Economics, Law and Policy
ISSN 2576-2060 (Print) ISSN 2576-2052 (Online)
Vol. 5, No. 2, 2022
www.scholink.org/ojs/index.php/elp

Original Paper

Crisis Preparedness in the Digital World

Demet Canakci[1]* & Geof Mortlock[2]

[1] Program Director, Toronto Centre, Toronto, Canada

[2] Program Leader, Toronto Centre, Wellington, New Zealand

* Demet Canakci, E-mail: dcanakci@torontocentre.org

Received: November 12, 2022 Accepted: November 22, 2022 Online Published: December 5, 2022

doi:10.22158/elp.v5n2p28 URL: http://dx.doi.org/10.22158/elp.v5n2p28

Abstract

This paper discusses the importance of crisis preparedness and the role of financial supervision in mitigating the risks posed by technological innovations in the financial ecosystem. The paper will focus on the important role that financial supervisors and regulators can play in promoting effective risk management, supervision and crisis preparedness in relation to fintech developments, and the need for coordination and collaboration with policymakers, government, and the financial sector to address potential threats to financial stability. It elaborates on the challenges associated with fintech developments in banking and the potential implications for financial supervision and considers the nature of crisis preparedness in the context of banking in the digital era. The paper also provides thoughts on the tools available to supervisory authorities and central banks in dealing with financial crises while enabling new technologies to enhance financial services provisions.

Keywords

financial crises, fintech, cyber risk, financial supervision, regulation

1. Introduction

Recent years have seen an increase in the development and uptake of financial technology (fintech (Note 1)) by financial institutions globally. This has been especially the case by banks and other financial intermediaries but also applies to many other types of financial institutions, including insurers (general, long-term and health insurers), wealth management providers, securities firms, and investment advisory firms.

The Covid-19 crisis has also promoted the digitization of the financial services industry. It has accelerated the shift towards technology-enabled, contactless, and customer-centric production and consumption of goods and services and working practices. The business model of financial institutions will become more digital-based as they accelerate the adoption of technology. There will be a further

shift away from the use of cash to digital retail payment systems (Note 2).

The uptake of new IT by financial institutions has the potential to bring many benefits, including to strengthen the contestability and competitiveness of financial services, to lower the costs of some financial services, to enhance aspects of risk management, and to better meet the needs of consumers and the real economy. However, it also comes with risks, including the development of "non-bank financial intermediation" in relatively under-regulated sectors and associated disintermediation, the increase in some financial sector risks (especially operational risks), and the potential to increase the risk of financial institution stress and financial instability. In particular, there is a danger that digital platforms, if not well structured and managed, could exacerbate operational risks in banks and non-bank financial institutions, including the risks of cyber-attacks, fraud and money laundering. These risks pose a potential threat to the soundness of individual financial institutions and can exacerbate intra-group contagion in financial conglomerates. Fintech-related risks, together with the emergence of financial services in relatively under-regulated sectors of financial systems, pose a somewhat heightened threat to financial stability. They reinforce the importance of financial sector regulation keeping pace with fintech developments and for supervisory and resolution authorities to be equipped to deal with financial stress in a rapidly evolving fintech environment.

Drawing from Toronto Centre's extensive worldwide supervisory capacity building, and other relevant sources, this paper looks at the risks associated with fintech, with a particular focus on banking and bank-like functions, the implications for financial stability and supervision, and the nature of the crisis preparedness needed by the regulatory and supervisory authorities to ensure that risk events are managed in ways that minimise impacts on financial stability.

2. Fintech Developments

2.1 Fintech in Banking

Financial technology is increasingly making its presence felt in the banking sector. Fintech is being adopted by existing mainstream banks to reduce operating expenses, make more efficient use of data in the assessment of risks, and expand market penetration.

Key areas where fintech is being adopted by mainstream banks include:

1) The increasing use of online and mobile banking to progressively reduce the need for physical customer interface via branch networks, and thereby reduce operating expenses, and facilitating enhanced efficiency for customer interface

2) The use of IT functionality to process large volumes of data to better identify and respond to risks, and to enhance the capacity to target particular market segments with products tailored to consumer needs

3) The use of IT functionality to process applications for credit and reduce the operational expenditure associated with such processes

4) Robo-advisory services to assist in customer queries and advice

Fintech is also being utilized by newly established digital banks and by non-bank financial entities.

The adoption of digital banking platforms takes many forms, and include the following key examples (Note 3):

Digital Payments and E-Money

Fintech innovations are being increasingly applied to wholesale payments, but most of the major developments have been in retail payments. This is particularly the case in developing countries, where cash accounts for the bulk of retail payments and where payment (debit and credit) cards are not widely used. In such cases, fintech firms offer options for peer-to-peer transfers, bill payments, and electronic purchases. In many cases, these services are attached to an e-money product—i.e., a digital wallet where customers can hold monetary value for an undetermined period of time. A pioneer was Kenya's M-PESA, offered by Safaricom, a mobile network operator, but there are numerous other examples. These products can also be tied to savings accounts or insurance products.

International Remittances

A substantial degree of fintech innovation has been focused on large international remittances corridors. Fintech has been used to simplify procedures and cut the costs of transfers, including to serve the undocumented diaspora in a variety of countries. The services may be based on e-money products, traditional bank accounts, cryptocurrencies, or combinations of these.

Personal and Business Loans

Fintech credit is a burgeoning market and can take many forms and target various customer segments, including low-income borrowers and micro, small and medium enterprises. Most often, fintech credit utilizes relatively novel credit-scoring methods based on a wide range of data, including data that are collected outside of the financial sector (e.g., Big Data, bill payments history, mobile phone usage). Many products are based on automated credit decisions, whereby a customer applies for credit and, if successful, has her loan disbursed in only a few minutes via her mobile phone.

Peer-to-Peer (P2P) Lending Platforms

Within fintech credit, an important development is P2P platforms, which are mostly internet-based services provided by a fintech firm where lenders and borrowers interact in a virtual intermediation framework. Platforms vary widely in format and operating rules. Typical characteristics of P2P lending are: (i) no necessary common bond or prior relationship between lenders and borrowers; (ii) intermediation by a P2P lending company; (iii) transactions take place online; (iv) lenders may often choose which borrowers to lend to or invest in, if the P2P platform offers that facility; (v) the loans can be unsecured or secured; (vi) loans are securities that can be transferred to others, either for debt collection or profit.

Crowdfunding Platforms

Crowdfunding platforms are mostly Internet-based services provided by fintech firms to facilitate funding/investment opportunities, including equity investment and donations. Like P2P lending platforms, these vary widely in shape and operating rules.

Robo-Advisors

Robo-advisors (also called "automated" or "digital investment" advisors) are online platforms that provide services such as financial advice and, most often, portfolio management with minimum or no human intervention.

The digital revolution has changed the demand for financial services and led the sector to become more customer centric. On the supply side, it has left some incumbents with ageing and increasingly inefficient technologies, such as an overreliance on rigid mainframes, and an overextended branch network. On the demand side, younger population cohorts increasingly want to bank with their mobile phones and online apps, rather than through the more conventional mainstream banking channels. The banking sector has overcapacity and, in some cases, the wrong kind of capacity. The industry is facing significant restructuring and IT investment costs, which is placing a strain on some banks' profitability, particularly given the low net interest margins on which many banks are currently operating (in particular in the Eurozone and Japan).

2.2 Bigtechs

Large technology companies (Bigtechs) are increasingly getting attention from policymakers due to the expansion of Bigtech firms (e.g., Google (Alphabet), Apple, Facebook, Amazon, and Microsoft) in financial services. This has generally been more rapid and broad-based in Emerging Market and Developing Economies (EMDEs) than that in advanced economies. The expansion of Bigtech firms in EMDEs has brought benefits, but can also give rise to risks and vulnerabilities, including risks relating to data privacy and cyber-attacks. Risks concerning consumer protection may also be larger in the case of EMDEs, particularly where customers have a lower financial literacy and to the extent that Bigtech firms make greater use of personal data (including that acquired from their non-financial business) without appropriate statutory protections of privacy being in place. Where Bigtech firms are the principal or even sole providers of financial services to some EMDE populations, there is a risk of excessive market concentration and attendant issues related to excessive market power and inadequate consumer protection. They may also be subject to heightened operational risks, particularly in environments with weaker communications and financial infrastructure. Competition from Bigtech firms may, in places, also reduce the profitability and resilience of incumbent financial institutions and lead to greater risk-taking.

Bigtechs also handle payment services as part of e-commerce, with some offering them as independent business units. Their business models leverage on their data analytics, network externalities, and interwoven activities, coupled with distinct platforms that process and settle payments, including: (i) overlay systems (using third-party infrastructures such as credit card or retail payment systems); and/or (ii) proprietary systems (using firm-owned infrastructures) (Note 4). Some common business applications include digital wallets, online banking, and domestic and cross-border funds transfers.

The experience of some jurisdictions demonstrates the positive role that well-targeted and designed regulation, supervision and other official-sector policy can play in supporting innovation in financial services while also mitigating risks. Governments in some jurisdictions have also played a key role in promoting the development of financial infrastructures. In doing so, they have facilitated the growth of financial technology, including that employed by Bigtech firms (Note 5). However, there are also examples where regulation has not kept pace with fintech developments, leaving consumers and the wider financial system exposed to significant risks, as discussed later in this paper.

2.3 Non-Bank Payment System Providers

Fintech is also enabling the evolution of "new" forms of banking, such as the development of purely digital/online banks which have no physical presence (e.g., UBank, RaboDirect and ME Bank in Australia; and Wise, Revolut and Starling in the UK, etc.) and non-bank payment system providers.

Non-bank Payment System Providers (PSPs) include Prepaid Payment Instrument (PPI) issuers, such as mobile wallets, card networks and "white label" ATM operators. These developments are an important aspect of fintech and have grown rapidly in many countries via a range of operators, such as Adyen, Braintree, PayPal and Stripe. For example, the Reserve Bank of India has recently announced that it has allowed non-banks to participate in its Centralised Payment Systems (CPS) through Real Time Gross Settlement (RTGS) and National Electronic Fund Transfer (NEFT) systems, in a phased manner.

PSPs are facilitating financial inclusion in EMDEs by providing electronic payments services to large numbers of people who are not currently serviced by banks—i.e., those without a bank account, as, for example, in much of Africa. Hence PSPs can help to promote greater financial inclusion goals by enabling unbanked individuals to use non-bank services as an alternative to payment instruments offered by banks (mainly due to the reason that they do not have a banking account or cannot open one).

Non-bank payment service provider can improve the efficiency of the retail payments system by increasing competition, providing new or improved payment options, and reaching sectors of the population that did not previously have access to payment services. In other situations, non-banks can contribute expertise that the incumbents lack and cooperate with banks to provide innovative services, such as mobile payments. At the same time, the growing involvement of non-banks could also impact risks in the system. The implications will vary by the type of non-bank and the services that they provide. For example, non-banks may specialize in certain services, thus generating large economies of scale or network effects. The nature of these effects could mean that the provision of such services may converge towards a small number of large providers, or in the extreme, a monopoly over the provision of a certain payment service. If a service is localized in a particular non-bank, the operational risk may also be concentrated.

An important feature of non-bank involvement in payments services is outsourcing, where payment service firms place considerable reliance on a wide range of outsourced IT and other functionality providers. Outsourcing offers a range of benefits, including enhanced efficiency, strengthened capacity for innovation and reduced operating costs. If managed well, outsourcing may also offer the potential to reduce operational risks. However, outsourcing also carries a number of risks do not present or not as prevalent with an insourced approach to functionality provision. These include risks of more complicated coordination between the financial service provider and the various outsourced providers of functionality, discontinuity of supply and inadequate contingency arrangements. This requires supervisory authorities to be particularly attentive to outsourcing risks, including the need for robust contractual documentation, testing requirements, backup arrangements and financial institutions maintaining contingency plans to deal with situations where outsource providers fail.

2.4 Digital Currencies

Another area of innovation by technological advancements has been the development of potential new mediums of exchange and store of value, and other means of payment such as central bank digital currency, cryptocurrencies including bitcoin or other digital coins, or claims such as payment services issued by banks or other intermediaries (Alipay, WeChat Pay, M-Pesa, or blockchain-based monies such as Paxos or USD Coin) (Note 6). These developments characterise a "dual" monetary system involving privately issued money (by banks, telecom companies, or specialised payment providers) built upon a foundation of publicly issued money (by central banks).

Claim-based monies can, in turn, be categorised according to whether their redemption is at a fixed value (e.g., bank money or e-money) or at a variable value in the case of Libra, for example, which may have exchange rate risk when converted into domestic currency. Another important distinction is whether the settlement is centralised (e.g., cash, bank money, e-money) or decentralised (e.g., crypto-assets).

Stablecoins are a specific category of cryptoassets that have the potential to enhance the efficiency of the provision of financial services but may also generate risks to financial stability, particularly if they are adopted at a significant scale. Stablecoins are an attempt to address the high volatility of "traditional" crypt-assets by tying the stablecoin's value to one or more other assets, such as sovereign currencies. They have the potential to bring efficiencies to payments systems and to promote financial inclusion. However, a widely adopted stablecoin with a potential reach and use across multiple jurisdictions (global stablecoin or GSC) could become systemically important in and across one or many jurisdictions, including as a means of making payments. The emergence of GSCs may challenge the comprehensiveness and effectiveness of existing regulatory and supervisory oversight. The FSB has agreed on ten high-level recommendations that promote coordinated and effective regulation, supervision and oversight of GSC arrangements to address the financial stability risks posed by GSCs, both at the domestic and international level (Note 7).

Another development in this area is central bank digital currencies which are becoming an important agenda item for many central banks: The Eastern Caribbean has created its own form of digital currency (DCash), which is designed to facilitate faster transactions and serve people without bank accounts. DCash was created by Barbados-based fintech company Bitt in partnership with the central bank. Unlike cryptocurrencies, it is issued by an official central bank and has a fixed value, tied to the existing Eastern Caribbean dollar used across much of the region.

Other countries are developing central bank digital currencies. For example, China launched the e-yuan in 2020; the ECB aims to launch its own digital currency in 2025, while the Bank of England and the Fed are actively exploring the issue. A January 2021 survey (Note 8) by the Bank for International Settlements reported that most central banks are considering digital currencies. The survey found that central banks representing a combined 20 per cent of the world's population are likely to launch their own digital currencies within three years.

Aside from central bank digital currencies, private-based digital currencies, while offering potential benefits in payments capability, also present significant risks. A key concern is the extreme volatility in the value of these digital currencies, with market prices moving by very large amounts intra-day and over a short trading horizon. They also represent a potential avenue for money laundering and other financial crimes unless subject to robust AML/CFT requirements. Moreover, private digital currencies also fail to have the liquidity needed to serve as efficient media of exchange, at least for the time being.

2.5 Regtech and Suptech

Regtech and Suptech are part of the fintech evolution. These tools could have important benefits for financial stability.

Regtech focuses on technology-based solutions to attenuate or solve regulatory and supervisory challenges, including the challenges posed by the expansion of fintech. It leverages digital data and analytical networks to supplement conventional processes to strengthen the capacity to manage risks and improve the decision-making process. For regulated institutions, the use of Regtech could improve compliance outcomes, enhance risk management capabilities, and generate new insights into the business for improved decision-making. For both authorities and regulated institutions, the efficiency and effectiveness gains, and possible improvement in quality arising from automation of previously manual processes offers potentially significant benefits.

Most of Regtech centres around solutions for regulated financial institutions, helping them to comply more efficiently and with greater certainty with regulations and improve risk management, while cutting costs (e.g., compliance costs).

Regtech developments are mainly in the following areas:

(i) *regulatory compliance*—e.g., systems to enable banks and other regulated entities to identify breaches of regulatory requirements and to facilitate quick remediation, and to maintain compliance with regulations;

(ii) *identity management and control*—e.g., anti-money laundering controls and fraud detection;

(iii) *risk management*-advanced data analytics supported by machine learning or other AI applications and regulatory reporting, transaction monitoring such as by using DLT, end-to-end integrity validation, anti-fraud and market abuse identification systems, back-office automation and risk alerts;

(iv) *trading in financial markets*-the automation of the procedures related to transacting in financial markets, such as calculating margins, choosing central counterparties and trading venues, assessing exposures, complying with good conduct-of-business principles, etc.

In some cases (regulatory reporting, KYC), Regtech solutions are developed and implemented jointly or use a third-party solution to achieve efficiency gains, while others are developed and implemented separately by individual financial institutions in bilateral partnerships with fintech firms.

Supervisory technology (Suptech) is being adopted by regulatory authorities to use fintech to assess trends more efficiently in market data to identify potential risk areas, to facilitate peer group analysis of banks and other institutions, and to assess early warning indicators of emergent stress. Suptech is mainly conducted in two types of application: (i) Data collection; and (ii) Data analytics:

(i) *Data collection* applications are used for supervisory reporting, data management and virtual assistance. Examples include the ability to pull data directly from IT systems of banks and other financial institutions; automated data validation and consolidation; chatbots to answer consumer complaints while collecting information that could signal potential areas of concern.

(ii) *Data analytics* applications are used for market surveillance, misconduct analysis as well as microprudential and macroprudential supervision. Examples include detecting insider trading activities, money laundering identification, monitoring supervised entities' liquidity risks and forecasting housing market conditions.

Suptech is a strategic priority for an increasing number of regulatory authorities. It is still at a relatively early stage of development but could evolve into the greater use of 'real time' access to and interrogation of data on financial institutions, and greater analysis of the "big data" contained in regulatory reporting by financial institutions and more widely in other information sets and social media. For authorities, the use of Suptech could improve oversight, surveillance and analytical capabilities, and generate real-time indicators of risk to support forward-looking, judgement based supervision and policymaking. However, such developments depend on supervisory authorities having the necessary resources and skills to take them forward.

3. Risks Associated with Fintech: Implications for Financial Stability

Fintech brings wide-ranging benefits, particularly for low-income countries, due to its potentially far-reaching economic and social impact. Those benefits include increasing access to financial services and financial inclusion; deepening financial markets; strengthening competitiveness in the financial markets; lowering the costs of some financial services; and improving cross-border payments and remittance transfer systems.

However, fintech also creates a number of significant risks in the financial system, and not least in the banking sector. In this paper, the focus is mainly on the risks and the regulatory and supervisory issues that arise from these risks. Supervisors should monitor the evolution of those risks closely and take necessary actions to mitigate them. Although most of the risks are not new, the nature of fintech increases the probability and potential impact of some key risks. Those risks include:

- *Operational risks*-such as cyber risks, IT malfunction fraud, money laundering/financing of crime, misselling of financial products and services, privacy breaches, and breaches of regulatory compliance
- *Credit risk* inadequately managed arising from P2P platforms
- *Reputation risk* for banks/insurers as a result of the above risks, with potential for intra-group contagion
- *Payment system disruption*—e.g., arising from operational dysfunction in non-bank payment providers
- *Business model risk*-as new technology, new entrants and greater competition threaten the viability of existing business models.

Unless these risks are subject to robust governance and risk management frameworks overseen by appropriate prudential and market conduct supervision, they have the potential to cause instability in individual financial institutions, payments networks and potentially the financial system as a whole. Moreover, the entry of new firms into the financial system, such as bigtechs and non-bank payment providers, have the potential to reduce the market share and profitability of the incumbents, with the potential that the established financial firms could come under financial stress, especially in a low net interest income environment.

Some of these risks pose a potential threat to the stability of financial systems via several channels (Note 9):

- **Contagion:** examples of contagion arising via fintech include: (i) significant and unexpected losses incurred on a single fintech lending platform could be interpreted as indicating potential losses across the sector, with flow-on effects to investor and creditor confidence in that sector. (ii) the technical failure of a fintech function in a financial conglomerate could trigger intra-group contagion through the transmission of losses, confidence effects and cross-defaults, and (iii) misconduct or misselling in new fintech sectors could erode market confidence in the wider financial system.

- **Procyclicality:** procyclicality can arise when market participants act in a way that exacerbates the degree and impact of fluctuations in economic growth and market prices over the short and/or longer-term, such as excess provision of credit in economic upswings and excessive deleveraging in a downturn. Examples of procyclicality that could potentially be generated by fintech include: (i) interaction between investors and borrowers on fintech lending platforms could potentially exhibit larger swings in sentiment than traditional intermediation of funds, as a sudden unexpected rise in non-performing loans could trigger a drying up of new funds; (ii) small investors involved in crowdfunding might be more prone to contributing to asset price bubbles (and subsequent bursting of bubbles) due to lower understanding of the risks involved in lending/investing.
- **Excessive volatility:** Excess volatility in financial markets is a key source of instability and can manifest through over-reaction to financial events, potentially creating solvency or liquidity problems that can spiral through the financial system, impairing the functioning of asset and credit markets. Fintech can contribute to this in various ways, including (i) algorithmic traders may tend to be more active during periods of low volatility but rapidly withdraw from the market during periods of market stress when liquidity demands are high, and thereby increase asset price volatility; (ii) crowdfunding investors and person-to-person lenders might be susceptible to exuberant investment in periods of buoyancy, but rapidly withdraw in periods of emerging stress, with adverse impacts on asset prices and flow-on effects to solvency.
- **Systemic importance—e.g., large market dominance:** The systemic importance of financial institutions is a key factor in posing a threat to financial instability. Although fintech does not currently pose a major risk in this regard, it does increase the risk of intra-group contagion as a result of reputation risk. Moreover, the non-bank financial intermediation sector poses a potential risk to instability to the extent that it experiences severe risk events, and these are not detected or responded to quickly and effectively by supervisors.
- **Financial risks being inadequately managed:** the inadequate management of risks associated with fintech pose a threat to financial stability—especially in non-bank financial intermediation and other under-regulated parts of the financial system.

It is worth highlighting two key risks to financial stability arising from fintech: the emergence of non-bank financial intermediation; and the growing threat of cyber risk.

Non-bank financial intermediation

Non-bank financial intermediation refers to the emergence of bank-like functions, such as payment services and intermediation functions, provided by non-bank entities. Examples of these services are mobile banking, e-wallets and P2P intermediation functions. These are increasingly providing an alternative to mainstream banking. Although this is a positive development in terms of strengthening competition for financial services, lowering costs, and increasing financial inclusion, it also poses a risk

to financial stability. This is particularly the case if non-bank fintech providers of financial services become systemically important and where a failure could cause significant disruption to the financial system and economy.

Payment networks using digital wallets provide a direct connection between consumers and merchant processors, operating via software-based systems that store users' payment information. Solutions within a consumer digital wallet can include merchant payments, P2P payments, international money transfers, bank accounts, lending, and cryptocurrency trading. Digital wallets allow a party to make electronic transactions and bypass traditional banks. According to market data provider Statista, digital wallets accounted for 44.5% of all global e-commerce transactions in 2020 (Note 10). In the case of P2P services, growth in these financial services has been relatively strong in some jurisdictions but has not yet reached the point where it poses a significant risk to the financial system.

The challenge in non-bank financial intermediation is when these non-bank providers of financial services grow to a size that could pose a threat to financial stability in the event of a failure event. This has the potential to cause disruption to the financial system through dislocation to the payment and settlement systems and through impacts on credit markets and the real economy. In the P2P area, there is also a risk of adverse confidence effects on depositors with funds at risk in the event of an upswing in credit losses and a risk of a rapid withdrawal of credit and associated asset price volatility.

All of these considerations suggest the need for the regulatory authorities to monitor developments in non-bank financial intermediation by obtaining data from market participants to better understand the nature and scale of their activities, the risks involved, and the adequacy of participants' risk mitigation capacity. This will assist the authorities to monitor the types of business being undertaken and the growth in volume and in market share in particular niches of the market. It will also provide a basis for regulators to assess the nature of the risks involved to affected users of financial services and to the providers of the services and the potential impact on the financial system. Ultimately, as discussed later in this paper, regulatory authorities should be moving to a form of regulation that regulates financial services in a competitively neutral and even-handed manner, regardless of the legal form or licensing status of the provider of financial services—i.e., a "form over substance" approach. The objective should be to regulate financial services on a risk-based basis, anchored to well-defined regulatory objectives based on maintaining financial system stability while also seeking to enable financial system innovation and fostering competition.

Cyber Risk

Another key risk that is of increasing relevance to financial stability is cyber risk. This is already a very significant risk and is likely to grow considerably as online banking, and other forms of digital financial services become more prevalent. Cyber risks of various forms arise in online banking and payment services across the mainstream banks and in the new digital non-bank financial service providers, as well as for networks of small banks using common platforms. Major cyber risk events in banks and other financial institutions have the potential for system-wide disruption, data theft, privacy

breaches, financial crimes and financial losses for financial firms. All of these risk channels have the potential to threaten financial stability, either through disruption to payment and settlement processes or through adverse impacts on market confidence.

In the securities trading area, greater reliance on automated transactions could potentially increase market volatility due to higher asset price correlations. The wider adoption of certain algorithms and technological solutions may increase vulnerabilities to cyberattacks. It may also increase concentration risk on key nodes within the global system as market structures adjust and network interconnections strengthen.

The increase in cyber risk has been a clear trend over the past decade, and regulators and supervisors, as well as the industry, face major challenges in effectively managing these risks. Numbers can be misleading, and even though many financial firms see an increase in attempts, it is the more advanced attacks that matter most. Good data on cyber incidents are scarce, and this is partly due to a lack of incentives for firms to report incidents. One lesson from two recent cyberattacks—on SolarWind's Orion software and on Microsoft Exchange Servers—is the need for a more integrated approach to risk management to combat the threats of cyberattacks. This includes the need for strengthened IT protection software and associated processes; regular IT security audits; strengthened focus by financial institutions' CROs, senior management teams and boards; regular stress testing of cyber protection arrangements; and developing and testing the capacity to respond to and recover from an attack.

The challenges in identifying and managing risks are considerable across areas such as cybersecurity, fraud, anti-money laundering, consumer protection, and cryptoassets. Addressing these risks require coordination among many authorities, nationally and internationally, not only to share information but also to identify events that may not cause losses to financial institutions but do harm consumers and investors.

4. Effective Regulation and Supervision of Fintech

Given the fast-evolving nature of fintech, it is essential that there is an effective regulatory response to fintech developments, particularly as it relates to areas that pose a potential threat to financial stability, such as banking, non-bank financial intermediation and payment systems. In most respects, existing regulatory and supervisory frameworks can be applied to fintech financial services and products, given that fintech risks are generally an extension or variant of existing financial risks rather than being completely new. However, some modifications to regulatory and supervisory frameworks are likely to be needed in the case of currently unregulated or under-regulated parts of the financial system and in respect of those risk factors which represent a significant shift from mainstream banking risks. In this section of the paper, we briefly identify the key areas in which enhanced monitoring and regulation might be needed and the types of regulatory responses that could be appropriate.

The need for greater monitoring of fintech and an assessment of appropriate regulatory measures to ensure that fintech-related risks are managed in ways that maintain financial stability has been recognised by a number of international bodies. These include the Financial Stability Board (FSB) (Note 11), Basel Committee on Banking Supervision (BCBS), International Monetary Fund and World Bank. All of these bodies have undertaken considerable work on fintech-related matters and have published a range of papers on the issues.

Bali Fintech Agenda

In this context, in October 2018, the IMF and World Bank held a conference to promote a wider understanding of fintech and the implications for regulation. This was held in recognition that countries want to harness the benefits that fintech can offer to financial systems, economies, consumers, depositors and investors, but also want to ensure that the risks associated with fintech are well understood and managed. The "Bali Fintech Agenda" (Note 12) resulted from the IMF-World Bank conference and outlined high-level issues for consideration by members of the IMF and World Bank as they seek to develop their policy responses to fintech. The agenda is focused on the implications of fintech for the financial sector and provides a high-level set of principles to guide regulatory oversight of fintech.

The Bali Fintech Agenda brings together key considerations for policymakers and the international community into twelve (12) elements arising from the experience of member countries. It is useful to briefly recap these elements:

- **Element 1**: Embrace the promise of fintech.
- **Element 2**: Enable new technologies to enhance financial service provision.
- **Element 3**: Reinforce competition and commitment to open, free, and contestable markets.
- **Element 4**: Foster fintech to promote financial inclusion and develop financial markets.
- **Element 5**: Monitor developments closely to deepen understanding of evolving financial systems.
- **Element 6**: Adapt regulatory framework and supervisory practices for orderly development and stability of the financial system.
- **Element 7**: Safeguard the integrity of financial systems.
- **Element 8**: Modernise legal frameworks to provide an enabling legal landscape.
- **Element 9**: Ensure the stability of domestic monetary and financial systems.
- **Element 10**: Develop robust financial and data infrastructure to sustain Fintech benefits.
- **Element 11**: Encourage international cooperation and information-sharing.
- **Element 12**: Enhance collective surveillance of the international monetary and financial system.

These elements provide a broad context for assessing the appropriate regulatory and supervisory responses to fintech developments.

Regulatory Objectives

It is clearly important that the authorities understand the risks associated with fintech and design regulatory responses to seek to ensure that the risks are appropriately managed. It is not about achieving "zero risk" outcomes. Innovations and economic activity of all kinds necessarily entail risks. Rather, it is about seeking to ensure that risks are identified, monitored and managed so as to maintain a stable but efficient financial system and to protect those least able to protect themselves—small depositors, policyholders and some categories of investors. National authorities have a delicate balancing act here. On the one hand, they need to ensure that fintech risks are appropriately managed. But on the other hand, they need to maintain their country's competitiveness in the global financial system and harness the consumer, investor and systemic benefits that fintech can provide. It involves seeking an appropriate balance between the promotion of a stable and resilient financial system, and the promotion of a contestable, competitive, innovative and efficient financial system.

There is a need for well-defined regulatory objectives in designing a regulatory approach to fintech.

In most respects, the main regulatory objectives for fintech are the same, in substance, as those that currently apply to conventional financial activities. In that regard, the main financial sector regulatory objectives are:

- To promote and maintain a stable, resilient financial system (i.e., a financial system that is capable of performing all critical functions in the face of severe shocks).
- To promote and maintain an efficient financial system (i.e., a financial system that is dynamically efficient, allocatively efficient and productively efficient).
- To facilitate competitiveness and contestability in the financial sector.
- To protect retail depositors and insurance policyholders within the scope of established protection schemes.
- To promote and maintain the integrity of financial markets.
- To seek to prevent financial crimes.

These financial sector regulatory objectives are just as relevant to fintech activities as they are to conventional financial activities. Fintech presents similar risks and externalities as do conventional financial activities—i.e., risks relating to information asymmetries, disruption to systemically important functions, contagion risks, risk of excessive market volatility, market conduct risks, and risks of financial crimes. Regulation of fintech should therefore seek to ensure that these risks and externalities are properly identified, monitored and managed. However, there is a need to make sure that the risks presented by fintech are well understood before developing new regulatory responses and to ensure that regulation appropriately addresses those risks in a proportionate manner. These new risks (or existing risks made more complex and more damaging in impact) will require particular regulatory attention—either using existing regulatory tools or, in some cases, new ones.

The main regulatory tools relevant to fintech are largely those that are already applied to providers of conventional financial services and products. The tools might need to be modified in some respect to suit the particular characteristics of fintech providers and products/services, and to ensure a proportionate regulatory response to the risks involved, but by and large, existing regulatory frameworks are likely to be applicable to most types of fintech providers. In this regard, the key elements are likely to include the following.

Licensing of Financial Service Providers

A key element of financial sector regulation is a framework to ensure that providers of defined categories of financial products and services are subject to a licensing process so that they meet minimum standards relevant to the risks involved. Licensing requirements will vary greatly depending on the type of entity and the financial products and services it provides. A consistent approach based on types of products and services, rather than legal form, is generally desirable, with a view to achieving a competitively neutral regulatory framework that treats similar products and services in much the same way. A licensing framework typically includes a focus on:

- minimum standards of fit and proper for key officers of the entity;
- the need for the entity in question to have a robust framework for the identification, measurement, monitoring and management of risks, including a well-articulated risk appetite statement, risk management systems and controls, and risk culture;
- robust governance arrangements, including a board (with suitably qualified directors, including non-executive and independent directors) to oversee the strategic direction of the entity and its senior management team, and board committees dedicated to overseeing risk management, audit and remuneration;
- policies for ensuring that conflicts of interest are appropriately managed;
- minimum capital and liquidity requirements, depending on the nature of the risks involved and the parties affected by those risks; and
- the capacity to comply with regulatory requirements.

In the case of financial institutions that are already licensed but whose business and risk profile are changing significantly due to fintech adoption, there is a need for the regulators to ensure that new financial services and products, and the associated risks, are appropriately integrated into the entity's business strategy and risk management framework. For new entities that fall outside the existing regulatory net, such as non-bank financial intermediaries, there is a need for the authorities to design a licensing framework that requires entities to meet defined licensing requirements relevant to the types of financial service they propose to perform on the basis of achieving a 'level playing field' in the financial sector and ensuring that similar products and services are regulated on a consistent basis, regardless of the legal form of the entity which provides them.

Regulatory Requirements

The nature of the regulatory requirements will vary greatly depending on the particular characteristics of the fintech provider and the services and products in question. As a general principle, regulations are designed to ensure that financial services are provided in a secure and reliable manner and in accordance with the prudent management of the risks involved to meet the defined objectives of the regulatory regime. Depending on the type of financial service/product, regulations might cover such matters as:

- market conduct requirements (including product disclosure, provider disclosure, and requirements in relation to advising and selling procedures);
- capital requirements, based on the risks borne by the financial institution and its risk mitigation capacity;
- liquidity requirements, based on the funding and liquidity risk profile of the financial institution;
- governance requirements, such as minimum number of directors on the board, composition of the board, board committees for risk management, audit and remuneration, and responsibilities of the board;
- requirements in relation to risk appetite and the risk management framework applicable to all material risks;
- limits on credit and funding exposure concentration;
- requirements for contingency plans in relation to business continuity, capital and liquidity—and, increasingly, a requirement for a comprehensive recovery plan to address severe financial and operational stress events;
- and fit and proper requirements applicable to key officers.

In the case of existing financial institutions that have adopted or plan to adopt fintech, regulatory authorities will need to ensure that the regulations in place adequately address fintech-related risks. This will be especially important for operational risks, such as cyber risks, IT security, financial integrity and business continuity. It will also be important to ensure that risks associated with market conduct are appropriately regulated through targeted disclosure requirements and measures to combat mi-selling. Regulations relating to information privacy will also be particularly important in the case of fintech services, as will regulations for financial integrity. Regulators will also need to ensure that regulatory arrangements for fintech providers include robust contingency planning, stress testing and crisis simulation requirements tailored to the types of financial technology and associated risks they have.

For new financial institutions not yet covered by regulatory nets, the authorities will need to consider the extension of regulatory requirements to such entities on the basis of seeking to ensure that these entities are brought into the regulatory framework in a competitively neutral manner, such that entities and their services are regulated on the basis of ‘substance over form’.

Supervision

The supervision of fintech will typically draw on existing supervisory frameworks. For a well-developed regulatory authority, supervision of financial institutions will generally be on a risk-based basis, where the supervisory authority has a framework for assessing the risk profile of each entity using a scoring system that evaluates the risks its business involves and the effectiveness of its risk mitigation and loss-absorption buffers, and where it also assesses the systemic importance of the entity. The combination of its risk rating and systemic importance rating will determine the level of supervision to which the entity will be subject, as well as informing the calibration of some of the prudential requirements to which the entity is subject—e.g., capital and liquidity.

Within the risk-based supervisory framework, a supervisory authority would generally conduct supervision using a combination of off-site monitoring based on regular data provided by the regulated entity in accordance with regulatory requirements and on-site assessments conducted by the supervision authority.

As with conventional financial services, a regulatory framework for fintech providers will likely involve the need for the supervisory authority to establish and maintain robust frameworks to monitor key risk areas, including early warning indicators of emerging risks and compliance with regulatory requirements. Particular focus will be needed on those risks that are associated with fintech developments, such as cyber risks, financial integrity risks, market conduct risks, data integrity risks, and contagion risks.

Supervisory arrangements for fintech providers could be expected to involve some form of on-site assessment by financial supervisors, designed to enable the supervisors to identify and evaluate the key risks of the entity in question and the effective management of those risks. A risk-based supervision framework is generally the appropriate model, whereby the calibration of on-site assessments is based on the assessed risk profile and risk mitigation capacity of the entity and its systemic importance. Those entities assessed as being relatively high risk and high systemic importance could be expected to receive greater supervisory attention than those assessed as being of lower risk and lesser systemic importance.

In a fintech context, on-site assessments are likely to focus on the risk areas of greatest relevance to the particular fintech product or service being provided. In many examples of fintech—such as mobile payment system providers, e-wallets, online banking, and P2P frameworks—the key risk areas are likely to be operational in nature, such as cyber risks, information risks, financial crime and market conduct. On-site assessments would also appropriately involve supervisory assessment of a financial institution’s governance arrangements in relation to fintech matters, especially the adequacy of the board’s understanding of the risks associated with fintech and their oversight of the risk management framework applicable to fintech.

Particular areas of focus for supervisors would also include the need to assess the stress testing capacity of financial institutions in relation to fintech risks, including testing the vulnerability to cyberattacks and financial integrity risk. Similarly, supervisors should ensure that fintech developments are fully integrated into a financial institution's "three lines of defence" risk management framework, such that front line staff are charged with responsibility for adhering to risk management requirements in the deployment of fintech, that a risk management unit (overseen by a CRO) has responsibility for overseeing the risk management framework for fintech (integrated into wider risks), and that internal audit has responsibility for regular assessments of adherence to fintech-related risk management requirements. Supervisors should also ensure that financial institutions that deploy or rely on fintech maintain robust contingency plans for dealing with risk impacts. These plans should include BCP arrangements modified to include fintech operational risk events, as well financial contingency plans designed to ensure that capital and liquidity impacts are addressed effectively and in a timely manner. There should be periodic testing of contingency plans, with the results of these being reviewed by the supervision authority.

The table below provides an overview of the types of regulatory responses that can be considered in relation to particular categories of fintech risks.

Table 1. Fintech Risks and Possible Regulatory Responses

Fintech Risks	Possible Regulatory Responses
Market misconduct—e.g., misselling and inadequate disclosure of financial product risks	Regulatory responses are likely to include: • Strengthened disclosure requirements in relation to financial products and services, with clear disclosure of the risk/reward trade-off, with appropriate penalties for breaches of requirements. • A licensing framework for providers of financial products and services to ensure that they meet minimum standards relevant to market conduct, including fit and proper requirements. • Supervisory requirements to ensure that market conduct regulations are complied with, that fit and proper requirements are applied on an ongoing basis, and that regulated entities comply with disclosure requirements.
Financial products and services evolving faster than the	Regulatory responses are likely to include: • Clear definition of the "problems" to be solved and regulatory

law—leaving legal uncertainty over the rules governing such products and services.	objectives. • Ensuring that the regulatory framework is applied on a consistent and competitively neutral basis, such that similar financial products and services are regulated in much the same way. • Increased resourcing for authorities to develop laws that keep pace with new technological developments. • Robust frameworks for legal and regulatory development, including well-structured cost/benefit analysis, consultation with interested parties, and regulatory accountability.
Disintermediation risk, resulting in Fintech providers operating outside regulatory nets.	Regulatory initiatives might include: • Ensuring that regulatory nets are based on clearly defined financial product and service delivery to ensure a competitively neutral framework. • Transitioning where appropriate from a regulatory framework based on defined categories of financial institution to one that is based on types of financial services provided to ensure that the regulatory net applies in a consistent manner across categories of financial services. • Ensuring that non-bank financial intermediaries and other unregulated entities are, at a minimum, brought into a monitoring and evaluation framework to enable the authorities to assess the nature of the business being undertaken, the risks involved, the quality of risk management, and the systemic importance of the business. This will help to inform the development of appropriate regulatory and supervisory requirements.
Cyber risks	Regulatory measures might include: • Licensing requirements for providers of defined types of online financial services, particularly those in which cyber risks (such as cyber-based fraud, identity theft, privacy

	information breaches, and operational dysfunction) are considered to be significant. • Supervisory requirements for cyber risks, including well defined "three lines of defence" risk management requirements, board responsibility for overseeing cyber risks, on-site assessment by supervisors, vulnerability stress testing, and targeted external audits. • A requirement for financial firms to have comprehensive contingency plans to enable them to recover quickly and effectively from a cyber risk event, including back-up arrangements, disaster recovery sites, firewalls to prevent IT risk events from impacting critical functions and services, and regular testing of contingency plans. • Possible extension of safety nets to incorporate losses due to cybercrime.
Financial crimes—e.g., money laundering, financing of illegal activity.	Regulatory requirements would likely include: • Extension of AML/CFT licensing and supervision to Fintech participants (if not already covered). • Enhanced surveillance of transaction activity—e.g., via Suptech and Regtech.
Contagion risk—e.g., as a result of operational dysfunction in one part of the financial system impacting other parts.	Regulatory requirements might include: • Ensuring that the risks of operational dysfunction (e.g., IT failures) are properly managed, and backup arrangements are regularly tested. • Seek to ensure that risk transmission buffers are in place to limit contagion, including robust capital requirements for financial market participants and IT firewalls to limit or prevent the transmission of operational shocks from one entity in a group to another.

	• Ensure that, within financial conglomerates, robust firewalls are in place between different categories of financial services within the conglomerate to limit contagion (including in respect of information and IT protection between entities in the group), and that the head of the group maintains robust contingency plans for addressing risk events.
Financial stability risks—e.g., due to potential asset price bubbles or excessive market concentration of systemically important functions.	Increased market surveillance, regulatory measures to promote improved management of risks that contribute to asset price bubbles, and regulation to limit the systemic dominance of Fintech providers.

5. Early Intervention and Crisis Management

Early Intervention

An important element in the supervisory framework for banks and other financial institutions is early intervention. Under most prudential supervision regimes, the supervisory authority has comprehensive legal powers to intervene and take a range of supervisory actions if a financial institution breaches regulatory requirements or its risk profile is deteriorating. These powers are normally supported by policies and practices under a preventive and corrective action framework, in which the supervisory authority sets out a range of triggers for taking remedial supervisory actions. The triggers generally include breaches of regulatory requirements, as well as deterioration in capital requirements, liquidity requirements, asset quality and other financial and prudential risk metrics. The framework typically sets out an escalating range of supervisory actions in response to particular triggers. These often include measures such as:

- intensification of off-site monitoring;
- more frequent and focused on-site assessments;
- a requirement for the financial institution to obtain an independent assessment of particular matters;
- a requirement for the financial institution to undertake specific actions to remedy the situation, potentially include strengthening risk management arrangements, increasing capital, limiting further risk-taking activity, and curtailing or ceasing the payment of dividends and bonus payments to senior management.

These early intervention frameworks are generally accompanied by contingency plans to enable a supervisory authority to deal with specific types of financial institution stress. Under best practice, the supervision authority undertakes regular testing of its early intervention framework and contingency plans for dealing with stress situations.

In the context of fintech, these arrangements for early intervention are particularly important. It is essential for supervisory authorities to integrate fintech-related risks into their early intervention frameworks and to develop contingency plans for dealing with stress events involving fintech matters. Examples of where early intervention arrangements are especially important are fintech risk events that threaten the financial or operational soundness of a financial institution or financial stability. Of particular relevance in this context are operational risks arising from fintech, such as cyberattacks that threaten a financial institution's operational soundness or pose a threat to payment system functionality, the emergence of high-risk lending and payment system activity in non-bank financial intermediation, and financial conduct that threatens the integrity of the financial system (such as money laundering and other financial crimes).

In these examples, it is important for the supervisory authorities to identify the triggers for different stages of early intervention and the response strategies they would apply to breaches of triggers. They should also develop and regularly test contingency plans for dealing with such risk events. In some cases, the fintech-related risk events would be able to be addressed through existing early intervention frameworks. However, in some areas, such as cyberattacks, modifications to existing early intervention frameworks and contingency plans may be necessary so as to incorporate specific responses to deal with the impact of the events and to facilitate effective remediation.

Part of the early intervention framework should include a requirement for a regulated entity to maintain and regularly test its own contingency plans for dealing with distress events. Typically, a bank, for example, would be required to have a liquidity contingency plan, a capital contingency plan and a business continuity plan. In addition, following the global financial crisis, banks in most countries have also been required to have recovery plans that set out comprehensive strategies for enabling a bank to restore itself to financial and operational soundness following (or in anticipation of) a severe financial or operational shock. Supervisory authorities should include in their early intervention frameworks a requirement for such plans to be activated and implemented upon defined triggers being breached.

In a fintech context, there is a need to ensure that financial institution contingency plans, including recovery plans, adequately identify fintech-related risk events and set out the strategies for responding to them. In some cases, fintech risk events can be integrated into existing contingency and recovery plans with only minor modifications. However, in the case of some fintech, especially ones that expose an institution to cyber risks and payments system network risks, there is a need for significant new response strategies to deal with such threats. The responses will include the initiatives needed to maintain critical functions and services, undertake capital and liquidity restoration, address stakeholder concerns, remediate reputation risk, and ensure that the underlying causes and vulnerabilities have been remedied. Supervisory authorities need to oversee these arrangements and ensure that recovery plans and other contingency plans are subject to regular testing.

Crisis Preparedness

When early intervention and recovery actions are insufficient to remedy a risk event, there is a need for the authorities to have the capacity to undertake some form of resolution. This might involve the appointment of a statutory manager or administrator to a financial institution in acute stress to implement remedial actions that the board and management are either unable or unwilling to undertake and to identify possible resolution options. It will also likely involve the authorities having the legal powers, policies and procedures to implement a specific resolution option if the financial institution is deemed non-viable. This could involve transferring critical functions and systems, associated assets and liabilities, to another (viable) entity or to a "bridge entity" established for the purpose by the resolution authority. It might involve some form of recapitalisation, such as the use of contractual or statutory bail-in of unsecured liabilities. Or it might involve an unwinding of the institution's business in an orderly and non-disruptive manner.

Since the global financial crisis, financial authorities globally have implemented a wide range of initiatives to strengthen the capacity to resolve a non-viable financial institution. These initiatives have been guided by the international standard on resolution issued by the Financial Stability Board—the *Key Attributes of Effective Resolution Regimes for Financial Institutions* (Key Attributes). Under this standard (which is non-binding but is encouraged by the IMF and World Bank through the FSAP process), resolution authorities are expected to have:

- a well-defined statutory mandate for the resolution of non-viable financial institutions, anchored to clearly stated objectives (generally anchored to financial stability);
- a resolution framework that applies to regulated entities, relevant holding companies and subsidiaries to enable a group-based resolution to be implemented;
- a broad suite of statutory powers with well-specified triggers to enable a range of resolution options to be implemented;
- the capacity to require a financial institution to prepare and maintain a recovery plan;
- the ability to undertake resolvability assessments and prepare a resolution plan for at least systemically important financial institutions;
- the maintenance of the ability to implement a range of resolution strategies, based on generic resolution policies and practices, and institution-specific resolution plans;
- safeguards to ensure that resolution actions are not used in an inappropriate manner, including a general requirement to ensure that no creditor is left worse off under a resolution than they would have been under a conventional winding up/liquidation under the relevant country's insolvency law.

To varying degrees, resolution authorities in many countries have implemented or are in the process of implementing resolution policies and practices, including institution-specific resolution plans, in broad alignment with the Key Attributes. This has typically included a strengthening of resolution-related laws, the development of generic resolution strategies, the undertaking of resolvability assessments of systemic institutions, and the development of resolution plans for such institutions. Domestic and

cross-border cooperation and coordination arrangements have also been strengthened for resolution purposes in many countries.

For the most part, these resolution frameworks have been designed to apply to mainstream banking (and to some extent, insurance and financial market infrastructure) without specific regard for fintech issues. What is likely to be needed in the next phase of implementation of resolution frameworks is the assessment of the extent to which fintech developments might change some aspects of resolution. In most respects, it is likely that the principles and practicalities of resolution will not be significantly altered by fintech. However, some aspects of fintech might require special attention in a resolution context. This is likely to be the case for non-bank financial intermediation to the extent that such institutions become systemically significant, either individually or collectively (e.g., due to network platform contagion risks). In this case, it will be necessary for the authorities in question to consider the need to develop effective resolution frameworks for application to non-bank financial institutions, such as mobile payment system providers and P2P platforms, so as to enable financial distress and failure events to be managed in a manner consistent with maintaining the stability of the financial system.

Similarly, it will be necessary for the authorities to assess the possible modifications needed to resolvability assessments and resolution plans to deal with cyber risk events where these cause a bank or other financial institution to become non-viable. In this case, consideration would need to be given to a number of factors, such as how cyber risk-impacted critical functions and services can be restored to a secure and viable state, either within the existing financial institution or by being transferred to another entity or via secured backup systems. Similarly, consideration will need to be given to how FMI resolution strategies would be implemented in a situation where one or more FMI providers has been severely impacted by a cyber risk event. These issues raise an important question as to the adequacy of operational risk firewalls between different entities in financial conglomerates and FMIs, and how critical functions and systems can best be protected from cyber risk events that originate in non-critical systems, but which could be transmitted to critical functions and systems.

These are still relatively new and evolving issues. It will take time for the authorities to assess the implications of fintech for resolution strategies, resolvability assessments and resolution planning. However, it will be increasingly important for fintech issues to be factored into resolvability assessments and resolution planning, given the increasing threat posed by cyber risk and some other fintech developments.

6. Conclusion

This paper has looked at the tools available to regulatory and supervisory authorities to strengthen the regulation and supervision of fintech in areas where fintech risks pose a potential threat to financial stability and to consumers of financial services. In doing so, four key themes have emerged.

First, a carefully considered balance needs to be drawn to embrace the benefits of fintech while addressing the potential risks. An appropriate balance needs to be struck between the promotion of financial stability, on the one hand, and financial system efficiency and innovation, on the other. This suggests the need for financial supervisors and regulators to further deepen their understanding of the benefits and risks associated with fintech across the financial system, to have a clearly defined public policy rationale for regulatory intervention, to have well-specified regulatory objectives, and to ensure that a proportionate regulatory response is applied based on robust cost/benefit analysis. In this context, it is important that regulation of financial services is based on sound principles of competitive neutrality and consistency, such that similar types of financial services and entities are regulated on a consistent basis—i.e., "substance over form".

Second, the use of Regtech and Suptech could improve supervision and support forward-looking, judgement based, supervision and policymaking. However, in order to be able to achieve this, supervisory authorities need to strengthen the skill sets of supervisors, and to continue to enhance their approaches to risk-based supervision. Regtech and Suptech should not be seen as substitutes for conventional supervision. These new technologies need to be harnessed in ways that supplement and strengthen existing risk-based supervisory frameworks, and where supervisory judgement remains a key factor in achieving desired regulatory outcomes.

Third, a key element in the effective regulation of fintech will be the promotion of robust governance and risk management frameworks in providers of financial services—whether they be mainstream financial institutions or newly established digital financial service entities. This will include the need for regulators to place emphasis on the quality of financial institution boards, risk management frameworks, internal audit, stress testing arrangements, and contingency plans.

Fourth, further attention needs to be given to how financial authorities respond to emerging stress and institutional non-viability in a digital environment. This is especially relevant for non-bank financial intermediation, which could increasingly pose a risk to financial stability, and cyber risks, which are an increasing potential threat to financial institution viability and financial stability. In this context, financial authorities need to pay particular attention to their early intervention frameworks for dealing with emerging stress and resolution arrangements for addressing institutional non-viability, with particular focus on the strategies for dealing with risk events associated with fintech, such as severe cyber attack scenarios and stress events in under-regulated non-bank financial intermediation.

References

Adrian, T., & Mancini-Griffoli, T. (February 2021). *Public and Private Money Can Coexist in the Digital Age*.

Andolfatto, D. (2018). *Assessing the Impact of Central Bank Digital Currency on Private Banks*. Federal Reserve Bank of St. Louis Working Paper 2018-026C. https://doi.org/10.20955/wp.2018.026

Auer, R. (2019). Beyond the Doomsday Economics of "proof-of-work" in Cryptocurrencies. In *Bank for International Settlements, Working Paper no. 765*. https://doi.org/10.24149/gwp355

Bank for International Settlements. (April 2022). *CBDCs in Emerging Market Economies*.

Bech, M. L., & Rodney, G. (2017). *Central Bank Cryptocurrencies*. Bank for International Settlements Quarterly Review.

BigTech Firms in Finance in Emerging Market and Developing Economies: Market developments and potential financial stability implications. (October 2020b).

Board, C., & Wehrli, A. (2021). Ready, steady, go?—Results of the third BIS survey on central bank digital currency. In *Bank for International Settlements, Working Paper no. 114*.

Crisis Binder. (October 2019).

Designing and Implementing a Systemic Financial Crisis Management Simulation. (March 2020).

Financial Stability Board. (February 2022). *Assessment of Risks to Financial Stability from Crypto-assets*.

Financial Stability Implications from FinTech Supervisory and Regulatory Issues that Merit Authorities' Attention. (June 2017).

FinTech and Market Structure in the COVID-19. (March 2022).

Guide to Supervision in the COVID-19 World. (September 2020).

International Monetary Fund and World Bank Group. (October 2018). *The Bali Fintech Agenda: A Blueprint for Successfully Harnessing Fintech's Opportunities*.

OECD. (February 2020). *Digital Disruption in Banking and its Impact on Competition*.

Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements Final Report and High-Level Recommendations. (October 2020c).

Statista. (2020). *Share of selected payment methods as percentage of total e-commerce transaction volume worldwide in 2020, by region*.

The future of monetary system BIS Annual Economic Report. (June 2022). III.

The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions Market developments and financial stability implications. (October 2020a).

Toronto Centre. (August 2017). *FinTech, RegTech and SupTech: What They Mean for Financial Supervision*.

Notes

Note 1. *In this paper, we use the FSB definition of Fintech: "Technologically enabled innovation in financial services 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."*

Note 2. *Toronto Centre (2020)*

Note 3. *Toronto Centre (2017)*

Note 4. *Auer (2019)*

Note 5. *Financial Stability Board (2020b)*

Note 6. *Adrian & Mancini-Griffoli (2021)*

Note 7. *Financial Stability Board (2020c)*

Note 8. *Condruta and Wehrli (2021)*

Note 9. *Financial Stability Board (2017)*

Note 10. *Statista (2020)*

Note 11. *1 Financial Stability Board (2020a & 2020b)*

Note 12. *International Monetary Fund and World Bank Group (2018)*