many fintech firms and their products – in particular, businesses focused on lending and investing activities – are currently focused at the national or regional level, some fintech firms already operate in multiple jurisdictions, especially in the payments and cross-border remittance businesses. The potential for these firms to expand their cross-border operations is high, especially in the area of wholesale payments.

Recommendation 6: Given the current and potential global growth of fintech companies, international cooperation between supervisors is essential. Supervisors should coordinate supervisory activities for cross-border fintech operations, where appropriate.

Observation 7: Fintech has the potential to change traditional banking business models, structures and operations. As the delivery of financial services becomes increasingly technology-driven, reassessment of current supervision models in response to these changes could help bank supervisors adapt to fintech-related developments and ensure continued effective oversight and supervision of the banking system.

Recommendation 7: Bank supervisors should assess their current staffing and training models to ensure that the knowledge, skills and tools of their staff remain relevant and effective in supervising new technologies and innovative business models. Supervisors should also consider whether additional specialised skills are needed to complement existing expertise.

Observation 8: The same technologies that offer efficiencies and opportunities for fintech firms and banks, such as AI/ML/advanced data analytics, DLT, cloud computing and APIs, may also improve supervisory efficiency and effectiveness.

Recommendation 8: Supervisors should consider investigating and exploring the potential of new technologies to improve their methods and processes. Information on policies and practices should be shared among supervisors.

Observation 9: Current bank regulatory, supervisory and licensing frameworks generally predate the technologies and new business models of fintech firms. This may create the risk of unintended regulatory gaps when new business models move critical banking activities outside regulated environments or, conversely, result in unintended barriers to entry for new business models and entrants.

Recommendation 9: Supervisors should review their current regulatory, supervisory and licensing frameworks in light of new and evolving risks arising from innovative products and business models. Within applicable statutory authorities and jurisdictions, supervisors should consider whether these frameworks are sufficiently proportionate and adaptive to appropriately balance ensuring safety and soundness and consumer protection expectations with mitigating the risk of inadvertently raising barriers to entry for new firms or new business models.

Observation 10: The common aim of jurisdictions is to strike the right balance between safeguarding financial stability and consumer protection while leaving room for innovation. Some agencies have put in place approaches to improve interaction with innovative financial players and to facilitate innovative technologies and business models in financial services (eg innovation hubs, accelerators, regulatory sandboxes and other forms of interaction) with distinct differences.

Recommendation 10: Supervisors should learn from each other's approaches and practices, and consider whether it would be appropriate to implement similar approaches or practices.

This Sound Practices paper includes an overview of the research and analysis conducted to arrive at the observations and recommendations outlined above. The observations and recommendations can be used as a basis for determining follow-up actions by individual supervisors, as well as future BCBS monitoring of risks associated with emerging technologies and innovative business models.

Part I – Introduction

In recent years, technology-driven innovation in financial services, or "fintech", has attracted increasing attention. The BCBS mandated a task force to analyse financial technology innovations and emerging business models in the banking sector. This consultative document presents the results of the analysis undertaken to identify and assess risks and related supervisory challenges, both for banks and bank supervisors.

The work was conducted in two main phases. First, the BCBS outlined the current fintech landscape and supervisory approaches to fintech developments, using industry research and surveys of member institutions. In the second phase, the BCBS identified the implications for banks and challenges for effective supervision, and conducted more detailed surveys on specific arrangements towards innovation and licensing practices. Using scenario analyses, the BCBS also developed its own forward-looking exercise, and analysed specific case studies. This paper presents the main findings from the work conducted and highlights 10 key observations and recommendations for banks and supervisors.

When analysing the issues at stake, the BCBS ensured that it focused not only on risks that could emerge or increase with the development of fintech but also on the benefits that technology-driven innovation could bring to financial services from the perspectives of different bank stakeholders (including customers and supervisors). The BCBS also maintained a balanced approach by considering not only the perspective of incumbent banks but also of new players.

Part II of this paper provides an overview of the fintech landscape and the current state of the industry. While the impact of fintech on banking remains uncertain, the paper suggests that change could be fast-paced and significant. Part III focuses on challenges and implications for banks. Given the considerable time required to adjust supervisory standards, practices and particularly regulations, supervisors need to take a forward-looking approach and assess what actions should be taken now to mitigate risks as well as promote positive developments in the years to come. Part IV provides recommendations for supervisors and regulatory frameworks.

Part II – Fintech developments and forward-looking scenarios

A. What is fintech?

The BCBS has opted to use the Financial Stability Board (FSB)'s working definition for 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".[3] The term fintech has exploded in popularity in recent years and is used variously to describe a wide array of innovations and actors in a rapidly evolving environment.

The results of a comparative survey on supervisory approaches indicate that most surveyed agencies have not formally defined fintech, innovation or other similar terms. Some of the reasoning provided for this lack of formal definitions was that other definitions already exist, such as that from the FSB, or that it would be premature to define a field that is rapidly evolving. However, some agencies and organisations reported that they had developed definitions for these terms. An observation from the various definitions of fintech, innovation or similar terms that were identified is that they designate an innovative service, business model (which can be provided by an incumbent bank or a non-financial

[3] The FSB has analysed the benefits and risks related to financial technology innovations from a financial stability perspective, and provides a definition in page 7 of its report *Financial Stability Implications from FinTech, Supervisory and Regulatory Issues that Merit Authorities' Attention*, 27 June 2017.

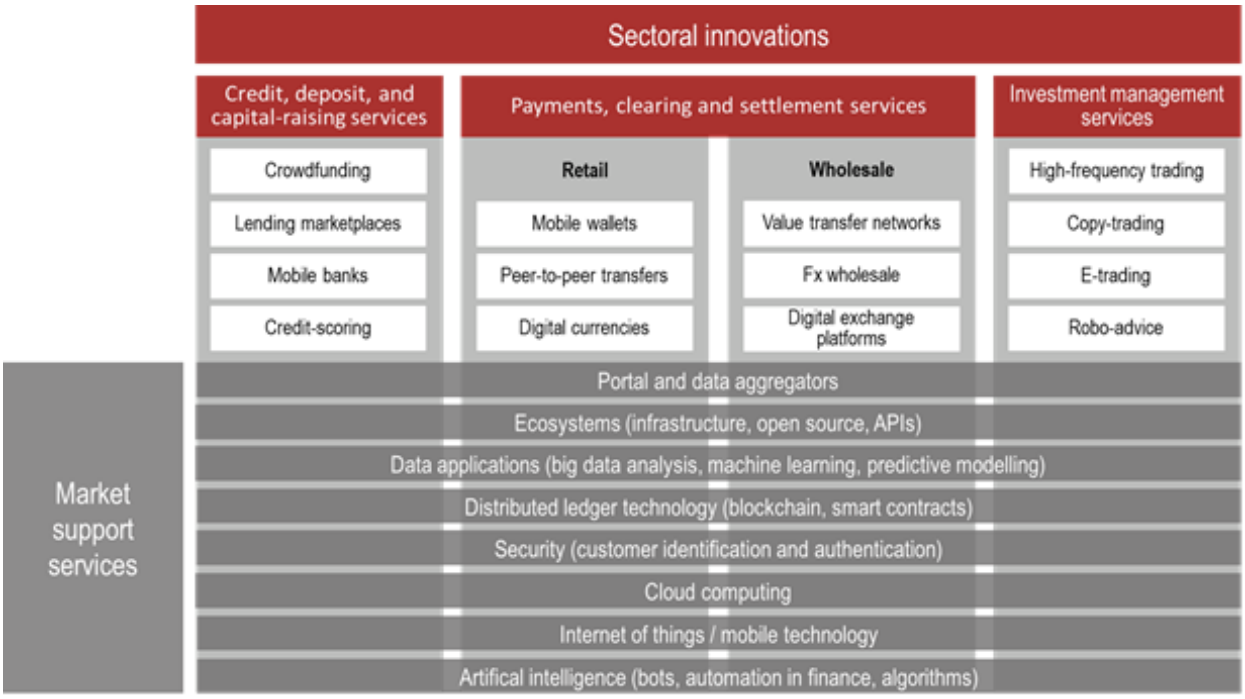
company) or a new-technology start-up in the financial industry. A second observation is that some definitions made clear distinctions between innovation and disruption, with innovation fitting within existing regulatory frameworks while disruption requires the development of new rules.

How fintech, innovation and other similar terms are defined is important, as the definition can influence how supervisors approach fintech. While no umbrella definition may be needed in order to consider fintech developments, jurisdictions may have to define specific products and services in order to set a specific approach for possible regulation. Because of the importance of clear definitions, a glossary of terms and acronyms used in this document is provided in Annex 1. This is a first attempt by the BCBS to provide a common definition of some terms related to the delivery of fintech products and services.

B. What are the key fintech products and services?

In addition to the FSB definition, the BCBS also used a categorisation of fintech innovations. Graph 1 below depicts the three product sectors, as well as market support services, that reflect the enabling technologies which support these innovative products. The three sectors relate directly to core banking services, while the market support services relate to innovations and new technologies that are not specific to the financial sector but also play a significant role in fintech developments.

Graph 1: Sectors of innovative services

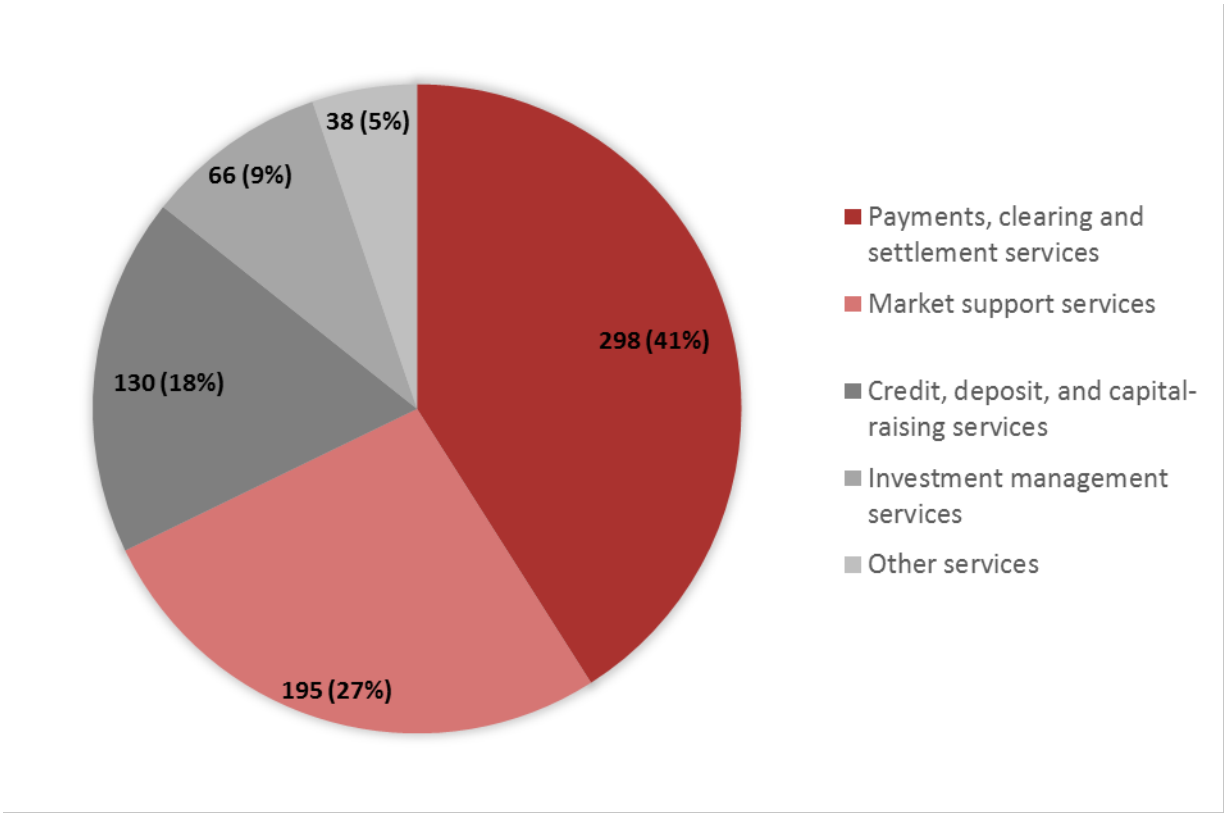


Source: BCBS.

The BCBS conducted an informal survey of its members, asking them to identify the significant fintech products and services within their jurisdictions. The number of fintech companies reported for each sector is shown in Graph 2 below.[4]

[4] Some jurisdictions have also taken steps to analyse the fintech market in more detail. See eg European Commission, *Fintech: a more competitive and innovative European financial sector*, March 2017, https://ec.europa.eu/info/finance-consultations-2017-fintech_en.

Graph 2: Survey of key providers per fintech activity[5]



Source: BCBS.

Respondents reported that the highest number of fintech service providers are in the payments, clearing and settlement category, followed by credit, deposit and capital-raising services. Within the payments, clearing and settlement category, retail payment services firms represented the majority of fintech firms identified, as compared with wholesale payment services providers. The number of market support servicers, meaning companies that provide support for fintech financial services, was second only to payments, clearing and settlement services in the number of players identified.

While the survey identified the names and made an initial attempt to quantify the number of key fintech providers and services, the absence of further data on details such as processing volumes and transaction values limits any assessment of the potential impact that these organisations may have on the incumbent banks as well as on financial systems. This exercise allowed supervisors to get a better understanding of the emerging fintech firms in the various jurisdictions, to identify the types of products and services with higher levels of entrants and showed that, for most services, fintech firms are focused on markets at a national or regional level.

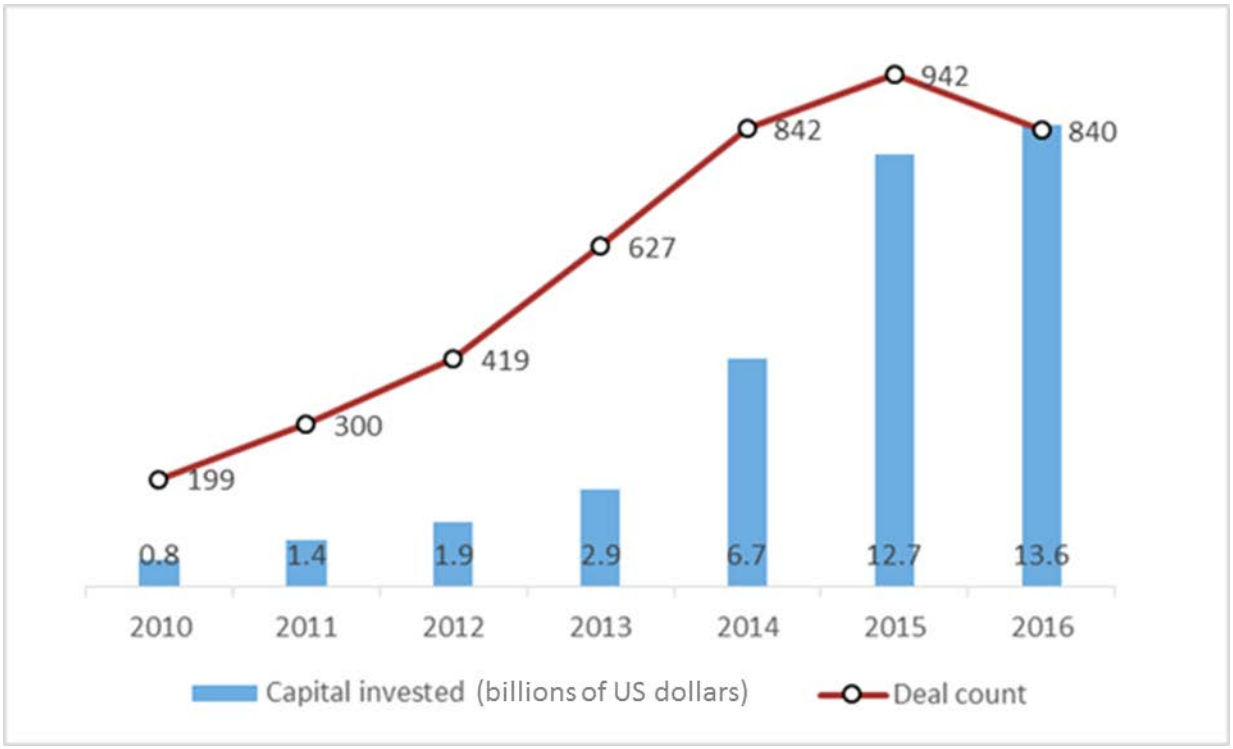
C. How big is fintech?

Quantifying the size and growth of fintech and its potential impact on the banking industry is difficult as the necessary data are often lacking, as noted above. One growth measure that can be used is venture capital (VC) investment in fintech companies. A KPMG report shows that, in 2016, global venture investment in fintech companies reached $13.6 billion across 840 deals (Graph 3). In addition to the

[5] Graph 2 is based on a survey conducted of BCBS members in mid-2016. The survey results do not represent an all-inclusive list of fintech providers. The chart shows a breakdown of prominent providers of more common fintech services within the participating BCBS jurisdictions, based on the views of BCBS members.

investment made by VC funds, many of which are backed by financial institutions, banks and other institutional investors are also making large direct investments in fintech companies.

Graph 3: Global venture investment in fintech companies 2010–16



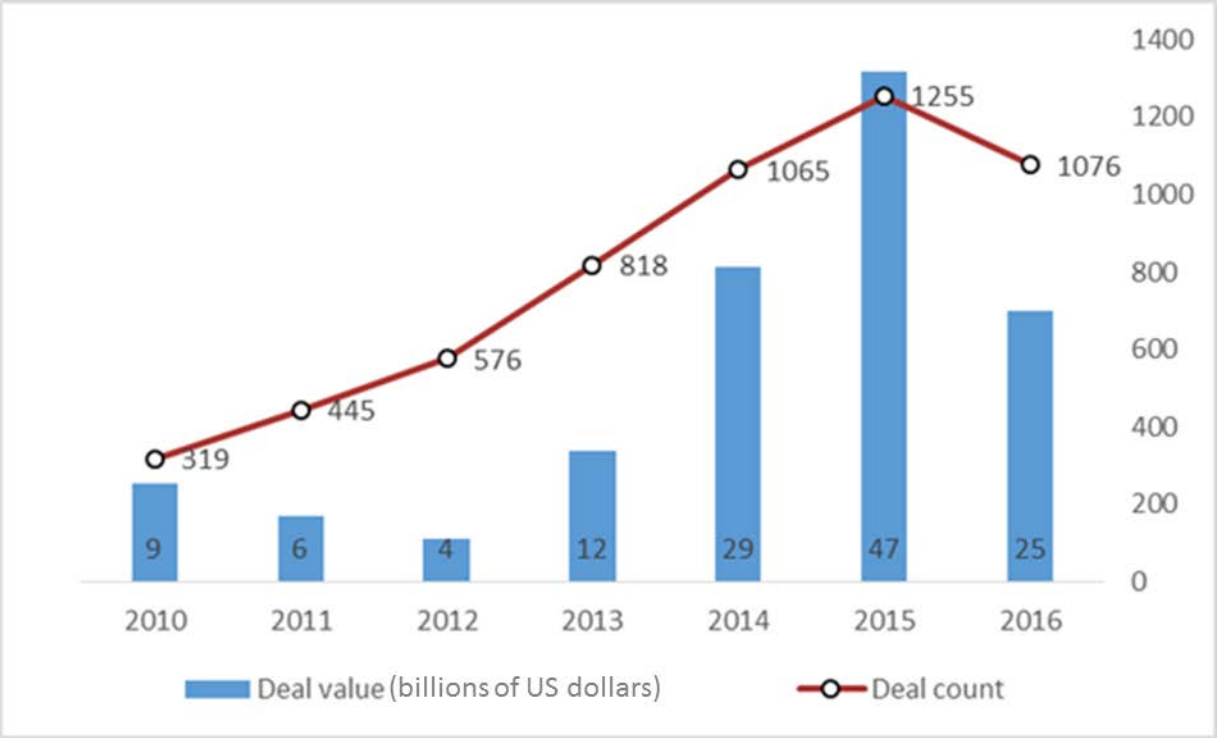
Source: KPMG International, *The Pulse of Fintech: Global Analysis of Investment in Fintech*, Fourth Quarter 2016 (data provided by PitchBook), updated February 2017.[6]

In 2016, the value of new fintech investments fell from $47 billion in 2015 to $25 billion (Graph 4). Data quoted in an IOSCO report[7] point to cumulative investments of over $100 billion in more than 8,800 fintech companies as at November 2016.

[6] See KPMG, *The Pulse of Fintech: Global Analysis of Investment in Fintech*, Fourth Quarter 2016, https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/02/pulse-of-fintech-q4-2016.pdf ; Updated figures available at: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2017/07/pulse-of-fintech-q2-2017.pdf.

[7] See IOSCO, *Research Report on Financial Technologies*, February 2017.

Graph 4. Total global investment in fintech companies 2010–16



Source: KPMG International, *The Pulse of Fintech: Global Analysis of Investment in Fintech*, Fourth Quarter 2016, (data provided by PitchBook), February 2017.

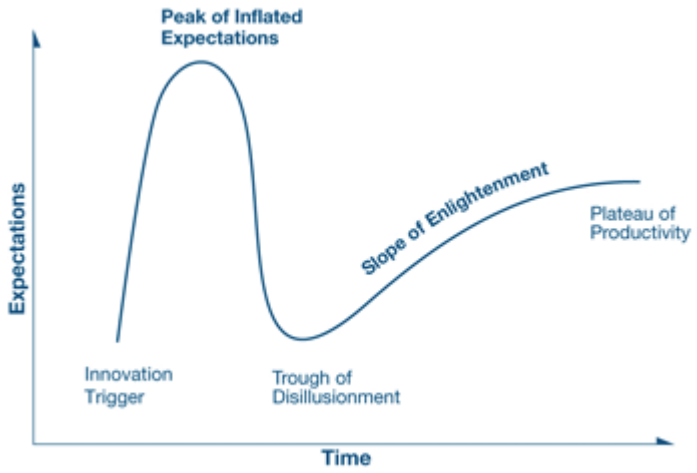
Although VC-invested capital has continued to increase, including in 2016, last year's apparent decline in volumes and total capital investment may indicate that the enthusiasm regarding fintech is reaching the initial peak of the "hype cycle". That is, there is typically a tendency to overestimate the implications of new technologies or innovations in the short term and underestimate the implications in the longer term.

Based on information available, the BCBS notes that, despite the hype, the large size of investments and the significant number of financial products and services derived from fintech innovations, volumes are currently still low relative to the size of the global financial services sector. That being said, the trend of rising investment and the potential long-term impact of fintech warrant continued focus by both banks and bank supervisors.

Box 1

The hype cycle

The hype cycle was formulated by Gartner, an IT consultancy. It represents the maturity and adoption of technologies and applications.



Innovation trigger: A potential technology breakthrough kicks off. Early proof-of-concept stories and media interest trigger significant publicity. Often no usable products exist and commercial viability is unproven.

Peak of inflated expectations: Early publicity produces a number of success stories — often accompanied by scores of failures. Some companies take action; many do not.

Trough of disillusionment: Interest wanes as experiments and implementations fail to deliver. Producers of the technology shake out or fail. Investments continue only if the surviving providers improve their products to the satisfaction of early adopters.

Slope of enlightenment: More instances of how the technology can benefit the enterprise start to crystallise and become more widely understood. Second- and third-generation products appear from technology providers. More enterprises fund pilots; conservative companies remain cautious.

Plateau of productivity: Mainstream adoption starts to take off. Criteria for assessing provider viability are more clearly defined. The technology's broad market applicability and relevance are clearly paying off.

Source: Gartner (retrieved 31 May 2017, www.gartner.com/technology/research/methodologies/hype-cycle.jsp).

D. Comparison with previous waves of innovation and factors accelerating change

As discussed, fintech firms currently represent a relatively small portion of the global banking services market. Regionally, however, some fintech companies already provide a considerable part of local banking services (eg M-Pesa in Kenya and Tanzania, and Alipay in China).[8] It remains an open question as to whether fintech firms could potentially take a significant share of more developed banking markets and thus challenge incumbent banks.

To get a better sense of current developments, fintech can be compared with previous waves of innovation, such as automated teller machines (ATMs), videotex, electronic payments, and internet

[8] The report draws on some examples from specific private firms involved in fintech. These examples are not exhaustive and do not constitute an endorsement by the BCBS or their members for any firm, product or service. Similarly, they do not imply any conclusion about the status of any product or service described under applicable law. Rather, such examples are included for purposes of illustration of new and emerging business models in the markets studied.

banking. Although not all of these innovations may have been successful, they have cumulatively changed the face of banking. Compared with the late 1960s, for instance, there are fewer branches and bank employees, larger IT budgets, longer opening hours (even 24/7), and shorter transaction times.

Technological innovations have also historically tended to follow the "hype cycle". A prime example is the internet, which went through a boom-bust cycle around the turn of the century. When the dotcom bubble burst in 2001, it seemed to blow away the promise of the internet as a major marketplace. Today, the internet has become a major platform for business, and large parts of the global population could not envisage their lives without it. Thus fintech in general may well be hyped and some innovations may already be entering the "trough of disillusionment" but, as history shows, this does not necessarily mean that fintech will have no lasting effect on the banking sector.

When assessing the recent impact of new technologies on the banking industry, two factors are especially relevant, namely (i) the adoption rate of the underlying technology in society, and (ii) the degree and pervasiveness of technological know-how within the general population. The current pace of innovation is arguably faster than in previous decades,[9] and there are clear signs that the pace of adoption has also increased. For instance, when comparing the length of time for adoption of different banking innovations, ATM adoption occurred over two decades, while internet banking and mobile banking have taken root over progressively shorter intervals. In addition, a generation of digital natives is growing up with a technological proficiency that is at the heart of fintech innovation. In fact, changing customer behaviour and demand for digital financial services are the key drivers for change. The faster pace of change means that the effects of innovation and disruption can happen more quickly than before, implying that incumbents may need to adjust faster.

E. Forward-looking scenarios

1. Background to the scenarios

To assess the impact of the evolution of fintech products and services on the banking industry, five stylised scenarios describing the potential impact of fintech on banks were identified as part of an industry-wide scenario analysis (see Graph 5).[10] It should be noted that these scenarios are not mutually exclusive and, in fact, the evolution of the banking industry will likely result in a combination of these scenarios.

In addition to the banking industry scenarios, six case studies focus on specific innovations, with three assessing enabling technologies (big data, DLT and cloud computing) and three assessing fintech business models (innovative payment services, lending platforms and neo-banks). The aim is to obtain a better understanding of the individual risks and opportunities of a specific fintech development through the different scenarios.

2. Overview of the banking scenarios

The key questions considered when developing the banking industry scenarios for the purposes of this paper were (i) which actor manages the customer relationship or interface, and (ii) which actor ultimately provides the services and takes the risk. The rise of fintech innovation has resulted in what some have dubbed the battle for the customer relationship and customer data. The outcome of this battle will be crucial in determining the future role of banks. The other key consideration surrounds potential changes in banks' business models and the different roles incumbent banks and fintech companies, including major

[9] See E Brynjolfsson and A MacAfee, *The second machine age: work, progress, and prosperity in a time of brilliant technologies*, Norton, 2014.

[10] The scenarios considered draw mainly from the following sources: Bank NXT, *The future of banking: four scenarios*, October 2015, https://banknxt.com/53478/future-banking-scenarios/; Accenture, *The future of fintech banking*, 2015, www.accenture.com/us-en/insight-future-fintech-banking; McKinsey & Co, *Cutting through the fintech noise,* December 2015, www.mckinsey.com.

technology companies ("bigtech", see Box 2), may play in either owning the customer relationship or, as service providers, supporting the processing of banking activities. The second question concerns who will be primarily responsible for what may be seen as traditional core banking services, such as lending, deposit-taking, offering payment and investment services, and managing risk. An overview of the five scenarios of the industry-wide forward-looking analyses is provided in Graph 5, while the individual scenarios are discussed in more detail in the next section.

Box 2

Bigtech

Bigtech refers to large globally active technology firms with a relative advantage in digital technology. Bigtech firms usually provide web services (search engines, social networks, e-commerce etc) to end users over the internet and/or IT platforms or they maintain infrastructure (data storage and processing capabilities) on which other companies can provide products or services.

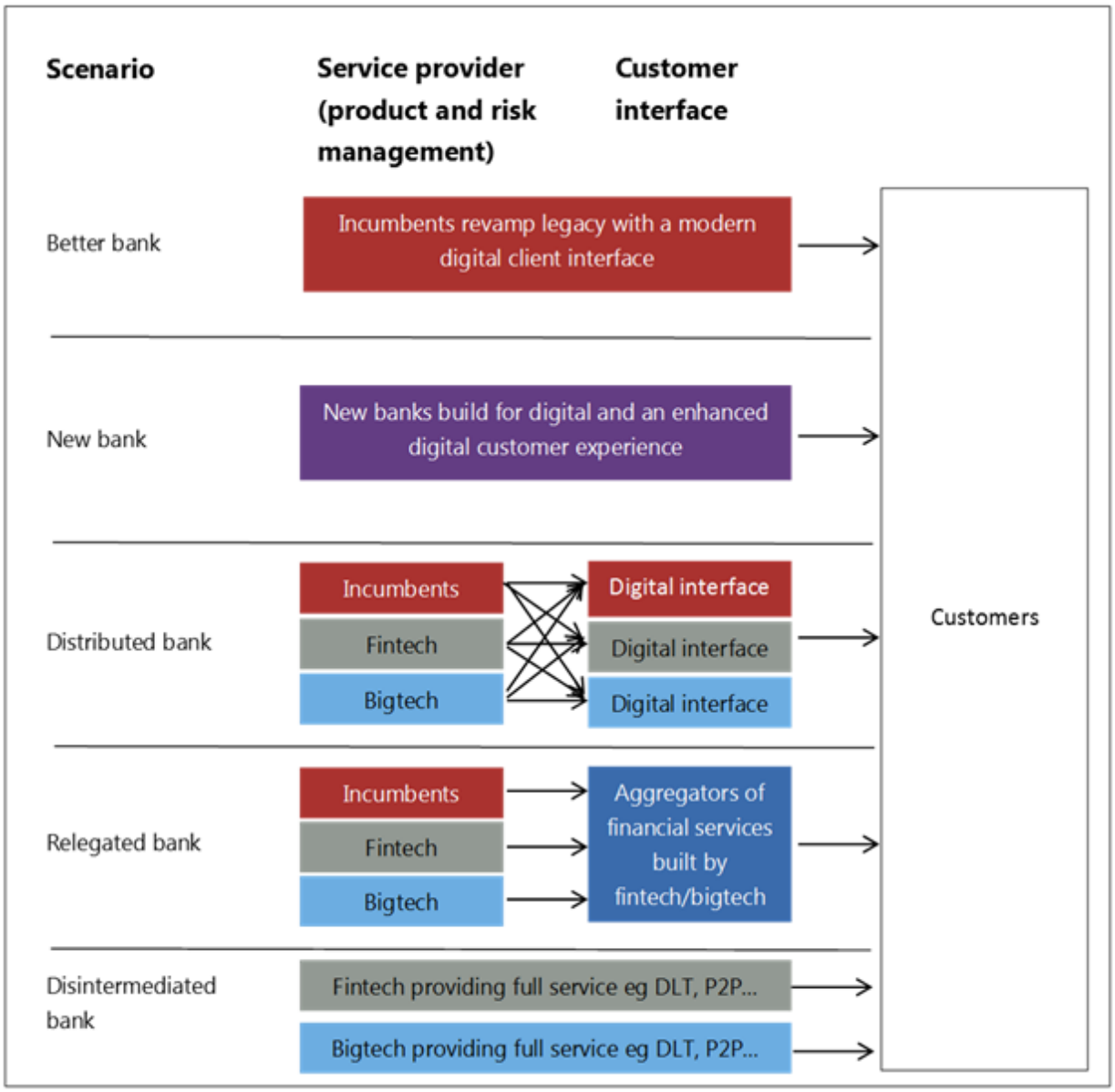
Just like fintech companies, bigtech firms typically have a highly automated operation and an agile software development process, giving them the agility to quickly adapt their systems and services to users' needs.

Bigtech firms have typically established global operations and a large customer base. They can use a vast amount of information about their customers to provide them with tailored financial services. Thus, bigtech firms may have a considerable competitive advantage over their competitors, eg incumbent banks, in the provision of financial services.

These companies can rapidly gain a significant global market share when launching a new financial product or service. Given the size of their operations and their investment capabilities, bigtech can also influence markets. Many banks, financial institutions and fintech companies are partnering with bigtech firms, which then become relevant third-party providers in the financial system. It will therefore be important to properly monitor and assess the concentration risk, given that bigtech firms could become systemically important.

Examples of bigtech firms in the western world are Google, Amazon, Facebook, and Apple, collectively known as GAFA. Similarly, BAT refers to three of the largest Chinese technology companies, namely Baidu, Alibaba and Tencent. In addition, traditional companies such as Microsoft and IBM are also tech companies relevant to the financial system and may be included in any analysis regarding bigtech.

Graph 5: Overview of the five scenarios and the role players



Colour code: maroon indicates incumbent banks; purple new players; grey fintech companies; and blue bigtech companies.
Source: BCBS illustration of scenarios based on the BankNXT study *The future of banking: four scenarios*, October 2015, https://banknxt.com/53478/future-banking-scenarios/.

3. Description of the scenarios

The better bank: modernisation and digitisation of incumbent players

In this scenario the incumbent banks digitise and modernise themselves to retain the customer relationship and core banking services, leveraging enabling technologies to change their current business models.

Incumbent banks are generally under pressure to simultaneously improve cost efficiency and the customer relationship. However, because of their market knowledge and investment capacities, a potential outcome is that the banks get better at providing services and products by adopting new technologies or improving existing ones. Enabling technologies such as cloud computing, big data, AI and DLT are being adopted or actively considered as a means of enhancing banks' current products, services and operations.

Banks use new technologies to develop value propositions that cannot be effectively provided with their current infrastructure. The same technologies and processes utilised by non-bank innovators can also be implemented by incumbent banks, and examples may include:

- New technologies such as biometry, video, chatbots or AI may help banks to create sophisticated capacities for maintaining a value-added remote customer relationship, while securing transactions and mitigating fraud and AML/CFT risks. Many innovations seek to set up convenient but secure customer identification processes.

- Innovative payment services would also support the better bank scenario. Most banks have already developed branded mobile payments services or leveraged payment services provided by third parties that integrate with bank-operated legacy platforms. Customers may believe that their bank can provide a more secure mobile payments service than do non-bank alternatives.

- Banks may also be prone to offer partially or totally automated robo-advisor services, digital wealth management tools and even add-on services for customers with the intention of maintaining a competitive position in the retail banking market, retaining customers and attracting new ones.

- Digitising the lending processes is becoming increasingly important to meet the consumer's demands regarding speed, convenience and the cost of credit decision-making. Digitisation requires more efficient interfaces, processing tools, integration with legacy systems and document management systems, as well as sophisticated customer identification and fraud prevention tools. These can be achieved by the incumbent by developing its own lending platform, purchasing an existing one, white labelling or outsourcing to third-party service providers. This scenario assumes that current lending platforms will remain niche players.

While there are early signs that incumbents have added investment in digitisation and modernisation to their strategic planning, it remains to be seen to what extent this scenario will be dominant.

The new bank: replacement of incumbents by challenger banks

In the future, according to the new bank scenario, incumbents cannot survive the wave of technology-enabled disruption and are replaced by new technology-driven banks, such as neo-banks, or banks instituted by bigtech companies, with full service "built-for-digital" banking platforms. The new banks apply advanced technology to provide banking services in a more cost-effective and innovative way. The new players obtain banking licences under existing regulatory regimes and own the customer relationship.

Neo-banks seek a foothold in the banking sector with a modernised and digitised relationship model, moving away from the branch-centred customer relationship model. Neo-banks are unencumbered by legacy infrastructure and may be able to leverage new technology at a lower cost, more rapidly and in a more modern format (see Box 3).

Elements of this scenario are reflected in the emergence of neo- and challenger banks, such as Atom Bank and Monzo Bank in the United Kingdom, Bunq in the Netherlands, WeBank in China, Simple and Varo Money in the United States, N26 in Germany, Fidor in both the United Kingdom and Germany,

and Wanap in Argentina.[11] That said, no evidence has emerged to suggest that the current group of challenger banks has gained enough traction for the new bank scenario to become predominant.

Box 3

Neo-banks

Neo-banks make extensive use of technology in order to offer retail banking services predominantly through a smartphone app and internet-based platform. This may enable the neo-bank to provide banking services at a lower cost than could incumbent banks, which may become relatively less profitable due to their higher costs. Neo-banks target individuals, entrepreneurs and small to medium-sized enterprises. They offer a range of services from current accounts and overdrafts to a more extended range of services, including current, deposit and business accounts, credit cards, financial advice and loans. They leverage scalable infrastructure through cloud providers or API-based systems to better interact through online, mobile and social media-based platforms. The earnings model is predominantly based on fees and, to a lesser extent, on interest income, together with lower operating costs and a different approach to marketing their products, as neo-banks may adopt big data technologies and advanced data analytics. Incumbent banks, on the other hand, may be impeded by the scale and complexity of their current technology and data architecture, determined by factors such as legacy systems, organisational complexity and historical acquisitions. However, the customer acquisitions costs may be high in competitive banking systems and neo-banks' revenues may be offset by their aggressive pricing strategies and their less-diverse revenue streams.

The distributed bank: fragmentation of financial services among fintech firms and banks

In the distributed bank scenario, financial services become increasingly modularised, but incumbents can carve out enough of a niche to survive. Financial services may be provided by the incumbents or other financial service providers, whether fintech or bigtech, who can "plug and play" on the digital customer interface, which itself may be owned by any of the players in the market. Large numbers of new businesses emerge to provide specialised services without attempting to be universal or integrated retail banks – focusing rather on providing specific (niche) services. These businesses may choose not to compete for ownership of the entire customer relationship. Banks and other players compete to own the customer relationship as well as to provide core banking services.

In the distributed bank scenario, banks and fintech companies operate as joint ventures, partners or other structures where delivery of services is shared across parties. So as to retain the customer, whose expectations in terms of transparency and quality have increased, banks are also more apt to offer products and services from third-party suppliers. Consumers may use multiple financial service providers instead of remaining with a single financial partner.

Elements of this scenario are playing out, as evidenced by the increasing use of open APIs in some markets. Other examples that point towards the relevance of this scenario are:

- Lending platforms partner and share with banks the marketing of credit products, as well as the approval process, funding and compliance management. Lending platforms might also acquire licences, allowing them to do business without the need to cooperate with banks.

- Innovative payment services are emerging with joint ventures between banks and fintech firms offering innovative payment services. Consortiums supported by banks are currently seeking to

[11] See for example Life-SREDA VC, *Money of the future*, p.59 *Neo challenger banks are coming*, March 2016, https://centres.insead.edu/global-private-equity-initiative/documents/MoneyOfTheFuture_2016_eng.pdf; KPMG, *A new landscape*, May 2016 https://home.kpmg.com/content/dam/kpmg/pdf/2016/05/challenger-banking-report-2016.PDF; Fintechnews, *The world's 10 neo and challenger banks in 2016*, September 2016 http://fintechnews.ch/fintech/the-worlds-top-10-neo-and-challenger-banks-in-2016/6345/.

establish mobile payments solutions as well as business cases based on DLT for enhancing transfer processes between participating banks (see Box 4 for details of mobile wallets).

- Robo-advisor or automated investment advisory services are provided by fintech firms through a bank or as part of a joint venture with a bank.

Box 4

Innovative payment services

Innovative payment services are one of the most prominent and widespread fintech developments across regions. Payments processing is a fundamental banking operation with many different operational models and players. These models and structures have evolved over time, and recent advances in technological capabilities have accelerated this evolution. Differences in types of model, technology employed, product feature and regulatory frameworks in different jurisdictions pose different risks.

The adoption by consumers and banks of mobile wallets developed by third–party technology companies – for example, Apple Pay, Samsung Pay,[12] and Android Pay – is an example of the distributed bank scenario. Whereas some banks have developed mobile wallets in-house, others offer third-party wallets, given widespread customer adoption of these formats. While the bank continues to own the financial element of the customer relationship, it cedes control over the digital wallet experience and, in some cases, must share a portion of the transaction revenue facilitated through the third-party wallets.

Innovation in payment services has resulted in both opportunities and challenges for financial institutions. Many of the technologies allow incumbents to offer new products, gain new revenue streams and improve efficiencies. These technologies also let non-bank firms compete with banks in payments markets, especially in regions where such services are open to non-bank players (eg the Payment Service Directives in the European Union and the Payment Schemes or Payment Institutions Regulation in Brazil).

The relegated bank: incumbent banks become commoditised service providers and customer relationships are owned by new intermediaries

In the relegated bank scenario, incumbent banks become commoditised service providers and cede the direct customer relationship to other financial services providers, such as fintech and bigtech companies. The fintech and bigtech companies use front-end customer platforms to offer a variety of financial services from a diverse group of providers. They use incumbent banks for their banking licences to provide core commoditised banking services such as lending, deposit-taking and other banking activities. The relegated bank may or may not keep the balance sheet risk of these activities, depending on the contractual relationship with the fintech company.

In the relegated bank scenario, big data, cloud computing and AI are fully exploited through various configurations by front-end platforms that make innovative and extensive use of connectivity and data to improve the customer experience. The operators of such platforms have more scope to compete directly with banks for ownership of the customer relationship. For example, many data aggregators allow customers to manage diverse financial accounts on a single platform. Consumers become increasingly comfortable with aggregators as the customer interface. Banks are relegated to being providers of commoditised functions such as product design, operational processes and risk management, as service providers to the platforms that manage customer relationships.

Although the relegated bank scenario may seem unlikely at first, below are some examples of a modularised financial services industry where banks are relegated to providing only specific services to another player who owns the customer relationship:

[12] See footnote 7.

- Growth of payment platforms has resulted in banks providing back office operations support in such areas as treasury and compliance functions. Fintech firms will directly engage with the customer and manage the product relationship. However, the licensed bank would still need to authenticate the customer to access funds from enrolled payment cards and accounts.

- Online lending platforms become the public-facing financial service provider and may extend the range of services provided beyond lending to become a new intermediary between customers and banks/funds/other financial institutions to intermediate all types of banking service (marketplace of financial services). Such lending platforms would organise the competition between financial institutions (bid solicitations) and protect the interests of consumers (eg by offering quality products at the lowest price). Incumbent banks would exist only to provide the operational and funding mechanisms.

- Banks become just one of many financial vehicles to which the robo-advisor directs customer investments and financial needs.

- Social media such as the instant messaging application WeChat[13] in China leverage customer data to offer its customers tailored financial products and services from third parties, including banks. The Tencent group has launched WeBank, a licensed banking platform linked to the messaging application WeChat, to offer the products and services of third parties. WeBank/WeChat focuses on the customer relationship and exploits its data innovatively, while third parties such as banks are relegated to product and risk management.

The disintermediated bank: Banks have become irrelevant as customers interact directly with individual financial services providers, for instance, using DLT

Incumbent banks are no longer a significant player in the disintermediated bank scenario, because the need for balance sheet intermediation or for a trusted third party is removed. Banks are displaced from customer financial transactions by more agile platforms and technologies, which ensure a direct matching of final consumers depending on their financial needs (borrowing, making a payment, raising capital etc).

In this scenario, customers may have a more direct say in choosing the services and the provider, rather than sourcing such services via an intermediary bank. However, they also may assume more direct responsibility in transactions, increasing the risks they are exposed to. In the realm of peer-to-peer (P2P) lending for instance, the individual customers could be deemed to be the lenders (who potentially take on credit risk) and the borrowers (who may face increased conduct risk from potentially unregulated lenders and may lack financial advice or support in case of financial distress).

At the moment, this scenario seems far-fetched, but examples of elements of the disintermediation scenario are already visible:

- P2P lending platforms become a primary source of lending activity. Such platforms manage to attract a significant number of potential retail investors so as to address all funding needs of selected credit requests. P2P lending platforms have recourse to innovative credit scoring and approval processes, which are trusted by retail investors. That said, at present, the market share of P2P lenders is small in most jurisdictions. Additionally, it is worth noting that, in many jurisdictions, P2P lending platforms have switched to, or have incorporated elements of, a more diversified marketplace lending platform business model, which relies more on the funding provided by institutional investors (including banks) and funds than on retail investors.

[13] See footnote 7.

- Cryptocurrencies, such as Bitcoin, effect value transfer and payments without the involvement of incumbent banks, using public DLT. But their widespread adoption for general transactional purposes has been constrained by a variety of factors, including price volatility, transaction anonymity – raising AML/CFT issues – and lack of scalability.

4. Actual illustration of a blend of scenarios: marketplace lending

As noted above, the scenarios presented are extremes and there will likely be degrees of realisation and blends of different scenarios across business lines. Future evolutions may likely be a combination of the different scenarios with both fintech companies and banks owning aspects of the customer relationship while at the same time providing modular financial services for back office operations.

For example, Lending Club,[14] a publicly traded US marketplace lending company, arguably exhibits elements of three of the five banking scenarios described. An incumbent bank that uses a "private label" solution based on Lending Club's platform to originate and price consumer loans for its own balance sheet could be characterised as a "distributed bank", in that the incumbent continues to own the customer relationship but shares the process and revenues with Lending Club.

Lending Club also matches some consumer loans with retail or institutional investors via a relationship with a regulated bank that does not own the customer relationship and is included in the transaction to facilitate the loan. In these transactions, the bank's role can be described as a "relegated bank" scenario. Other marketplace lenders reflect the "disintermediated" bank scenario by facilitating direct P2P lending without the involvement of a bank at any stage.

Part III – Implications for banks and banking systems

This section focuses on the risks and opportunities associated with the developments described above. Graph 6 below lists the new opportunities and risks identified for banks and the banking system based on a survey of existing publications on fintech. Traditional banking risks (such as operational or liquidity risks) are only considered to the extent that fintech developments add a new dimension or specific features to the existing ones.

[14] See footnote 7.

Graph 6: List of risks and opportunities emanating from financial technologies and innovation

	Risks	Opportunities
Impact on consumer sector	Data privacy Data security Discontinuity of banking services Inappropriate marketing practices	Financial inclusion Better and more tailored banking services Lower transaction costs and faster banking services
Impact on banks and banking system	Strategic and profitability risks Increased interconnectedness between financial parties High operational risk – systemic High operational risk – idiosyncratic Third-party/vendor management risk Compliance risk including failure to protect consumers and data protection regulation Money laundering – terrorism financing risk Liquidity risk and volatility of bank funding sources	Improved and more efficient banking processes Innovative use of data for marketing and risk management purposes Potential positive impact on financial stability due to increased competition[15] Regtech

Source: BCBS.

A. Opportunities

Many of the findings and observations in this paper are based on forward-looking scenarios and assumptions emanating from emerging financial technologies and business models.

Observation 1: *The nature and the scope of banking risks as traditionally understood may significantly change over time with the growing adoption of fintech, in the form of both new technologies and business models. While these changes may result in new risks, they can also open up new opportunities for consumers, banks, the banking system and bank supervisors***.**

Recommendation 1: Banks and bank supervisors should consider how they balance ensuring the safety and soundness of the banking system with minimising the risk of inadvertently inhibiting beneficial innovation in the financial sector. Such a balanced approach would promote the safety and soundness of banks, financial stability, consumer protection and compliance with applicable laws and regulations, including anti-money laundering and countering financing of terrorism (AML/CFT) regulations, without unnecessarily hampering beneficial innovations in financial services, including those aimed at financial inclusion.

Fintech innovations hold potential benefits for all users of financial services. These include expanding access to financial services (financial inclusion), reaching under-served consumers, reducing transaction costs, providing greater transparency with simpler products and clear cost disclosures, providing greater convenience and efficiency, and enabling tighter controls over spending and budgeting. Collectively, these can result in an enhanced customer experience by providing a better understanding of products and terms. Of note, where the risks associated with fintech vary significantly across the different

[15] See T Philippon, "The fintech opportunity", working paper, New York University, Stern School of Business, July 2016.

scenarios, the identified opportunities will depend less on particular scenarios and more on the technologies that will allow them to be realised. The most important opportunities to be kept in mind are:

- **Financial inclusion:** Digital finance has improved access to financial services by under-served groups. Technology can reach remote locations. Only six out of 10 adults have a bank account, but there are more mobile devices than people in the world.[16] The promise of digital finance to reach scale, reduce costs and, if coupled with the appropriate financial capability, broaden access is unprecedented. Financial services could be provided to more people with greater speed, accountability, and efficiency.

- **Better and more tailored banking services:** Banks are already regulated and know how to bring products to a regulated market. Fintech companies could help the banking industry improve their traditional offerings in many ways. Banks may, for example, white-label robo-advisors to help customers navigate the investment world and create a better and tailored customer experience. Partnerships with fintech companies could also increase the efficiency of incumbent businesses.

- **Lower transaction costs and faster banking services:** Innovations from fintech players may speed up transfers and payments and cut their costs. For instance, in the area of cross-border transfers, fintech companies can provide faster banking services at lower cost.

- **Potential positive impact on financial stability due to increased competition**: The entry of new players competing with incumbent banks could eventually fragment the banking services market and reduce the systemic risk associated with players of systemic size.

- **Regtech:** Fintech could be used to improve compliance processes at financial institutions. Regulation is increasing globally but the effective development and application of "regtech" (see Box 5 below) could create opportunities to, for example, automate regulatory reporting and compliance requirements as well as facilitate more cross-sectoral and cross-jurisdictional cooperation for improved compliance (eg AML/CFT).

Box 5

Regtech

Innovative technologies can help financial institutions comply with regulatory requirements and pursue regulatory objectives (prudential requirements including reporting, consumer protection, AML/CFT). In this context, regtech may provide banks with more effective ways to improve their compliance and risk management. It may also be a means of coping with change in the regulatory environment and driving down the costs involved in meeting the corresponding requirements.

Regtech could result in new processes, new distribution channels, new products or new business organisations that help banks comply with regulatory requirements and manage risk more effectively and efficiently. Some regtech firms offer compliance and risk management solutions to banks, through outsourcing or insourcing processes. Examples include the FundApps automated monitoring service for regulatory changes in the United Kingdom, and Fintellix in India, which offers data management for compliance with accounting rules.[17]

[16] World Bank, *Global financial development report*, 2014, http://siteresources.worldbank.org/EXTGLOBALFINREPORT/Resources/8816096-1361888425203/9062080-1364927957721/GFDR-2014_Complete_Report.pdf.

[17] See footnote 7.

Regtech may open up opportunities for digital transformation of control and support functions within banks (risk, compliance, legal, finance, IT).

Regtech could address a wide array of requirements related to regulatory reporting, financial crime, operational risk (including cyber-security and fraud detection), consumer protection and data protection regulation. Examples in these domains include BearingPoint's Abacus solution for compliance with the European supervisory reporting requirements, and Trulioo's and Qumran's "know your customer" solutions in Canada and Switzerland, respectively, for compliance with AML/CFT rules.[18] In Italy, anti-money laundering requirements for the opening of a new online account can be met by making a transfer from any bank account the customer holds at any other bank. All other necessary information and documents can be exchanged between the customer and the bank using e-mail, webcam, chat and other online tools.

The technologies used include IT (software, cloud computing, API, automation and AI), data technologies (big data, machine learning, risk scoring, real-time monitoring), identity technologies (biometrics, vocal recognition) or new technologies such as the DLT that combines cryptography and IT solutions.

Another potential use of regtech includes risk data reporting capabilities. During the financial crisis, firms were unable to aggregate risk data and perform analytics to aggregate risk exposures in response to events in a timely fashion. These failures influenced the BCBS's compilation of the *Principles for risk data aggregation and reporting*. Regulators have placed increased expectations on firms to be able to accurately and completely aggregate risk data, with a view to improving their risk management and also facilitating supervisory requests, such as supervisory stress testing. Use of AI, advanced data analytics and other emerging technologies could improve firms' ability to provide coherent and timely risk data.

While there are clear benefits from fintech, as noted above, innovation cannot be supported at the expense of safety and soundness, and consumer protection. Banks and bank supervisors need to maintain the same level of risk management, control standards and protections to new emerging delivery channels and services being introduced by financial institutions through fintech. However, prescriptive standards and rules, developed well before many of the technologies in use today were even considered possible, could potentially create unnecessary barriers. Banking standards and expectations should be sufficiently flexible to accommodate new innovations within the appropriate statutory authorities of jurisdictions; nonetheless, the high standards for safety and soundness and consumer protection objectives required in the banking industry need to be maintained.

B. Key risks

Observation 2: *For banks, the key risks associated with the emergence of fintech include strategic risk, operational risk, cyber-risk and compliance risk. These risks were identified for both incumbent banks and new fintech entrants into the financial industry.*

Recommendation 2: Banks should ensure that they have effective governance structures and risk management processes in order to identify, manage and monitor risks associated with the use of enabling technologies and the emergence of new business models and entrants into the banking system brought about by fintech developments. These structures and processes should include:

- **robust strategic and business planning processes that allow banks to adapt revenue and profitability plans in view of the potential impact of new technologies and market entrants;**

[18] See footnote 7.

- **sound new product approval and change management processes to appropriately address changes not only in technology, but also in business processes;**
- **implementation of the Basel Committee's *Principles for sound management of operational risk* (PSMOR) with due consideration to fintech developments;[19] and**
- **monitoring and reviewing of compliance with applicable regulatory requirements, including those related to consumer protection, data protection and AML/CFT when introducing new products, services or channels.**

The rise of fintech will likely lead to more competition for banks from non-traditional players in an already challenging market environment, which could impact the sustainability of banks' earnings. It also puts pressure on banks to improve digital interfaces to better meet customer expectations. Incumbent banks may find it increasingly difficult to respond quickly and competitively to emerging technologies so as to keep control of customer relationships. The proliferation of innovative products and services may increase operational complexity and risks.

Many of the challenges outlined above are consistent with risk issues outlined in the existing PSMOR. Below are applicable interpretations of the PSMOR in relation to current and future fintech developments, for the reference of both incumbent and new banks, as well as their third-party service providers.

Graph 7: Practical instances of PSMOR applied to fintech

	PSMOR	Practical implementation for fintech developments
Fundamental principles of operational risk management		
1	Ensuring a strong risk culture	Ensuring integrated risk culture shared throughout the supply chain.
2	Risk management framework	Capturing fintech-driven new risks and risk profile changes.
Governance		
3	Effectively implementing risk policies, processes and systems	Building up framework to capture and control fintech-driven new risks.
4	Setting and reviewing risk appetite and risk tolerance	Setting appropriate risk appetite and tolerance with effective thresholds to trigger prompt remedial action.
5	Implementing the policies, processes and systems to control risks	Ensuring prompt reporting, assessment and early risk mitigation for fintech-driven risks.
Risk management environment		
6	Identifying/assessing risks in all processes and systems	Enhancing capacity to identify, assess and mitigate risks arising from extended processes and systems in fintech migrations.
7	Assessing risks in the launch of every product, activity, process and system	Ensuring the timely and overarching identification, assessment of risks in the launch and delivery of fintech-driven processes and systems.
8	Appropriate risk monitoring and proactive risk management	Updating the frequency of monitoring and reporting with appropriate escalation according to the size and nature of the risks.
9	Strong risk control environment	Affording appropriate capacities and resources allocated to promptly and effectively control fintech-driven risks.
Business resiliency and continuity		
10	Business resiliency and continuity plans for severe business disruption	Incorporating business continuity and disaster recovery plan with business disruption scenarios in fintech-driven processes and systems.
Role of disclosure		
11	Public disclosure of risk management	—

[19] In June 2011, the BCBS published its *Principles for the sound management of operational risk* to provide guidance to banks on the management of operational risk, www.bis.org/publ/bcbs195.htm.

Source: BCBS.

Overview of risks using scenarios analysis

The BCBS used the five banking scenarios described in Part II.E and case studies to obtain a better understanding and overview of the individual risks, their likelihood under each scenario and their impact on individual banks, the financial sector, and consumers and society more broadly.

Graph 8: Description of key risks per scenario

Better bank	The key risks under the better bank scenario focus on the execution risk related to the implementation of the new strategy (banks' ability to manage and effectively implement both the technology and business process changes) and the strategic and profitability risks. Even in the better bank scenario, there is likely to be tough competition among incumbent players to select the winning strategy and the right time to market. While some aspects of operational risk management may benefit from improved and more efficient banking processes, operational risk may increase because of the further development of cyber-risks and increased reliance on outsourcing. Indeed, the incumbent banks, which still carry legacy technologies and premises, are likely to accelerate the transition from legacy environments to new digital platforms. The new digitised environment may carry cyber-security risk in its various forms. This scenario also raises issues about the supervisory authorities' ability to effectively supervise the new technologies and products (see Part IV).
New bank	The size and scale of many incumbent banks may make it difficult to effectively modernise and digitise their current processes to achieve cost-effective operations as well as to provide innovative products for customers within an acceptable timeframe. If neo-banks were to gain significant scale, the combination of customer drain to challenger banks, lower profitability on reduced revenues, and investors moving funds to more profitable challenger banks could raise safety and soundness issues for incumbent banks.
Distributed bank	The key risks highlighted in most of the case studies for the distributed bank scenario focus on banks' and bank supervisors' ability to monitor and manage end-to-end transactions across one or multiple third parties. Effective third-party risk management processes would be essential for banks. Whether fintech companies are service providers, business partners or provide the primary customer interface, banks will need processes in place to conduct appropriate due diligence, contract management and ongoing control assurance and monitoring of outsourced services operations in order to safeguard themselves and their customers. Also, questions on ownership of the customer relationship and the use of customer data with regard to consumer protection and data protection regulations were raised as part of the distributed bank scenario. Finally, there might be questions about risk management functions as a consequence of weaker, less stable and more fragmented customer relationships. The loss of the customer relationship can result in loss of revenue and cross-selling opportunities. Also, on the compliance side, banks will need to have appropriate AML/CFT monitoring processes in place if they process transactions on behalf of fintech companies' customers. From a financial stability perspective, the distributed bank scenario may reduce the "too big to fail" issue, since increased competition and a sharing of the value chain is likely to lead to a more fragmented banking sector. On the other hand, the distributed bank scenario is associated with increased interconnectedness between financial institutions and the dilution of accountability.

Relegated bank	In this scenario, banks become a back office service provider for front office customer-facing platforms, with banks providing the necessary licences, access to payment networks and maintaining deposits and access to funding. There is a risk that banks and bank supervisors will have limited ability to monitor end-to-end transactions and systemic risk. As in the distributed bank scenario, the loss of the customer relationship and the dependence on these new platforms that channel financial products may have adverse consequences for risk management functions and revenue streams (revenues would need to be shared with the new intermediaries). Front office customer platforms are also expected to accentuate competition between banks, which may further accelerate customer mobility, deposit transfer speeds and aggressive pricing on loan offers. This scenario raises also significant issues for consumer protection, since the customer relationship will be handled by new platforms, which would be based on automated processes and extensive and innovative uses of consumer data. In addition to data privacy and data security issues, inappropriate marketing practices could emerge under this scenario. If the number of new platforms is low, concentration risk will increase, especially if bigtech firms gain a large market share. This would also lead to "too-big-to-fail" issues.
Disintermediated bank	The disintermediated bank scenario is considered unlikely to gain significant scale in the short to medium term. Indeed, large-scale use of public distributed ledgers for processing payments is still impeded by many technological and legal factors. P2P lending platforms also face difficulties in matching lending and borrowing, which underlines the continuing economic need for balance sheet intermediation. Moreover, P2P lending platforms are currently pivoting to a business model where institutional investors such as banks, pension funds or insurance companies progressively replace retail investors in the investor base. However, these scenarios were covered as there is a potential risk that banks could be disintermediated from certain aspects of financial services. The key risk in these scenarios would be that financial activities taking place outside regulatory environments would be subject to looser standards and oversight, and as a result be inherently less controlled and secure. Bank supervisors could potentially find that their ability to monitor systemic areas of risk in the financial industry is eroded.

Source: BCBS.

Fintech presents a wide variety of risks that cut across various sectors and often blend both tactical and strategic risk elements. A number of these risks feature more or less prominently in all five scenarios:

- **Strategic risk:** The potential for rapid unbundling of bank services to non-bank fintech or bigtech firms increases risks to profitability at individual banks. Existing financial institutions stand to lose a substantial part of their market share or profit margin if new entrants are able to use innovation more efficiently and deliver less expensive services that better meet customer expectations. In today's environment, a disruptive deterioration of profitability due to the loss of profitable direct customer relationships and/or margin compression might weaken the ability of incumbent institutions to weather future business cycles, for example, if banks react to falling profits by engaging in riskier activities, such as moving down the credit spectrum.

- **High operational risk – systemic dimension:** The rise of fintech leads to more IT interdependencies between market players (banks, fintech and others) and market infrastructures, which could cause an IT risk event to escalate into a systemic crisis, particularly where services are concentrated in one or a few dominant players. The entrance of fintech firms to the banking industry increases the complexity of the system and introduces new players which may have limited expertise and experience in managing IT risks.

- **High operational risk – idiosyncratic dimension:** A proliferation of innovative products and services may increase the complexity of financial services delivery, making it more difficult to manage and control operational risk. Legacy bank IT systems may not be sufficiently adaptable or implementation practices, such as change management, may be inadequate. As such, banks

are using greater numbers of third parties, either through outsourcing (eg cloud computing) or other fintech partnerships, thereby increasing complexity and reducing the transparency of end-to-end operations. This increased use of third parties may increase risks surrounding data security, privacy, money laundering, cyber-crime and customer protection. This is particularly the case if banks are less efficient in applying the required standards and controls to manage those risks, or where fintech firms may not be subject to the same stringent security standards.

- **Increased difficulties in meeting compliance requirements and especially AML/CFT obligations:** The risk of loss of the customer relationship can result in loss of revenues and cross-selling opportunities. Also, on the compliance side, banks will need appropriate AML/CFT monitoring processes in place if they process transactions on behalf of fintech companies' customers. If the customer makes payments with a bank card or account, the bank currently has some level of responsibility for authenticating the customer and may be responsible for covering fraudulent transactions under several regulatory regimes. The higher level of automation and distribution of the product or service among banks and fintech companies can result in less transparency on how transactions are executed and who has compliance responsibilities. This can increase conduct risk for banks as they may be held accountable for the actions of fintech partners if a customer suffers loss or compliance requirements are not met (see Box 6 below for further details).

- **Compliance risk with regard to data privacy:** The risk of not complying with data privacy rules may increase with the development of big data, more outsourcing due to tie-ups with fintech firms, and the associated competition for ownership of the customer relationship.

- **Outsourcing risk:** If more parties are involved in the offering of financial products and services than at present (distributed bank, relegated bank, disintermediated bank), ambiguity could arise regarding the responsibilities of the various actors in the value chain, potentially increasing the likelihood of operational incidents. Within banks, a proliferation of innovative products and services from third parties could increase operational complexity and risks, if controls fail to keep pace. A key challenge for financial institutions will lie in their ability to monitor operations and risk management activities that take place outside their organisations at third parties. Outsourcing risk would be even more prominent if some part of the services provided by third parties were to become dominated by globally active players, resulting in a concentration of risk. Where fintech companies are the service providers, business partners or provide the primary customer interface, banks will need processes in place to conduct appropriate due diligence, contract management and ongoing control assurance and monitoring of operations in order to safeguard the bank and its customers.

- **Cyber-risk:** Cyber-risk is likely to rise in all scenarios. New technologies and business models can increase cyber-risk if controls do not keep pace with change. Increased interconnectivity between market players can create benefits for banks and consumers, while amplifying security risks. Heavier reliance on APIs, cloud computing and other new technologies facilitating increased interconnectivity could potentially make the banking system more vulnerable to cyber-threats, and expose large volumes of sensitive data to potential breaches. This emphasises the need for banks, fintech firms and supervisors to promote the need for effective management and control of cyber-risk.

- **Liquidity risk and volatility of bank funding sources:** The use of new technology and aggregators creates opportunities for customers to automatically change between different savings accounts or mutual funds to obtain a better return. While this can increase efficiency, it can also affect customer loyalty and increase the volatility of deposits. This in turn could lead to higher liquidity risk for banks.

Box 6

Risks and opportunities of fintech for anti-money laundering and countering the financing of terrorism (AML/CFT)

Increased risk: Digital finance raises news risks and challenges with regard to AML/CFT. New areas of vulnerability might develop because of new financial products (virtual cryptocurrencies) and new technologies (eg a permissionless distributed ledger based on anonymous users and on decentralised governance without accountability). Digital finance gives rise to an increasing number of financial players and eases cross-border transactions, which makes the monitoring of transactions more complex for financial institutions and public authorities. Finally, while new financial players are reshaping the financial sector, they may be outside the scope of banking sector regulation and subject to less stringent AML/CFT rules than are banks. If not proportionate to the AML/CFT risks, these regulatory gaps or loopholes may lead to some distortion of competition, which may violate the level playing field principle and lead to increased potential for financial crime.

Innovative solutions: New technologies may support greater efficiency for AML/CFT policy. Regtech companies are especially keen to enter this field, which could attract significant investment by banks. Analytics of non-structured data (big data) associated with machine learning and AI can support banks' financial crime divisions in the monitoring and reporting of suspicious transactions. While non-face-to-face relationships are usually considered as a "high risk" for AML/CFT, requiring enhanced due diligence (see Financial Action Task Force's 2012 report on money laundering),[20] technologies such as biometry (eg fingerprints, iris or vocal recognition, touch ID etc), and scanning technologies may also help identify fraud in a digital environment and promote remote but secure customer identification and authentication processes. E-identification and e-signatures may provide new secure opportunities to facilitate the digital on-boarding of customers and non-face-to-face business relationships.

Initiatives in a number of countries involving the use of innovative technologies for identification services are in different stages of development. For example, the UK government is promoting e-identification through its Verify programme,[21] to which banks such as Barclays contribute by certifying the identity of their customers. In Canada, SecureKey,[22] a private sector company that includes a number of banks as investors, proposes to use a third-party blockchain as an identity and authentication provider to simplify consumer access to online services and applications.

Similarly in the Netherlands, a service called IDIN,[23] supported by seven Dutch banks, was launched in 2016 to enable customers to identify themselves to other organisations online using bank authentication credentials.

Both the UK and Canadian initiatives are supported, to some degree, by governments. In these identity "ecosystems", banks may provide identity information, subject to customer consent, as well as receive it.

Some regtech providers and countries would like to set up shared KYC utilities for due diligence using cloud and online platforms. The BCBS acknowledges such utilities for conducting customer due diligence in its revised guidelines on the sound management of risks related to money laundering and financing of terrorism.[24] However, jurisdictions may follow different approaches in promoting innovative business models and emerging technologies, while mitigating and addressing associated money laundering and terrorist financing risks.

C. Implications of using innovative enabling technologies

Observation 3: *Banks, service providers and fintech firms are increasingly adopting and leveraging advanced technologies to deliver innovative financial products and services. These enabling technologies, such as*

[20] Financial Action Task Force, *International standards on combating money laundering and the financing of terrorism & proliferation*, 2012, www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.

[21] See https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify.

[22] See http://securekey.com/.

[23] See www.idin.nl/.

[24] See BCBS, *Revisions to the annex on correspondent banking*, June 2017, www.bis.org/bcbs/publ/d405.htm.

artificial intelligence (AI)/machine learning (ML)/advanced data analytics, distributed ledger technology (DLT), cloud computing and application programming interfaces (APIs), present opportunities, but also pose their own inherent risks.

Recommendation 3: Banks should ensure they have effective IT and other risk management processes that address the risks of the new technologies and implement the effective control environments needed to properly support key innovations.

As part of the BCBS's research for this paper, three fintech-enabling technologies, namely AI/machine learning (ML)/advanced data analytics, DLT and cloud computing, were studied in detail to assess the impact that their development may potentially have on the banking industry. These enabling technologies are not new financial products or services themselves, but instead are the catalyst that allows for the development of new innovative products and for fintech companies to enter the banking markets. These technologies may lower barriers for entrants by allowing for low-cost infrastructure and access to direct delivery channels to customers, thus bypassing traditional channels.

1. Artificial intelligence /machine learning /advanced data analytics

AI makes possible advanced analytical tools that, by leveraging the capability to process large volumes of data, support innovative solutions for business needs. This capability enables the development of multichannel customer access, increased self-service by customers, ability to gain greater insight into customer needs and the provision of more tailored or customised services. There is an increasing use of AI/ML for the termination of credit limits, although the accuracy and validity of these models is as yet unproven. Many fintech companies have leveraged these capabilities to provide data collection, aggregation and storage services, advanced data analytics and personal finance management directly to customers. In modernising and digitising incumbent banks, most of these services support a better bank scenario where banks use advanced data analytics to research customer needs, provide real-time service delivery and enhance their risk management. Fintech companies based on data aggregation business models, or bigtech companies, utilise customer data to gain an in-depth knowledge of their users (through search history, personal data and preferences shared on social media, consumption and spending habits etc) and tend to compete directly with banks for ownership of the customer relationship (the distributed, relegated and disintermediated bank scenarios). Many data aggregators provide customers with the opportunity to manage diverse financial accounts on a single platform with limited need for direct contact with multiple financial service providers.

The answers to questions such as who owns customer data, the conditions under which personal data can be used, and for what purposes, will likely shape developments in advanced data analytics and big data. These legal questions are being debated in several jurisdictions.[25]

2. Distributed ledger technology

As an emerging technology, DLT solutions tend to be more complex than other enabling technologies and have the potential to be applied for multiple purposes.

DLT is being considered for a large number of use cases. Some DLT developments focus on facilitating value transfer exchanges between parties without the need for intermediation, such as central counterparties and central securities depositories, while others target the efficiency of the intermediary functions, without challenging the role of intermediaries, by reducing settlement times or improving the transparency of recordkeeping and reporting. Some DLT solutions also focus on banks' back office operations. Current DLT solutions can be used to enable better automation, specifically through the use of smart contracts. Thus, better information-sharing via DLT could also benefit banks' business processes.

[25] See for example the European Union's Global Data Protection Regulation that will enter into force in 2018.

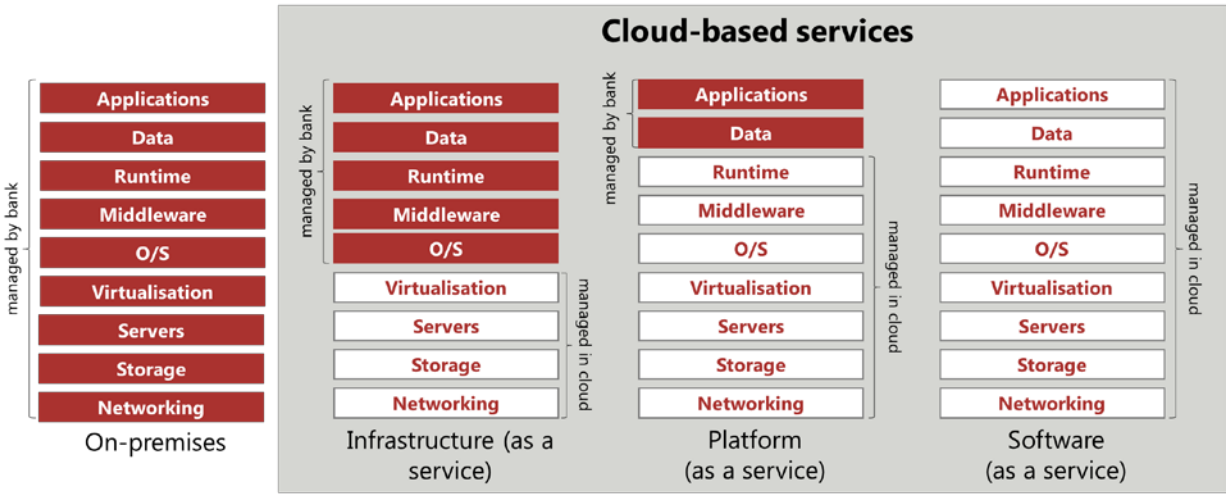
Depending on the DLT solution, other benefits could include eliminating data duplication and reducing maintenance costs to support different databases.

DLT developments, although still heterogeneous and immature, could trigger concerns as some solutions still display limited scalability, and a lack of data privacy or harmonised industry standards, with little in the way of interoperability and recourse mechanisms. Exploratory investments are being made by financial institutions, with some projects achieving limited internal deployment for intragroup purposes with the aim of improving services. Examples of DLT platforms moving into testing or production include platforms for trade finance, syndicated loans, repo clearing, and derivatives recordkeeping and processing.

3. Cloud computing

Cloud computing allows the sharing of on-demand computer processing resources in a way that promotes efficiencies and economies of scale. Such cost-cutting is attractive for banks, but concerns over safety and privacy initially inhibited banks from using cloud computing infrastructure. Now, however, many banks are experimenting with public cloud operations.[26] For fintech companies, cloud solutions often allow easier access to back office infrastructure that incumbents spent decades building, helping to engage in operations at a lower cost. Cloud-based services can take many forms, ranging from infrastructure only to fully fledged software solutions (including white-labelled banking solutions), as shown in Graph 9 below.[27] While responsibility for managing cloud operations (see Graph 9) would be located variously in each of the different scenarios depicted, banks continue to retain risk management and oversight responsibilities for all their activities, including those outsourced.

Graph 9: Range of usage of cloud-based services



Source: Technet.

Cloud computing as a service provider to banks can act as an enabler in all fintech-related scenarios, and need not in itself cause business models to be disrupted. However, while cloud computing helps both incumbent banks and new players, it is more of an enabler for new players and therefore fits scenarios that challenge the current banking system (all scenarios apart from the better bank). Incumbent banks can use cloud computing to develop new solutions and migrate away from legacy systems. In doing so they face the challenge of integrating the new technology with the old, which is usually not an easy task. For new players, on the other hand, cloud computing is a pure enabler as they would have traditionally had to invest time and money in building up their own infrastructure. The use of cloud computing therefore allows them to focus on their business and increase their scale as the business grows.

[26] C Boulton, "Why banks are finally cashing in on the public cloud", *CIO magazine*, 10 May 2016.

[27] On the infrastructure side, bigtech firms are already dominant providers of cloud services worldwide. Banks and banksupervisors are currently dealing with the global bigtech firms on a national level, and in different ways.

Banks' dependency on technologically complex systems could increase significantly, including the use of cloud-based services and infrastructure (all scenarios), requiring an enhanced technological expertise to understand and supervise effectively. In cases where banks outsource important parts of their operational processes, especially in the case of internationally active players, further attention to the supervision of these processes could be warranted as well.

D. Focus on outsourcing and partnering risk

Observation 4: *Banks are increasingly partnering with and/or outsourcing operational support for technology-based financial services to third-party service providers, including fintech firms, causing the delivery of financial services to become more modular and commoditised. While these partnerships can arise for a multitude of reasons, outsourcing typically occurs for reasons of cost-reduction, operational flexibility and/or increased security and operational resilience. While operations can be outsourced, the associated risks and liabilities for those operations and delivery of the financial services remain with the banks*.

Recommendation 4: Banks should ensure they have appropriate processes for due diligence, risk management and ongoing monitoring of any operation outsourced to a third party, including fintech firms. Contracts should outline the responsibilities of each party, agreed service levels and audit rights. Banks should maintain controls for outsourced services to the same standard as the operations conducted within the bank itself.

The rise of fintech is expected to continue to increase operational risks as the banking industry becomes more complex. The financial sector is becoming more modular, both at the front end with fintech firms partnering with banks (via for instance APIs), and in back offices and supporting functions where more IT infrastructure and services are outsourced to globally active bigtech firms and start-ups. While in certain cases these developments could increase security, these new business models and their supporting technologies could also potentially increase operational complexity and risk.

The key areas of interest that emerge in most – if not all – of these scenarios are:

- When engaging a service provider or fintech partner, banks and new entrants should consider the Basel principles addressing operational risk and outsourcing risk, such as the Basel Committee's *Core principles for banking supervision* (2012), the PSMOR (2011)[28] and the guiding principles established by the Joint Forum about *Outsourcing in financial services* (2005). Some of the principles address corporate governance frameworks in general, which is relevant not only for incumbent banks but also for new entrants including non-financial ones. Others addressing risk culture and risk appetite/tolerance are applicable to all financial services firms. However, it is uncertain whether emerging fintech players will adhere to these principles. The larger the gap of "risk culture" and "risk tolerance" among entities participating in the financial system, the more likely it is that weaknesses will develop in the operational risk control framework.

- The risk management culture must also extend its reach to third parties performing operational activities on behalf of the bank, particularly those supporting fintech technologies or dependent products.

- The operational risk framework is expected to be able to identify emerging risks and to enable a timely response to any developments that materially change existing operational risks, or introduce new risks.

[28] See Graph 7 and footnote 19.

- Periodic reviews of the framework should also assess whether risk functions are capable of maintaining effective oversight of the emerging risks posed by new technologies, which may require specialist competencies to address.

- Business impact assessments should take account of relevant business disruption scenarios, which should then be reflected in the firm's business continuity and disaster recovery plans, and incident management procedures.

From the point of view of banking supervision, the use of third-party service providers poses operational risks that need to be specifically addressed. At the same time, there are concerns that direct regulation of this sector could hinder the growth of innovative models.

Part IV – Implications for bank supervisors and regulatory frameworks

A. Increased need for cooperation

Observation 5: *Fintech developments are expected to raise issues that go beyond the scope of prudential supervision, as other public policy objectives may also be at stake, such as safeguarding data privacy, data and IT security, consumer protection, fostering competition and compliance with AML/CFT*.

Recommendation 5: Bank supervisors should cooperate with other public authorities responsible for oversight of regulatory functions related to fintech, such as conduct authorities, data protection authorities, competition authorities and financial intelligence units, with the objective of, where appropriate, developing standards and regulatory oversight of the provision of banking services, whether or not the service is provided by a bank or fintech firms.

In several jurisdictions, some of the risks associated with the emergence of fintech, such as compliance with data privacy, data security, and AML/CFT standards, fall under the remit of public authorities separate from bank supervisors but still affect compliance risk for banks. Therefore cross-sectoral cooperation across regulatory agencies may be warranted within certain jurisdictions to address risks that concern prudential supervision, but which may overlap with the mandates of other agencies. This coordination may provide more consistent and effective supervision related to areas such as consumer protection, data protection, competition and cyber-security.

Observation 6: *While many fintech firms and their products – in particular, businesses focused on lending and investing activities – are currently focused at the national or regional level, some fintech firms already operate in multiple jurisdictions, especially in the payments and cross-border remittance businesses. The potential for these firms to expand their cross-border operations is high, especially in the area of wholesale payments*.

Recommendation 6: Given the current and potential global growth of fintech companies, international cooperation between supervisors is essential. Supervisors should coordinate supervisory activities for cross-border fintech operations, where appropriate.

Existing fintech companies are developing mainly within individual jurisdictions. If some services are provided across borders (by relegated, disintermediated, or new banks), this would increase the need for coordination and cooperation, both between jurisdictions as well as across sectors. This increases the need for more international coordination and cooperation between bank supervisors, in particular on the regulatory treatment of cross-border tech companies. Bank supervisors are increasingly engaging with these companies, but often on a national level and using different approaches. Given the international expansion of these companies, increased international cooperation may be beneficial for all parties. The

scale of international cooperation between supervisory agencies should keep up with the pace of globalisation of these companies.

B. Bank supervisors' internal organisation and human resources policies

Observation 7: *Fintech has the potential to change traditional banking business models, structures and operations. As the delivery of financial services becomes increasingly technology-driven, reassessment of current supervision models in response to these changes could help bank supervisors adapt to fintech-related developments and ensure continued effective oversight and supervision of the banking system*.

Recommendation 7: Bank supervisors should assess their current staffing and training models to ensure that knowledge, skills and tools of their staff remain relevant and effective in supervising new technologies and innovative business models. Supervisors should also consider whether additional specialised skills are needed to complement existing expertise.

The financial industry is undergoing rapid technological changes in all scenarios considered. Bank supervisors will need to continuously re-evaluate necessary skill-sets and approaches to supervision to keep up with changes in the banking industry.

Based on surveys and interviews, prudential supervisors have generally relied on existing divisions, risk specialists and internal working groups to identify, monitor and assess fintech-related risks. However, some agencies have set up standalone units with dedicated resourcing and reporting lines in response to fintech issues. The mandates of these units are wide-ranging and include functions such as policy and research, licensing, public-facing contact points, supervision or the use of emerging supervisory technology ("suptech"). While most groups were staffed with approximately five full-time equivalents, a small number of units were allocated up to 10 and, in one instance, 20 full-time equivalents. It is important to note, however, that many of these units are still at a nascent stage and resource allocations may evolve based on a variety of factors.

Fintech education/training is a key area of focus for most agencies. Most agencies noted that fintech-related modules had been included in recent training activities. Participants noted attending, participating in, and hosting conferences as ways to gather intelligence and build networks. A number of agencies noted frequent meetings with fintech entrants and technology companies. Two agencies have formal fintech training and/or lecture programmes currently in place.

It was observed that, while many supervisors have instituted training programmes, only a few are reviewing the adequacy of their human resources policies, including hiring profiles, or engaging in direct experimentation (eg with DLT or other network-based technologies) to advance regulatory understanding of technological innovations. With regard to specific fintech developments, many agencies noted that their current recruitment programmes for IT risk supervision already emphasise technical skills and knowledge. A number of agencies with central banking mandates noted adding resources in the area of payments infrastructure and/or DLT.

Fintech business models can broadly impact operational processes and strategies, as well as IT processes. As a result, supervisors may want to review the adequacy of their human resources policies, including hiring profiles and training programmes, to ensure appropriate responsiveness to developments in financial technology.

C. Suptech opportunities

Observation 8: *The same technologies that offer efficiencies and opportunities for fintech firms and banks, such as AI/ML/advanced data analytics, DLT, cloud computing and APIs, may also improve supervisory efficiency and effectiveness*.

Recommendation 8: Supervisors should consider investigating and exploring the potential of new technologies to improve their methods and processes. Information on policies and practices should be shared among supervisors.

Based on survey results, respondents' involvement with suptech is nascent and difficult to compare given their state of development. Suptech lets supervisors conduct supervisory work and oversight more effectively and efficiently. This differs from regtech, as suptech is not focused on assisting with compliance with laws and regulations, but on supporting supervisory agencies in their assessment of that compliance.

The benefits of suptech may include increased efficiency and effectiveness, including (near) real-time data access. However, barriers to implementation may include standardised internal or government-wide policies around IT procurement, restrictions on cross-border data movement, and a lack of transparency as to how the new technology works and is being controlled (eg AI).

A small number of agencies are currently exploring the feasibility of using innovative technologies such as AI/ML and distributed ledgers to enhance existing supervisory functions. As with other industries/sectors, big data holds the promise of expanding supervisors' capacity by providing insights into large amounts of unstructured data. This functionality could be used to support financial institution risk assessments, monitoring/review exercises, or enhancements to regulatory guidance. DLT-based markets and reporting systems could potentially allow supervisors to monitor exposures and transactions of market participants in real time as "nodes" on the network which, if combined with AI capabilities, could further enhance supervisory functions.

For instance, one integrated supervisor recently used natural language-processing AI to analyse visit reports from pension funds in order to highlight paragraphs containing potentially sensitive information. The same institution is also running an experiment in which a third-party AI solution is used to analyse banks' annual reports. Some agencies are also using "accelerator" or "hackathon"[29] models to work with fintech companies to address supervisory challenges. For instance, one supervisor's website disclosed summarised information regarding a proof of concept conducted with a partner specialising in AI/ML in which AI tools were used to detect anomalies in supervisory data. In addition to developing specific suptech applications, these initiatives may have benefits such as building a network of firms to draw on in the future, applying the lessons learned to other supervisory areas (eg cyber-security), and supporting start-ups.

D. Continued relevance of regulatory frameworks

Observation 9: *Current bank regulatory, supervisory and licensing frameworks generally predate the technologies and new business models of fintech firms. This may create the risk of unintended regulatory gaps when new business models move critical banking activities outside regulated environments or, conversely, result in unintended barriers to entry for new business models and entrants*.

Recommendation 9: Supervisors should review their current regulatory, supervisory and licensing frameworks in light of new and evolving risks arising from innovative products and business models. Within applicable statutory authorities and jurisdictions, supervisors should consider whether these frameworks are sufficiently proportionate and adaptive to appropriately balance ensuring safety and soundness and consumer protection expectations with mitigating the risk of inadvertently raising barriers to entry for new firms or new business models.

[29] A "hackathon", combining the words "hacker" and "marathon", is a collaborative computer programming event typically lasting several days.

1. Supervision of third-party service providers

An example of differences in supervisory frameworks is the oversight of third-party service providers. While many fintech firms offer financial services directly to their customers, many others partner or act as third-party service providers to banks. Use of fintech firms as third-party service providers can provide financial institutions with access to products, technical expertise and efficiencies from economies of scale that they may not have if the service were developed in-house. While access to third-party services can benefit financial institutions and provide their customers with access to a wider array of financial products, the operational, security, reputational and other risks remain with the financial institution. As such, financial institutions are expected to have sound due diligence, risk management and ongoing oversight programmes in place for the engagement and use of service providers. Third parties that provide critical services to large numbers of financial institutions may pose systemic risk to the financial sector and raise the concerns of bank supervisors as to the safety and soundness of their operations.

Financial firms in most jurisdictions are supervised at the legal entity level focused on licensed financial institutions. Thus, in the light of the growing use of non-bank third parties, several bank supervisors have developed alternative ways of monitoring and supervising the risks posed by these third-party providers. To understand the varying degrees of supervisory authority across jurisdictions, a stocktake of current supervisory regimes for third-party service providers was performed (see Annex 2 for an overview).

Based on this stocktake, two regimes for third-party supervision were identified. In the first regime, the bank supervisor has the statutory authority to directly supervise third-party service providers or activities provided by third-party service providers to banks. Examples of supervisors with such statutory powers include the Commission de Surveillance du Secteur Financier (CSSF) in Luxembourg, the Saudi Arabian Monetary Authority (SAMA), and the Federal Reserve, Federal Deposit Insurance Corporation (FDIC) and the Office of the Comptroller of the Currency (OCC) in the United States. The second approach, which is most common among bank supervisors internationally, is to gain access to third parties via the contracts these parties have signed with supervised banks. Regardless of which regime is applied, bank supervisors were also asked whether they actively used this authority and had structures in place to regularly supervise third-party service providers on a regular basis. While some bank supervisors had supervision programmes in place, the majority of supervisors responded that they supervise third-party service providers only under limited circumstances and had no programme in place.

2. Licensing regimes

To assess how different regulatory structures affect the development of fintech firms, the BCBS conducted a survey on licensing frameworks. Agencies in 19 jurisdictions in several regions responded. Based on a comparison of the products, business model structures and licensing frameworks, the following observations emerged.

- The survey showed that licensing regimes typically have a range of options that include full banking licences, limited banking licences, and other types of licence with requirements and restrictions that vary based on the type of entity and/or activity. In most jurisdictions, traditional financial services are under some type of licence; generally full banking licences for activities typically conducted by banks (eg lending or deposit-taking) and/or another type of licence for financial services that usually involve non-bank financial entities (eg payment services or investment services).

- There are few global providers for the fintech financial products and services reviewed and only limited examples of products and services being offered in more than one jurisdiction. It is difficult to determine whether this is driven by the complexity of managing across differing licensing and regulatory frameworks, or if the fintech business models have yet to achieve full penetration of domestic markets that would warrant the increased investment.

- Completely new financial products and services tend to be subject to limited licensing or supervisory framework precedents, or none at all. This was observed with the issuance or transfer of digital cryptocurrencies, such as Bitcoin and its exchanges, where few jurisdictions have licensing requirements.

The potential influence of different licensing regimes on the business models reviewed was observed for different fintech lending business model structures. These differences appear to be more directly tied to licensing differences than payment services and investment advisory services. However, basic regulatory and consumer protection requirements were applicable in all surveyed jurisdictions (see Annex 3).

Recognising this potential influence, potential changes to licensing frameworks are being considered related to the emergence of fintech. Annex 3 provides examples from the European Union, India, Switzerland, the United Kingdom and the United States, where regulators have reassessed or revised certain processes by which new financial services providers, including banks, are authorised to better facilitate or support new entrants to the financial industry. Other jurisdictions also noted that they are considering additional changes to licensing regimes.

Supervisors should closely monitor changes in how financial services are delivered and managed based on new innovative business models and how those changes affect their ability to supervise end-to-end financial transactions under current regulatory and licensing frameworks. Supervisors should consider:

1. Changes to business models from emerging fintech companies that can potentially result in gaps in traditional supervisory and regulatory frameworks. Such gaps may arise if fintech companies are performing activities that are traditionally performed by regulated banks, or if banks are highly dependent upon activities that are not defined as regulated activities. Supervisors should closely monitor changes in bank business models and the delivery of financial services and, where warranted, should adapt their regulatory frameworks and supervisory approaches.

2. In BCBS surveys, most authorities responded that they are comfortable with the applicability of regulatory requirements to banking services offered by fintech firms. However, many noted examples of new business products and models that operate outside what is considered traditional banking, such as crowdfunding, digital currencies and other innovative products that may not necessarily be covered by bank supervisors. As a result, nearly half of regulatory authorities are considering new regulations or guidance related to emerging fintech services.

3. Recognising the above, supervisors should establish processes to assess and monitor potential risks that financial service innovations, and the enabling technologies that support them, may pose to financial stability, and determine suitable responses. The range of actions that agencies have taken to date include research and papers on fintech developments, engagement with existing firms and new entrant fintech firms, and changes to supervisory processes and, in some cases, to regulatory requirements and processes.

4. A transparent view of end-to-end operations and the management of risk for financial services, regardless of legal entity structure, will be essential to effective supervision. The entry of new non-bank players, both as the main providers of banking services and as third-party service providers, could result in significant financial services activities that are integral to banks but not subject to prudential supervision under current supervisory frameworks. Each jurisdiction should monitor trends and consider whether their regulatory framework and supervisory approaches continue to be appropriate based on changes in the banking industry and how financial services are delivered. Virtually all jurisdictions conduct prudential supervisory and enforcement activities at the legal

entity level, not by types of activity. Nonetheless, within most of these frameworks, opportunities exist to conduct supervision based on activity, rather than legal entity type.

5. Evaluating whether the current regulatory frameworks and supervisory processes may present unintended barriers to fintech innovations. These barriers could inadvertently result in the development of innovations outside the regulated financial industry, creating an unlevel playing field for competitors and potentially exposing financial consumers to unwarranted risk.

E. Facilitation of innovation

Observation 10: *The common aim of jurisdictions is to strike the right balance between safeguarding financial stability and consumer protection while leaving room for innovation. Some agencies have put in place approaches to improve interaction with innovative financial players and to facilitate innovative technologies and business models in financial services (eg innovation hubs, accelerators, regulatory sandboxes and other forms of interaction) with distinct differences*.

Recommendation 10: Supervisors should learn from each other's approaches and practices, and consider whether it would be appropriate to implement similar approaches or practices.

As technological innovation has become a focal point in bank supervision and regulation, some jurisdictions have decided to take a more active approach in facilitating it while pursuing their regulatory objectives (such as financial stability, consumer protection and AML/CFT). To this end, these jurisdictions have set up a variety of innovation facilitation mechanisms captured under labels such as innovation hubs, accelerators and regulatory sandboxes. The BCBS and FSB conducted a joint survey on fintech supervisory approaches, supported by follow-up bilateral meetings between the BCBS and some supervisory authorities. Graph 10 below summarises the high-level findings with examples of the supervisory initiatives.

The aim of these initiatives is to help companies navigate the supervisory regulations applicable to fully operational financial service institutions. While the level of support offered by each initiative varies, they all seek to provide regulatory guidance to innovative companies. From the authorities' perspective, these interactions with innovative firms add value by deepening the supervisory understanding of the risks and benefits emerging from the new technologies, products and services, as also noted by the FSB.[30] A proactive approach towards innovation also has the benefit of helping regulatory agencies identify and explore the use of new technologies for internal supervisory purposes (suptech).

The BCBS's survey of innovation hubs, accelerators and sandboxes suggests that these terms are tailored to the individual authority and should therefore be approached with caution. The list of approaches is non-exhaustive and some agencies have labelled their innovation facilitator differently (catalyst, innovation lab, innovation programmes, task forces, helpdesk etc). In particular, programmes under the same label may differ in terms of mandate and resources. Each programme's range of actions is specific and depends on the regulatory framework and the agency's mandate. Thus, while the objectives are broadly similar, the implementation remains jurisdiction-specific.

As most of these initiatives were set up in the past two years and continue to evolve, it is too early to draw firm conclusions on the benefits and challenges of these initiatives and to identify best practices. The BCBS will continue monitoring these innovation facilitators and simultaneously encourage

[30] Financial Stability Board, *Financial Stability Implications from Fintech*, June 2017, Recommendation 7: Shared learning with a diverse set of private sector parties: In order to support the benefits of innovation through shared learning and through greater access to information on developments, authorities should continue to improve communication channels with the private sector and to share their experiences with regulatory sandboxes, accelerators and innovation hubs, as well as other forms of interaction. See www.fsb.org/wp-content/uploads/R270617.pdf.

supervisors to observe and learn from other authorities' approaches and experiences as an input when considering the development of supervisory initiatives towards innovation.

Graph 10: Jurisdictions' initiatives to facilitate innovation

	Innovation facilitators		
	Innovation hub	Accelerator	Regulatory sandbox
	A place to meet and exchange ideas	"Boot-camp" for start-ups, culminating in a pitch presentation	Testing in a controlled environment, with tailored policy options
Australia	ASIC	ASIC	ASIC
Belgium	NBB/FSMA		
ECB	SSM[31]		
France	ACPR/AMF	BDF	
Germany	BaFin		
Italy	BOI		
Hong Kong	HKMA		HKMA
Japan	BoJ/FSA		
Korea	FSC		FSC
Luxembourg	CSSF		
Netherlands	DNB/AFM		DNB/AFM
Singapore	MAS	MAS	MAS
Switzerland	FINMA		FINMA
UK	BOE/FCA	BOE	FCA[32]

Source: BCBS-FSB survey.

Since fintech companies interact with prudential supervisors and also with conduct authorities or financial market agencies, the BCBS has looked at initiatives and programmes put in place by both member and non-member agencies. Box 7 outlines the distinctive features of these various approaches.

Box 7

Innovation hubs, accelerators and regulatory sandboxes

Innovation hubs

Innovation hubs aim at supporting, advising or guiding regulated or unregulated innovative firms in navigating the regulatory framework. An innovation hub can be described as an information exchange regime on fintech matters. In this framework, new companies as well as incumbent institutions with a new technology-driven project can enter into

[31] To be launched in Q3 2017 (see *Digital na(t)ive? Fintechs and the future of banking,* statement by Sabine Lautenschläger, Member of the Executive Board of the ECB and Vice-Chair of the Supervisory Board of the ECB, at an ECB Fintech Workshop, Frankfurt, 27 March 2017, www.bankingsupervision.europa.eu/press/speeches/date/2017/html/se170327_1.en.html. In contrast to the national innovation hubs, the Single Supervisory Mechanism's (SSM) Fintech Hub interfaces with the 19 euro zone national hubs as a means of promoting information exchange and best practices amongst the supervisory authorities.

[32] The UK authorities also offer the Mobilisation Route, which applies to new banks, is limited to 12 months, and deposits are capped at GBP 50,000.

a dialogue with the respective supervisor. Communication between the company and the supervisor usually has a rather open and informal character. Innovation hubs can range from hosting and attending industry events to informal guidance or assistance in preparing and making an application for authorisation or new products. Supervisors may use innovation hubs to understand and monitor the new business models and technologies as well as to identify regulatory and supervisory challenges associated with fintech risks and opportunities. Against this background, single points of contact, dedicated newly created units, identified networks of experts or similar organisational arrangements can be considered as innovation hubs.

Accelerators

Accelerators are usually founded and run by experienced private sector participants. They are fixed-term programmes that include mentorship or education from the sponsoring partners. They can culminate in a public pitch event or a demo day where selected young firms can present their solutions to a problem.

Against this background, accelerators can be understood as projects or programmes by supervisors or central banks where private sector firms are involved to address specific problems or to explore new technologies. Through joint partnership and projects with private sector fintech firms, agencies can explore how innovative solutions could be used in central banking operations including in the conduct of supervisory tasks (suptech).

Regulatory sandboxes

A regulatory sandbox usually refers to live testing of new products or services in a controlled environment. Sandboxes may be considered to be more than just a dialogue or an informal exchange as they engage a supervisor's active cooperation during the test period. Sandboxes also imply the use of legally provided discretions by the supervisory agency. Their use depends on the jurisdiction.

In contrast to innovation hubs, which provide regulatory advice upon request, the sandbox approach usually entails a prior application process and selection by the supervisor. Several criteria may have to be met by a firm when applying for a sandbox: for example, being a genuine innovation with a consumer benefit, not easily fitting into an existing regulatory framework and being ready for market. Based on initial feedback received on regulatory sandboxes, it is worth noting that these test runs may or may not involve regulated activities (deposit-taking, lending, payment services etc), even if financial firms are applying new technologies or new uses for data. Therefore, the sandbox can be made available to regulated as well as unregulated firms.

Sandboxes may also grant temporary regulatory forbearance or alleviation to selected firms. Since the sandbox regimes have been set up only recently, concrete insights about the regulatory implications of the sandbox are still limited. If they provide regulated products and services, they may be granted with a restricted licence or permission. It is worth observing that regulatory challenges are not always related to prudential banking regulation. They can also stem from data protection, consumer protection or AML/CFT rules. Therefore, sandbox participants must typically inform consumers and all relevant stakeholders that the company is providing the service under a sandbox regime. Confidentiality of customer data must also be ensured.

In addition, the testing environment often involves operating restrictions or parameters for the firms conducting the test (eg a maximum number of clients or maximum transaction level). Sandbox testing typically runs for a predefined period of time. Some authorities that have set up sandboxes also require sandbox participants to have a proper exit strategy to ensure that any obligation to customers is fulfilled or addressed before exiting the test.

Sandbox approaches aim at encouraging fintech experimentation, especially with technologies that do not fit easily into the current regulatory framework. When authorities consider establishing a sandbox, they should ensure that the potential risks are properly managed, including those surrounding the ability of supervisors (as opposed to that of the market) to select promising companies, the supervisory authority's liability in case of failure or complaints by consumers, any potential unlevelling of the playing field, and any potential violation of the authority's duty of impartiality towards market participants.

Annex 1 – Glossary of terms and acronyms used in this document

Anti-money laundering and countering the financing of terrorism (AML/CFT) measures are defined by the Financial Action Task Force (FATF), the international standard setter in this area. The BCBS regularly issues guidance to facilitate banks' compliance with their obligations in this area.

An **application programming interface (API)** is a set of rules and specifications followed by software programmes to communicate with each other, and an interface between different software programmes that facilitates their interaction.

Artificial intelligence (AI) is defined as 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. Machine learning (see below) is one subcategory of AI.

Big data designates the large volume of data that can be generated, analysed and increasingly used by digital tools and information systems. This capability is driven by the increased availability of structured data, the ability to process unstructured data, increased data storage capabilities and advances in computing power.

Bigtech refers to large, globally active technology firms with a relative advantage in digital technology. The GAFA acronym refers specifically to a set of the largest technology companies, namely Google, Amazon, Facebook and Apple (the GAFAA acronym is also used to include the largest Chinese technology company Alibaba).

Cloud computing refers to 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 (eg networks, servers, storage facilities, applications and services) that can be rapidly released with minimal management effort or service provider interaction.

Copy trading refers to trading strategies on platforms that allow users to automatically copy positions taken by a selected investor. Copy trading links a portion of the copying trader's funds to the account of the copied investor. These strategies evolved from "mirror trading," and both are categories of a broader phenomenon known as "social trading," or the use of social network platforms to compare trading strategies.

Crowdfunding is the practice of funding a project or venture by raising monetary contributions from a large number of people. It is often performed today via internet-mediated registries that facilitate money collection for the borrower (lending) or issuer (equity).

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

Cyber-risk, according to the definition given by the CPMI-IOSCO 2016 Guidance,[33] is 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 given organisation.

A **digital currency** (or non-fiat currency) is an asset that only exists electronically and that can be used as a currency (means of payment, store of value, unit of account) although it is not legal tender. Digital currencies are often underpinned by distributed ledger technology (see below) to record and verify transactions made using the digital currency. These can include private currencies and digital versions of national bank currencies. Because of the use of cryptography techniques, a (large) subset of digital currencies are referred to as "cryptocurrencies".

Distributed ledger technologies (DLT) such as blockchain are a means of recording information through a distributed ledger, ie a repeated digital copy of data at multiple locations. These technologies enable 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.

Innovation accelerator is 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.

[33] Committee on Payments and Market Infrastructures and International Organization of Securities Commissions, *Guidance on cyber resilience for financial market infrastructures*, June 2016, www.bis.org/cpmi/publ/d146.pdf.

Innovation hub is 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.

The **internet of things (IoT)** is the networking of physical devices, vehicles, buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to (a) collect and exchange data and (b) send, receive, and execute commands.

Machine learning (ML) is a method of designing problem-solving rules that improve automatically through experience. Machine-learning algorithms give computers the ability to learn without specifying all the knowledge a computer would need to perform the desired task, as well as study and build algorithms that can learn from and make predictions based on data and experience.

Online lending platforms intermediate loans online, and may be operated by banks or non-banks. Some online lenders keep all or some of the loans they originate, while others sell or securitise them. Funding for loans may come from traditional sources, such as deposits, if the lender is a bank, securitisations, private investors and capital raisings, and loans from banks. Additionally, funding may come from "peer-to-peer" arrangements that directly match lenders with borrowers via online platforms. Together with non-loan forms of finance such as invoice trading, these models make up the "fintech credit" category.

Mobile wallets replicate a physical wallet in a digital interface on a mobile phone. Customers can add credit and debit cards, as well as prepaid cards, gift cards and rewards cards to be stored and carried. This use case not only replaces physical plastic cards, but also allows those cards to be enhanced by additional services.

Neo-banks are newly created banks that offer mobile-only banking products and services using smartphone applications that serve as an alternative to traditional banking with bricks-and-mortar branch networks.

Regtech (regulatory technology) is defined as any range of fintech applications for regulatory reporting and compliance purposes by regulated financial institutions. This can also refer to firms that offer such applications.

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. 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).

Robo-advisors are applications that combine digital interfaces and algorithms, and can also include machine learning, in order to provide services ranging from automated financial recommendations to contract brokering to portfolio management to their clients, with limited human intervention or none. Such advisors may be standalone firms and platforms, or can be the in-house applications of incumbent financial institutions.

Security biometric services provide a security mechanism used to identify, authenticate and provide access to a facility or system based on the automatic and instant verification of an individual's physical characteristics, such as fingerprints, retina patterns etc.

Smart contracts are programmable applications that, in financial transactions, can trigger financial flows or changes of ownership if specific events occur. Some smart contracts are able to self-verify their own conditions and self-execute by releasing payments and/or carrying out others' instructions.

Suptech (supervisory technology) is the use of technologically enabled innovation by supervisory authorities.

Annex 2 – Indirect supervision of third-party service providers

Graph 11: stocktake of current supervisory regimes for third-party service providers

	Authority to supervise or examine third-party service providers[1]	Regulatory requirement for contracts to allow supervisory access	Programme/process to supervise service provider activities
Argentina – BCRA	Yes	Yes	Depends
Australia – APRA	No	Yes	Depends
Australia – RBA	No	Yes	No
Australia – ASIC	No	No	No
Belgium – NBB	Yes	Yes	Yes
Brazil – CBB	No	Yes	Depends
Canada – OSFI	No	Yes	No
China – CBRC	Depends	Yes	Depends
European Central Bank	Yes	Yes	Yes
France – ACPR	Yes	Yes	No
Germany – BuBa	Yes	Yes	Yes
Germany – BAFIN	Yes	Yes	Yes
Hong-Kong – HKMA	No	Yes	No
India – RBI	Depends	Yes	Depends
Italy – BoI	Yes	Yes	Depends
Japan – FSA	Yes	Yes	Depends
Japan – BoJ	No	No	Depends
Korea – BoK	No	No	No
Korea – FSS	No	Yes	No
Luxembourg – CSSF	Yes	Yes	Yes
Mexico – BoM	No	Yes	No
Mexico – CNBV	Depends	Yes	Yes
Netherlands – DNB	Yes	Yes	Depends
Russia – CBR	No	Yes	Yes
Saudi Arabia – SAMA	Yes	Yes	Yes
Singapore – MAS	No	Yes	No
South Africa – SARB	No	Yes	No
Spain – BoS	Yes	Yes	Yes
Sweden – Finansinspektionen	Yes	Yes	No
Switzerland – SNB and FINMA	Depends	Depends	No
Turkey – BRSA	Yes	Yes	Depends
United Kingdom – BoE and FCA	Yes	Yes	No
United States – FRB	Yes	No	Yes
United States – FDIC	Yes	No	Yes
United States – OCC	Yes	No	Yes

The responses to the questions above are general summarisations of authorities and approaches. Each jurisdiction's authorities and approaches are unique to the specific agency. Use of the "Depends" response reflects that actual authorities, requirements and/or approach to supervision will differ based on a number of factors unique to the circumstances of a given situation (eg powers limited to the systems, tools and applications used in the provision of services to banks).

[1] *For European countries, the authority to supervise third-party service providers is usually limited to activities and services provided to the bank, with the aim to inspect if the proper business organisation of the bank is ensured and not compromised. If deficiencies are identified, further regulatory actions can be taken towards the bank, not towards the third-party service provider.*

Source: BCBS survey.

As can be seen in the responses above, supervisory approaches are not necessarily straightforward and may be dependent on the type of service, organisational relationship or requirements of the individual contract. In order to demonstrate the differences in approaches to third-party service providers, outlined below are comparisons between the United States, the European Union and Japan.

In the United States, the Bank Service Company Act (BSCA), 12 USC §1867(c) provides the federal banking agencies with the authority to regulate and examine the performance of certain services by a third-party service provider for a depository institution "to the same extent as if such services were being performed by the depository institution itself on its own premises". Other statutory authority may also be

relevant in specific situations, such as the enforcement authority over third-party service providers that meet the definition of "institution-affiliated party" (IAP) in the Federal Deposit Insurance Act (FDI Act), 12 USC §1813(u). In the United States, the federal banking agencies have used this authority to conduct individual examinations of service providers, but have further developed a formal supervisory programme for significant technology service providers (TSPs) for the US banking industry. These examinations focus primarily on technology and operational risk. However, where appropriate, the inter-agency examination team may expand the scope of review for product-specific risks or other risk areas that can impact the services provided to the client depository institutions. In addition to the federal banking agencies, other financial supervisors, such as the Consumer Financial Protection Bureau (CFPB) and several state banking agencies have varying levels of authority to conduct examinations of third-party service providers.

Agencies from the European Union have the authority to supervise third parties to whom credit institutions have outsourced operational functions or activities. But this authority is limited to the activities and services that are provided to the bank. According to European law, authorities may obtain all necessary information from third parties and conduct all necessary investigations including inspections at their business premises. A regulatory requirement for supervisory access is guaranteed in a specific clause in the outsourcing contract (see 2006 CEBS guidelines on outsourcing).[34] In some countries such as Italy, outsourcing contracts of operational functions can be subject to prior validation by the supervisory authority.

Supervisory powers in the European Union are granted by the Capital Requirements Directive (CRD4), which is transposed into national law as well as into the regulation of the ECB's Single Supervisory Mechanism. In practice, the national transposition process results in differing national laws and outsourcing requirements across countries. Against this background, the EBA is currently working on a common recommendation on outsourcing to cloud service providers.[35]

Moreover, there are substantial differences in the extent to which supervisory agencies use their powers. For instance, Luxembourg has developed a formal supervision programme for third-party service providers of operational functions, since they are registered as such by the CSSF ("*professionnel du secteur financier de support*"). By contrast, the United Kingdom does not supervise service provider activities as part of a formal programme. Other agencies make use of this power only during on-site investigations at credit institutions (for instance, the Netherlands, Germany, France and Spain as part of the ECB on-site investigations programme).

In Japan, the Financial Services Agency (FSA) has the authority to supervise third-party service suppliers to banks including assignees engaged indirectly in the extended supply chains (Articles 24, 25 etc of the Banking Act). While the Bank of Japan (BoJ) does not have a similar level of supervisory authority, the BoJ can conduct on-site examinations into assigned service providers (and re-assignees) on their consent as well as consent by the assignor bank and initially assigned service providers. In addition to on-site examinations, the BoJ conducts day-to-day off-site monitoring on their activities.

While this analysis was conducted based on high-level questions and only addressed selected jurisdictions and supervisors, the differences highlight the varying degrees of oversight and supervision of banking operations supported by non-bank third-party service providers. As fintech evolves, scope exists for greater outsourcing of bank operations, which would then potentially take place outside a supervised environment.

[34] A revision of the 2006 CEBS guidelines on outsourcing is foreseen in the 2017 EBA work programme.

[35] See European Banking Authority, Recommendations on outsourcing to cloud service providers, May 2017, http://www.eba.europa.eu/regulation-and-policy/internal-governance/recommendations-on-outsourcing-to-cloud-service-providers.

Annex 3 – Licensing frameworks: comparative analysis for specific business models

Overview of existing licensing regimes and comparative analysis for business models

The BCBS's survey on licensing frameworks attracted responses from agencies in 19 jurisdictions, across all geographical areas.[36] Below is an overview of licensing regimes, based on survey results:

Graph 12: Overview of licensing regimes per services and jurisdictions

	Number of jurisdictions with available licensing category			
	Full banking licence	Limited banking licence	Other financial licence	No licence
Authorities to extend credit and make loans	16	10	11	5
Deposit-taking authorities or other repayable funds from the public	20	7	8	1
Indirect lending and credit services (ie underwrite credit on behalf of others)	11	4	11	7
Providing payments and value transfer services	16	7	19	1
Issuance / transfer of non-fiat digital currency	6	2	7	12
Providing clearing and/or settlement of payment transactions or transactions in financial instruments	6	3	16	1
Investment services (receipt, execution, transmission of trading orders on behalf of third parties, own-account trading, portfolio management, investment advice)	16	5	19	0
Fiduciary and custody services	14	6	15	0

In comparing the licensing frameworks for financial services across jurisdictions, the main observations are:

- All but one participating jurisdiction required some form of financial licence in order to take public deposits. The majority require a full banking licence, but 50% of respondents did allow for some form of deposit-taking based on a limited banking or other financial licence. These survey results may not be fully transparent as the definition of a deposit can vary between jurisdictions.
- Almost all jurisdictions allowed extensions of credit under more than one licence type with options for limited banking or other financial licences. Approximately 25% of jurisdictions report that some forms of lending could be conducted without a financial licence.
- Almost all jurisdictions allow payment services through more than one licence type with options for limited banking, other financial licences or other licensing schemes. However, as opposed to

[36] Argentina, Belgium, Brazil, Canada, China, France, Germany, India, Italy, Japan, Luxembourg, Mexico, the Netherlands, Singapore, South Africa, Spain, Sweden, the United Kingdom and the United States. European regulators (the European Banking Authority, the European Commission and the ECB) also participated.

lending, only one jurisdiction permitted some types of payment services to be delivered without a licence.

- Clearing, settlement and other investment services are permitted through other financial licences outside the banking sector across almost all respondents. However, more than 60% of jurisdictions also allowed investment services to be conducted under banking licences and 32% permitted clearing and settlement activities under a banking licence.

Given the differences observed between licensing regimes in various jurisdictions, the influence of licensing requirements on business models and structures has been analysed. Based on a comparison of the products, business model structures and licensing frameworks across some jurisdictions, the following observations were noted concerning the fintech business models reviewed.[37]

The licensing framework may influence not only the business model, but also the range of permissible activities (eg consumer finance is not permitted by the French P2P regulation). Concerning the business models, in some jurisdictions, the platforms obtain licences or registration to originate loans by acting as an intermediary between borrowers and investors (eg France or the United Kingdom) while, in others, the platforms need to partner with licensed financial institutions to carry out the lending business (eg Germany); or have the option of either method (eg the United States). Under the second framework, loans are originated by a collaborating bank, for example, and then sold to investors through the platform or to the platform itself. In both cases, lending platform business models rely on fees, but if the platform's balance sheet is committed, the platform may also generate interest income from the loans held on its balance sheet. Supervisory oversight may be also determined by licensing regimes across jurisdictions.

In the case of lending platforms that extend credit and make loans, there are various types of licensing framework, depending on the jurisdiction, ranging from a full banking licence to other licences. The majority of jurisdictions issue full banking licences that authorise lending by making use of balance sheet funding capacities. In addition, many jurisdictions issue limited banking or other licences for lending. Some limited banking licences and other licences do not authorise deposit-taking activities. However, in some jurisdictions, no licence is required for lending activities but deposit-taking activities are not allowed (eg Spain, Germany and the United Kingdom). However, in all jurisdictions, consumer protection regulations, AML/CFT regulations, and investor protection requirements are applied to these non-bank lenders. But lending platforms challenge this regulatory framework since they generally seek to implement an originate-to-distribute business model without making use of their balance sheet to conduct lending. Thus, in some jurisdictions, the platforms obtain specific licences or registrations to act as an intermediary between borrowers and investors (eg France or the United Kingdom) while, in others, the platforms need to partner with licensed financial institutions to carry out the lending business (eg the United States and Germany).

In the case of payment platforms, the large majority of jurisdictions surveyed require some form of licence to provide payment services. This typically takes the form of a full or limited banking licence or other financial licence (see Graph 12). Regarding the payments products reviewed, different business models across jurisdictions have been identified, but no significant differences because of licensing frameworks were observed.

Payments platforms and value transfer services business models are structured so as to be subject to limited or varied licensing. The most usual form of regulation is licensing as a money services business or an e-money institution. Payment services that only establish a connection to existing bank accounts and provide an aggregation service are not subject to a licensing requirement in most jurisdictions except in the European Union, but are subject to other regulatory requirements around data privacy/protection.

[37] The lending platforms reviewed are Lendix (France), Lending Club (United States), Lendico (Germany) and Funding Circle (United Kingdom). The payment platforms reviewed are Venmo (United States), Circle (US/UK), WeChatPay (China), Ipagoo (United Kingdom), Swish (Sweden) and Tink (Sweden) and the robo-advisors reviewed are Acorn (United States), Wealthfront (United States), Betterment (United States), Nutmeg (United Kingdom) and MoneyFarm (United Kingdom).

Many fintech firms in the payments business typically have some association with incumbent banks. However, this linkage can vary from direct partnership to shared processes for the authentication of customer banking information.

The provision of investment services requires financial licences in all jurisdictions (usually another financial licence or a full or limited banking licence, see Graph 12). All the robo-advisors reviewed are hybrid model (ie there is some level of human intervention) and offer similar services. Nevertheless, how the businesses are structured does differ, primarily due to licensing/registration requirements. Hence, in the United Kingdom, advisory and management services can be offered by the same company (registered by the Financial Conduct Authority), while, in the United States, two separate companies – an investment adviser and a broker dealer – would be required.

Examples of fintech-related changes to licensing frameworks

Instances exist where policy developments have enabled the adoption of technology in line with new developments. For example, responding to innovation in the use of API technology to enable payment origination by third parties, the EU's Payment Services Directive (PSD) was introduced in 2007, updated in 2009, and has been further updated to PSD2, due to come into force in 2018. PSD2 is a significant reform to the EU regulatory regime for payment services in that it caters for innovations in payment services such as aggregation and payment initiation.

Also within Europe, the ECB's Single Supervisory Mechanism (SSM), together with 19 national bank supervisory authorities, has established a policy on the assessment of fintech bank licensing applications. This policy was developed in response to an increasing number of firms developing fintech business models that are seeking a banking licence. It is envisaged that the SSM policy will be externally published for consultation in Q3 2017 to enhance transparency for potential fintech bank applicants.

Regulators have taken steps to revise the process by which new financial services providers, including banks, are authorised to remove any undesirable barriers to new entrants. The UK Financial Conduct Authority (FCA) and the Bank of England have jointly set up a New Bank Start-up Unit, which, among other things, seeks to ensure that there are no disproportionate barriers to entry for new entrants, whether fintech or traditional banks.

In the United Kingdom, a review of requirements for firms entering into or expanding into the banking sector in 2013 resulted in the introduction of an alternative route to becoming a fully operational bank. New banks can now be authorised at an earlier stage to help new entrants to secure further investment, recruit staff, invest in IT systems and commit to third-party suppliers without uncertainty regarding initial authorisation. Under this approach, the amount of deposits the new bank can hold is limited (usually up to £50,000) until it is fully operational, which allows the firm to test out its value proposition without impacting the wider financial system. Firms are expected to produce a mobilisation plan during the authorisation period and are expected to fully deliver the plan within a year. Once it is fully operational, the restrictions on the bank are lifted.

In the United States, the OCC has begun to lay the foundation for considering applications from fintech companies seeking special purpose national bank charters. In March 2017, the OCC added to its Licensing Manual a draft supplement on evaluating charter applications from financial technology companies. The supplement outlines how the OCC would evaluate a fintech company that applies for a special purpose national bank charter. The agency solicited public comments on the draft supplement, which are currently being reviewed before the agency determines its next steps.

The Reserve Bank of India (RBI) issued restricted payments bank licences in India during 2015 with the aim of furthering financial inclusion by providing small savings accounts and payments/remittance services to migrant workers, low income households, small businesses and other unorganised sector entities. Payments banks will initially be restricted to holding a maximum balance of about USD 1,500 per individual customer. They will be able to issue ATM and debit cards, but not credit

cards, and they will offer payments and remittance services through various channels. The minimum paid-up equity capital for payments banks will be equivalent of USD 15 million. A payments bank should have a leverage ratio of not less than 3%.

In Switzerland, an innovation area ("sandbox") was implemented on 1 August 2017. The acceptance of public deposits up to CHF 1 million no longer requires a banking licence. The government argues that this change will provide innovative market entrants with the opportunity to test the conceptual and commercial effectiveness of their business models in a limited way before having to apply for authorisation. However, businesses operating within the sandbox are required to inform depositors that their deposits are not protected by deposit protection mechanisms. Furthermore, businesses within the sandbox still have to comply with anti-money laundering regulations if their business activities fall within the scope of the Anti-Money Laundering Act. Furthermore, the Swiss parliament advocated in December 2016 the creation of a new authorisation category (authorisation for financial innovators). This category is intended for business models that are not involved in a typical banking business, but require certain elements of banking activity (in particular, a limited acceptance of client deposits). In view of the reduced risks involved, the authorisation requirements can be less comprehensive than would be the case for a traditional banking licence. Simplified and efficient authorisation and operation requirements, as compared with current banking licensing standards, are envisaged (eg reduced financial reporting obligations, exemption from depositor protection provisions, and exemption from liquidity provisions). Companies with such a licence are allowed to accept public funds up to a maximum of CHF 100 million. The licence is currently expected to enter into force in mid-2018.