TC NOTES

PRACTICAL **LEADERSHIP**
AND **GUIDANCE** FROM
TORONTO CENTRE

SUPERVISING FINTECH TO PROMOTE FINANCIAL INCLUSION

DECEMBER 2019

TORONTOCENTRE
Global Leadership in Financial Supervision

SUPERVISING FINTECH TO PROMOTE FINANCIAL INCLUSION

TABLE OF CONTENTS

SUPERVISING FINTECH TO PROMOTE FINANCIAL INCLUSION

Introduction[1]

This Toronto Centre Note discusses how financial regulation and supervision can enhance the benefits of fintech[2] for financial inclusion and gender equality, taking into consideration the roles of incumbent financial institutions and new entrants, the roles of supervisors and regulators, and the varying experiences of different jurisdictions.

This Note is based in part on a round-table discussion hosted by Toronto Centre during the IMF and World Bank Group annual meetings in October 2019. It addresses three main issues:

First, the potential impact on financial inclusion and gender equality from the adoption of various types of fintech, including access to financial services through mobile money services, more efficient retail payment systems, the availability of credit for micro enterprises, the availability of insurance for individuals and for smallholders in rural areas, and the introduction of digital identification.

Second, the risks inherent in fintech-enabled financial services, including greater exposure to cyber attacks, risks to consumer protection and risks to data privacy and security.

Third, the supervisory and regulatory responses to fintech and the need to achieve a sound, sustainable and consumer-centric development of fintech so that fintech can contribute effectively to financial inclusion and gender equality.

Financial inclusion and gender equality

Financial inclusion, the gender gap, and the potential for fintech to enhance financial inclusion have been discussed in previous Toronto Centre Notes (Toronto Centre 2018a, 2019a and 2019b).

Although financial inclusion is increasing, there is still a long way to go in many countries, and in particular in emerging economies. There remains a significant and persistent gender gap in many emerging economies - women's financial inclusion has remained 9 percentage points below men's in emerging economies between 2011 and 2017 (World Bank (2018)). In some countries this gap has even widened.

Greater financial inclusion, including in particular of women, depends not just on fintech but also on changing the laws, cultures and practices that may limit or preclude access by women to financial services and their broader participation in society and labour markets.

---

[1] This Note was prepared by Clive Briault.

[2] This Note follows the Financial Stability Board definition of fintech as "technology-enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on the provision of financial services". https://www.fsb.org/work-of-the-fsb/policy-development/additional-policy-areas/monitoring-of-fintech/

Benefits of fintech, especially for financial inclusion

Fintech has delivered – or has the potential to deliver – benefits to financial inclusion and gender equality through multiple channels. Some of the most significant benefits have so far been limited to a small number of countries, but there is scope for this to expand over time. In other cases, the innovations are at an early stage of development or realisation.

Technology enabled access to financial delivery mechanisms

Mobile money services (for basic savings and payment services) and the ability to use local agents/access points offer potential benefits in terms of greater access to financial services for a wider population. This brings benefits to previously unbanked and under-served populations and regions, and improves the safety and timeliness, and reduces the cost, of payment systems.

Similarly, households and micro, small and medium sized enterprises may benefit from greater access to credit through crowdfunding and peer to peer lending, and greater access to insurance. The use of alternative data from online transactions and payments, government databases and payment of utility and mobile bills could improve loan and insurance underwriting, and enable borrowers with no credit history to access credit and individuals and micro enterprises to access insurance.

The impact of mobile phones and other electronic delivery mechanisms on the availability of financial services to individuals, households and micro and small enterprises is the most advanced and widespread contribution of fintech to financial inclusion.

This has been particularly true in Sub-Saharan Africa, the global leader in the use of mobile money. Mobile money accounts are particularly widespread in Kenya, where 73 percent of adults have one, as well as in Ghana, Tanzania, Uganda and Zimbabwe.

Mobile money accounts have spread geographically to many other countries in West Africa and beyond, and are spreading to the provision of other types of financial products and services such as credit, insurance and investment in government bonds and other securities.

These experiences demonstrate how fintech can help emerging economies to increase financial inclusion through by-passing traditional financial services providers, or by partnering with them.

Emerging economies are usually less burdened by complex legacy systems than are developed economies. However, countries have very different positions in terms of financial inclusion and the nature of their financial systems. For example, in some countries state-owned and other banks have already been providing products and services for people who might otherwise have been financially excluded, and retail payment systems have already been developed by incumbent banks. It might be difficult for fintech players to break into this space.

Technology enabled improvements to the safety of financial services

Distributed ledger technology[3] has the potential to improve collateral and security arrangements by recording property rights (land registries) and ownership of other forms of security (such as movable assets), and generally to increase the transparency and integrity of data, in particular through the provision of an immutable audit trail.

Distributed ledger technology is also usually the platform for various types of crypto assets, offering the potential also to use crypto assets for domestic and international payments.

In addition, increased transparency of financial transactions and less use of cash for payments could reduce the scope for corruption and money laundering.

Big Data and data analytics

The greater availability of data and the ability to analyse these data (including gender disaggregated data) offer the potential for better informed credit and insurance underwriting decisions, by both existing players and new entrants (as already seen in crowdfunding and peer to peer lending). This often relies on cloud computing to store and process the data. Cloud computing is particularly important for smaller fintech companies without the money to invest on their own infrastructure.

Artificial intelligence and machine learning technology can be used to provide consumers with more interactive comparison websites, clearer information on financial products and services and how they can be accessed, and automated advice, all of which could enhance understanding of and access to financial products and services. They also provide financial institutions with new ways to monitor for signs of money laundering and market abuse.

Know Your Customer

Know your customer (KYC) requirements can be simplified through the use of digital (biometric) identification, making it easier to access financial services. Providing digital identification and an electronic means of KYC is important for individuals to be able to define who they are in digital space.

Competition

Reduced barriers to entry and greater market contestability should encourage and facilitate innovation, increase consumer choice, expand the offering of new customised products and services to segments of the market that were previously underserved, and increase access to high-quality and good value financial products and services.

Supervision

Supervisors can use fintech to monitor financial institutions more effectively and efficiently

[3] A distributed ledger system is a database shared between multiple parties to record information or to execute mutually agreed-upon transactions based on some consensus mechanism.

(Suptech)[4], while regulators and supervisors can cooperate more closely in designing standards and oversight practices, both domestically and internationally.

Fintech risks

For all its actual and potential benefits, fintech also poses risks. Fintech could pose mis-selling and data privacy risks to consumers; undermine the business model viability of some incumbents; increase technology risk, cyber security risk and other operational resilience risks; lead to an increasing reliance on third party suppliers; and there may be a lack of board and senior management understanding (in both financial institutions and supervisory authorities) of some aspects of fintech (in particular around the use of artificial intelligence and machine learning).

Some of the risks of fintech may be even higher in those emerging economies where supervisory and regulatory capacity is low and where legal frameworks are weak.

Cyber security

Vulnerabilities arising from the use of technology may threaten the feasibility or business model case for at least some fintech applications, for both incumbent financial institutions and new entrants.

The increasing use of technology, big data and artificial intelligence, and the increasing complexity and interconnectedness of financial systems (arising from digitalisation, customer access, open banking and other forms of third party access, and systems interoperability), create vulnerabilities both to cyber attacks and to a lack of operational resilience.

Cyber attacks can be made by a variety of players, including disaffected employees, criminal gangs, state-sponsored agents and bored teenagers, and can take a variety forms, ranging from disruption of service to the theft of assets. Meanwhile, software bugs, conflicts between different systems and other types of system failure can cause serious disruption to the operations of a financial institution such as website failures, the inability of customers to access their accounts online, and the closure of ATMs.

Cyber attacks and other operational resilience failures can limit the ability of customers to access services, products and even their cash and other assets; and can expose customers and financial institutions to various types of fraud and to the loss or manipulation of data. This can be exacerbated when financial institutions lack the ability to recover and respond effectively when operational failures do occur.

Indeed, improvements in cyber security and in operational resilience may not be keeping up with the threats and risks, thereby increasing the possibility that various types of failure could undermine confidence in specific fintech applications or even in fintech more generally.

Outsourcing

Although financial institutions have outsourced parts of their operations to third parties for many years, this has accelerated in response to the continuously increasing use and complexity of information technology.

In part this reflects the natural economies of scale in technology and in the handling of data,

[4] Toronto Centre (2018b).

while large service providers may also benefit from their understanding of technology and their ability to protect themselves against cyber security risks. This makes it commercially attractive for financial institutions to outsource functions to specialist third party providers.

However, this also generates risks. The financial institutions undertaking the outsourcing may not understand fully the services being provided by third parties, and may not be well placed to monitor and control this outsourcing. While these financial institutions remain responsible for the functions they outsource, this responsibility may therefore prove to be more in name than in substance.

Supervisors may also find it difficult to assess and respond to the risks arising from outsourcing, especially to unregulated service providers and to service providers located in foreign jurisdictions. This may be most pronounced for financial institutions and supervisors in emerging economies, where issues of 'reach' to service providers may be most intractable.

Meanwhile, the increasing concentration on a small number of large and globally active third party providers (for example in the provision of cloud computing) may generate concentration risks and risk to financial stability (Financial Stability Board (2019b)).

Managing change

Incumbent financial institutions, new players and supervisors all face challenges in managing change and in understanding the risks arising from fintech developments.

Incumbent financial institutions may seek to improve and reduce the cost of their existing financial products and services, and to expand the range of products and services they offer through the adoption of fintech developments. However, this is often hampered by legacy systems that may not be inherently unsatisfactory but are expensive to maintain, expensive to replace entirely and difficult to run alongside more modern systems.

In addition to this challenge in merging old and new technology, the boards and senior management of incumbent financial institutions may not understand fully the complexities of new technology and the implications of the increased use of big data, artificial intelligence and cloud computing, and may not put in place the necessary controls and risk management.

Innovative start-ups use new technology to create novel financial products and services or to provide existing products and services in new and lower cost ways. These firms are typically small, innovative and have a very strong growth focus. Their operations may be difficult for supervisors to understand, and they may not have an approach and mindset centred on the importance of good governance, risk management, financial soundness and long-term stability.

This could manifest itself in an inadequate level of cyber security and of IT security more generally, with this becoming more pronounced if these start-ups experience rapid growth. Start-up firms also often rely heavily on outsourcing to third party providers and cloud services.

BigTech firms are using use their advanced technology, data handling and existing customer base as the platform for a move into financial services (Financial Stability Board (2019a)). Given the extensive reach of BigTech firms, the impact of a movement into financial services could come with both high speed and a large scope. This is something that

supervisors need to assess carefully on a continuous basis.

Consumer protection

Risks to consumers from fintech can take various forms, including misconduct, fraud, data mis-handling and financial exclusion.

Mis-selling – although fintech can be used to provide financial products and services more effectively and efficiently, and to provide products and services that are better aligned to customer needs, fintech also provides new ways for financial institutions to mis-treat their customers. Such mis-treatment could take the form of pressure selling through digital channels and social platforms to sell poor products to poor people, and using actual or apparent complexity to increase the asymmetry of information and understanding between financial institutions and their customers.

Mis-advising – innovations such as robo-advice are only as good as the data and programming on which they operate. Financial institutions may be tempted to rig the process in their favour by asking for incomplete information and by programming machines to recommend their own products and services.

Complaints handling – new fintech entrants may not have the organisational structure to handle complaints effectively, while the increasing fragmentation of product and service providers (for example through open banking and a more modular approach to banking and insurance) can lead to lack of clarity as to who is responsible.

Financial exclusion and discrimination - big data analytics and artificial intelligence tools could make insurance cover and credit more difficult to obtain or more expensive for some consumers. This could be exacerbated by model biases. Meanwhile, some consumers may be excluded through the increasing use of technology to which they do not have access and by the reducing use of cash.

Data privacy and security - consumers are vulnerable to the loss and mis-use of data, and are unlikely to understand fully the ways in which their data are being used. Traditionally, financial institutions have sought to protect and use their own customers' data, under well-established legal and regulatory frameworks in some countries. In contrast, social media firms regularly collect and sometimes share extensive data from their users (with their consent). The fintech future envisages the gathering of a broad range of financial and non-financial data from, and sharing across, a wider set of parties. A more intense debate can be expected about whether there are appropriate frameworks for the gathering, storing and sharing data, both domestically and cross-border.

Reduced competition - economies of scale in the use of technology and data may lead to increasing concentration among a small number of large financial institutions and BigTech companies, harming consumers through high prices and a reduced choice of products and services.

Fraud and scams – the use of digital channels, and in particular social media, increases the scope for attempted frauds and scams on unsuspecting and vulnerable consumers.

Financial stability

The main threats to financial stability arising from fintech relate to the disruption of existing market structure and infrastructure; concentration risk (the emergence of new market

concentrations and monopolies, from either incumbent players becoming even larger, or from the entry and dominance of BigTech companies); the emergence of alternative channels of financial intermediation; herd-like behaviours (for example where trading firms use and follow similar algorithms); the potential growth of crypto assets; and the potential system-wide impact of cyber security and other risks to operational resilience.

Regulatory and supervisory responses

There is a growing supervisory interest (from prudential, retail conduct, wholesale conduct and AML supervisors) in the use of fintech innovations by financial institutions. Some of the underlying themes are already familiar from earlier supervisory initiatives on outsourcing, cyber security and risk management, but supervisory concerns and responses are beginning to extend further.

Regulatory and supervisory responses to fintech

Regulators and supervisors have begun to introduce regulatory requirements and supervisory expectations relating to various aspects of fintech, including:

Regulatory perimeter – many countries have revisited, or are revisiting, the regulatory perimeter, to clarify and extend the regulatory perimeter to cover at least some new and previously unregulated types of financial instrument or financial activity (for example, crypto assets and financial instruments that reference crypto assets, and crowdfunding and peer to peer lending). This in turn has implications for the authorisation or licensing of new fintech-based financial institutions, and for the need for these firms and platforms to meet the minimum authorisation criteria for senior managers, systems and controls, resources and ownership.

Sandboxes – some supervisors are using sandboxes and innovation hubs to test fintech applications, to identify and address risks in a constrained environment, and to act as a first point of contact for companies that are unsure about the applicable regulations (Toronto Centre (2017)).

Governance and risk management – supervisors are focusing increasingly on how financial institutions identify, monitor and manage the risks to them arising from fintech, including strategic, operational, compliance, cyber security and outsourcing risks.

Supervisors are assessing how well the boards and senior management of financial institutions understand fintech applications and the risks arising from them; how well they embed fintech opportunities in their strategic and business planning; how they operate new product approval processes; how they manage operational and outsourcing risks; and how they monitor and review the impact of fintech on their compliance with applicable regulatory requirements, including those related to consumer protection, data protection and anti-money laundering.

Consumer protection – traditional consumer protection requirements are being extended to fintech applications, including transparency and disclosure requirements; risk warnings to consumers; prohibitions or limits on the sale of some products to retail investors (for example crypto assets and derivatives referencing crypto assets, and restrictions on funders of lending platforms according to the wealth and sophistication of the investor); client money segregation; complaint handling and redress procedures; and prudential requirements to establish various types of default or loss funds.

Data privacy and security – supervisors and other relevant authorities are focusing increasingly on disclosure of the types of data used by financial institutions; on measures to enable consumers to understand better how a financial institution is using their data and to be able to grant or withdraw permission for personal data to be used; data protection legislation; and data protection constraints on sending data across national borders.

Data and artificial intelligence – supervisors are focusing on how well financial institutions control and mitigate the risks arising as they make increased use of artificial intelligence and machine learning, not least in terms of governance, the level of understanding of how artificial intelligence drives business decisions, and relationships with third party providers. In addition, and extending across all sectors, not just financial services, increasing attention is being paid to ethical, legal and societal issues relating to artificial intelligence, machine learning and the use of big data (see for example European Commission (2019)).

Anti-money laundering – the Financial Action Task Force has published guidance on the money laundering threats arising from the use of crypto assets (Financial Action Task Force (2019)).

Outsourcing – in response to the increasing reliance of financial institutions on outsourcing, the difficulties faced by these firms in checking the activities of third party providers and the potential for a small number of concentrated providers to pose a risk to financial stability, some supervisors are beginning to consider not only the revision of their outsourcing rules and guidelines (European Banking Authority (2017)), but also the introduction of an oversight framework for monitoring critical service providers, in particular cloud computing providers (European Supervisory Authorities (2019)).

Cyber security – various national regulatory and supervisory authorities have launched initiatives on cyber security, based in part on international standards[5]. Supervisory authorities are already considering cyber security risk as an additional risk separate from operational risk that requires special attention. The focus here is on the key elements of cyber security:

Preparedness – governance, workforce skills and capabilities

Risk identification – risk analysis and assessment

Protection – information security, security controls and incident prevention, expertise and training

Detection – monitoring, penetration testing

Incident response – incident response and recovery, and the sharing of information domestically and internationally across the relevant authorities and with other financial institutions.

Operational resilience – outsourcing and cyber security are two examples of a wider trend towards supervisors focusing increasingly on the ability of financial institutions not only to prevent operational failures from occurring, but also to respond and recover effectively and quickly if and when such failures do occur.[6]

Suptech – supervisors are increasingly using fintech to improve supervisory efficiency and effectiveness, including the regulatory reporting process and the supervisory analysis of data

[5] Toronto Centre (2018c) and World Bank (2019).
[6] See, for example, Bank of England (2018).

and other information (for example to detect outlier regulated firms and suspicious trading patterns).[7]

Improvements in cyber risk management, financial inclusion and fintech can reinforce each other. Many infrastructures established to promote financial inclusion and fintech can also support improved cyber risk management, for example digital identification for companies, including small and medium enterprises; digital KYC mechanisms to facilitate electronic access to readily available information; improving the resilience of wholesale and retail payment infrastructures; and strengthening the digital ecosystem more generally.

Differences across countries

When applying these regulatory and supervisory responses to fintech, each supervisory authority usually claims that it is trying to strike the right balance between facilitating and encouraging fintech, remaining 'technology neutral', and responding to the various risks it has identified. However, the details of these regulatory and supervisory responses have differed significantly across countries. This may reflect:

- The different types of fintech developments and applications emerging in each country.
- Different levels of supervisory capacity, in terms of resources, expertise and training.
- The absence of international standards in many of the areas where national regulators and supervisors are formulating their responses to fintech developments.
- Different strategic approaches or attitudes across countries towards fintech developments, based on different assumptions or policies with regard to the benefits and risks of fintech and to the possibilities for fintech to contribute to the development of the financial sector and to the economy more widely. For example, some countries have been more willing than others to encourage and facilitate the development of electronic payments, blockchain and crypto assets.
- Differences across countries in the extent to which financial inclusion has been achieved and in the extent to which financial inclusion is a key public policy objective. Some countries have a lot further to go than others to achieve financial inclusion and to ensure the provision of good and suitable financial products and services for poorer people. Some countries are therefore considering how actively they could or should encourage and facilitate financial inclusion through innovation, including through more lenient authorisation and licensing and more accommodative financial regulation, less onerous KYC requirements, the use of taxation and subsidies, and the provision of cheaper smart phones.

While this combination of different starting points and attitudes creates a virtual 'global laboratory' of approaches that financial sector supervisors can observe and learn from, it also highlights that there may be a need for greater international cooperation to ensure effective policy responses and to limit risks arising from divergences in national regulatory frameworks.

Next steps: tackling the remaining challenges

Fintech is happening. The inevitability of technological innovation requires supervisory authorities to be ready to respond to the emergence of new players, processes, products, services and distribution channels, and greater use of outsourcing. Supervisory authorities need to assess the sufficiency of their powers, resources and expertise; consider the

[7] Financial Stability Institute (2019).

adaptability/flexibility (or lack thereof) of existing regulations and guidance and of existing supervisory processes; and ensure their ability to remain aware of and respond to fintech developments.

As new firms have begun to offer financial services and thus perform economic functions in the financial system, the general approach has been to adopt a 'same activity, same regulation' approach, under which new entrants are regulated and supervised in much the same manner as the incumbent firms that perform the same, or similar, economic functions[8].

The benefits of digital financial inclusion can only be fully achieved where financial services, products and market infrastructure seize the opportunities provided by fintech; regulatory and supervisory responses to fintech-related risks are both proportionate and robust; and the adoption of fintech is inclusive and breaks down barriers to women's access to financial products and services.

Many difficult balances need to be struck in response to fintech developments. Regulators and supervisors are very aware of the balancing act in promoting the growth and benefits of fintech while at the same time addressing and mitigating the related risks.

Further debate and discussion are required to determine a workable and practical way forward:

- Achieving financial inclusion goals, competition and innovation, while maintaining adequate consumer protection, market integrity, prudential soundness and financial stability.
- Realizing the benefits of greater affordability and accessibility while maintaining trust in financial institutions and in the financial system more generally.
- Meeting different consumer preferences – users of financial services may have different views on the balance between data privacy and security concerns and the convenience and cost of financial products and services.
- Creating a level regulatory playing field that treats incumbent and new providers fairly – but the mantra of applying the same requirements to the same risks and activities becomes more complicated when new entrants (or indeed incumbent financial institutions) are using fintech to provide new or modified products and services, and to do so through new or modified distribution channels.
- Will the regulation and supervision of fintech-related activities be too restrictive? Perhaps not - the fintech sector has seen tremendous growth and innovation in the area of financial services, while the further development of fintech will depend at least as much on market forces as on regulation and supervision. Indeed, the market power of incumbent financial institutions may hamper fintech developments more than any regulatory and supervisory constraints.
- There are potential tensions between the development of international standards for fintech by countries that do not have a financial inclusion deficit and the preferred approaches of countries where financial inclusion is a pressing public policy issue.

[8] Although as noted by Restoy (2019) this 'same activity, same regulation' principle may need to be adjusted to take account of which firm is performing the activity, for example to take account of the possible systemic risks arising from BigTech companies.

References

Bank of England. *Building the UK financial sector's operational resilience*. July 2018. https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf

European Banking Authority. *Recommendations on outsourcing to cloud service providers.* December 2017. https://eba.europa.eu/eba-issues-guidance-for-the-use-of-cloud-service-providers-by-financial-institutions

European Supervisory Authorities. *Advice to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector*. April 2019. https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf

European Commission. *Ethics guidelines for trustworthy AI*. April 2019. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

Financial Action Task Force. *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. une 2019. https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html

Financial Stability Board*. BigTech in finance: market developments and potential financial stability implications*. December 2019. https://www.fsb.org/wp-content/uploads/P091219-1.pdf

Financial Stability Board. *Third-party dependencies in cloud services: considerations on financial stability implications*. December 2019. https://www.fsb.org/wp-content/uploads/P091219-2.pdf

Financial Stability Institute.*The suptech generations*. October 2019. https://www.bis.org/fsi/publ/insights19.pdf

Restoy, Fernando. *Regulating fintech: what is going on, and where are the challenges? Speech at the ASBA-BID-FELABAN XVI Banking public-private sector regional policy dialogue, Washington DC.* 16 October 2019*.* https://www.bis.org/speeches/sp191017a.pdf

Toronto Centre. *Regulatory Sandboxes*. October 2017. https://res.torontocentre.org/guidedocs/Regulatory%20Sandboxes%20FINAL.pdf

Toronto Centre. *Advancing Women's Digital Financial Inclusion*. January 2018. https://res.torontocentre.org/guidedocs/Advancing%20Womens%20Digital%20Financial%20Inclusion%20FINAL.pdf

Toronto Centre. *SupTech: Leveraging Technology for Better Supervision*. July 2018. https://res.torontocentre.org/guidedocs/SupTech%20-%20Leveraging%20Technology%20for%20Better%20Supervision%20FINAL.pdf

Toronto Centre. *Supervision of Cyber Risk.* September 2018. https://res.torontocentre.org/guidedocs/Supervision%20of%20Cyber%20Risk%20FINAL.pdf

Toronto Centre. *What Role Can Financial Supervisors and Regulators Play in Promoting Gender Equality and the Economic Empowerment of Women?* October 2019. https://res.torontocentre.org/guidedocs/What%20Role%20Can%20Financial%20Supervisors%20and%20Regulators%20Play%20in%20Promoting%20Gender.pdf

Toronto Centre. *Removing the barriers to women's financial inclusion.* November 2019. https://res.torontocentre.org/guidedocs/Barriers%20to%20Womens%20Financial%20Inclusion.pdf

World Bank. *The Global Findex database 2017*. April 2018. https://globalfindex.worldbank.org/

World Bank. *WB Financial Sector's Cybersecurity: A Regulatory Digest*. May 2019. http://pubdocs.worldbank.org/en/208271558450284768/CybersecDigest-3rd-Edition-May2019.pdf