



The Evolution of the Nature and Scale of DFS Consumer Risks A Review of Evidence



FEBRUARY 2022

Majorie Chalwe-Mulenga, Eric Duflos,
and Gerhard Coetzee

ACKNOWLEDGMENTS

The authors would like to thank the experts listed in the annex for providing invaluable feedback on this study. They are also grateful to Barbara Scola and Ivo Jenik for reviewing this slide deck, Juan Carlos Izaguirre for his insights, as well as Natalie Greenberg, Lamis Daoud, and Jahda Swanborough for their editorial support.

CONSULTATIVE GROUP TO ASSIST THE POOR

1818 H Street NW, MSN F3K-306
Washington DC 20433
Internet: www.cgap.org
Email: cgap@worldbank.org
Telephone: +1 202 473 9594
© CGAP/World Bank, 2022.

Cover slide: Photo for CGAP by Lorena Velasco via Communication for Development Ltd.

RIGHTS AND PERMISSIONS

This work is available under the Creative Commons Attribution 4.0 International Public License (<https://creativecommons.org/licenses/by/4.0/>). Under the Creative Commons Attribution license, you are free to copy, distribute, transmit, and adapt this work, including for commercial purposes, under the following conditions:










Attribution—Cite the work as follows: Chalwe-Mulenga, Majorie, Eric Duflos, and Gerhard Coetzee. 2022. “The Evolution of the Nature and Scale of DFS Consumer Risks: A Review of Evidence.” Slide Deck. Washington, D.C.: CGAP.

Translations—If you create a translation of this work, add the following disclaimer along with the attribution: This translation was not created by CGAP/World Bank and should not be considered an official translation. CGAP/ World Bank shall not be liable for any content or error in this translation.

Adaptations—If you create an adaptation of this work, please add the following disclaimer along with the attribution: This is an adaptation of an original work by CGAP/World Bank. Views and opinions expressed in the adaptation are the sole responsibility of the author or authors of the adaptation and are not endorsed by CGAP/World Bank.

All queries on rights and licenses should be addressed to: CGAP Publications, 1818 H Street NW, MSN F3K-306, Washington, DC 20433 USA;
e-mail: cgap@worldbank.org

TABLE OF CONTENTS

	Executive Summary.....	4		V. Special Focus: Overindebtedness of Digital Credit Users.....	37
	I. Benefits of Digital Financial Services (DFS).....	8		VI. The Path Forward: A Call to Action.....	41
	II. A New DFS Consumer Risk Typology.....	11		Annexes.....	47
	III. Evolution of the Scale of DFS Risks.....	16		References.....	64
	IV. Vulnerable Consumers and DFS Risks.....	31			

EXECUTIVE SUMMARY

The changing face of risks in digital financial services

Digital financial services (DFS) have undoubtedly delivered substantial financial inclusion benefits and contributed immensely to economic growth and development. Among the positive impacts DFS have on consumers are improved saving behavior, empowerment through greater privacy, and the ability to better weather shocks. At the same time, DFS have exacerbated existing consumer risks and continue to introduce new and ever-evolving risks, given the dynamic nature of financial technology. These risks undermine the delivery of DFS to underserved and low-income consumers and, if ignored, are likely to erode consumer trust in DFS.

Our objectives and methodology

In October 2020, CGAP started research to understand the **evolving nature and scale of DFS consumer risks** as part of our work in consumer protection.

The research seeks to identify new DFS consumer risks that have developed following the CGAP 2015 Focus Note, [Doing Digital Finance Right: The Case for Stronger Mitigation of Consumer Risks](#), and to create a risk typology consistent with these developments. We also wanted to get a sense of how much DFS consumer risks have increased or decreased in the past several years. We believe that this information is critical for stakeholders that are interested in building a responsible DFS ecosystem.

Recognizing that some customer segments are more vulnerable to DFS consumer risks than others, this slide deck highlights risks that affect vulnerable consumers, particularly low-income women and rural populations, and explores how overindebtedness may arise as an outcome of a combination of DFS risks.

The deck summarizes the findings of our research, which is based on a review of over 170 publications, along with consultations with 74 experts from 33 organizations, as detailed in the Annex.

EXECUTIVE SUMMARY

Who is the audience for this deck?

The deck aims to provide a comprehensive framework for various stakeholders, including policymakers, regulators, supervisors, funders, consumer organizations, and DFS providers on the evolution of the nature and scale of DFS consumer risks. Each stakeholder plays a role in building consumer awareness about risks and the capacity to avert these risks. The deck also outlines proactive measures stakeholders can take to mitigate risks and ensure that consumers maintain their trust in DFS.

DFS have introduced several new consumer risks, including mobile app fraud, synthetic identity fraud, authorized push payment scams, and artificial intelligence risks such as algorithmic bias. Concurrently, **preexisting consumer risks** such as SIM swap fraud, data breaches, social engineering scams, and Ponzi schemes **have become more complex**.

We have identified 66 DFS consumer risks which are grouped into:

- **Four broad risk types:** fraud, data misuse, lack of transparency, and inadequate redress mechanisms
- **Two cross-cutting risk types:** agent issues and network downtime

We considered other risk typologies, which are outlined in the annex, but settled on the chosen typology because of its simplicity.

It is worth noting that fraud, data misuse, and some network downtime and agent risks are directly linked to **cyber security**. Also, the two cross-cutting DFS consumer risk types – agent issues and network downtime – undermine the delivery of DFS to underserved and low-income consumers.

EXECUTIVE SUMMARY

Some risks are outgrowing technological progress and DFS adoption.

Based on available evidence, there has been a massive increase in the volume of records exposed. Fraudulent activity such as mobile app fraud, SIM swap fraud, account takeovers, and social media scams have also worsened. Anecdotal evidence additionally indicates that lack of transparency has deteriorated, while redress mechanisms show limited improvements in some countries.

50% of companies increased customer support in 2020, yet only **25%** of customers received quicker responses or were able to connect with customer service

Source: Experian Global Identity and Fraud Report, 2021.



Source: Statista (global data created); Risk Based Security “2020 Year End Report” (global number of records exposed).



Source: Outseer Fraud and Payments Report, Q1 2018 and Q2 2021.

EXECUTIVE SUMMARY

Low-income women and rural populations are likely to be more exposed to DFS consumer risks. While low-income women and rural segments face similar risks to other consumers, low levels of digital literacy and financial skills amplify their exposure to DFS risks. Rural women are the most adversely impacted. Women and rural populations experience risks that include agent fraud and failure to use complex phone interfaces. Social norms may also limit women's ability to complain about DFS issues. Women and rural populations are also more likely to share their phone or PIN with others. Due to the paucity of disaggregated data, we were unable to assess the evolution of risks that affect women and rural populations.

A combination of several consumer risks may lead to overindebtedness. Evidence shows that digital platforms such as mobile applications and peer-to-peer (P2P) lending platforms have exposed consumers to risks that lead to overindebtedness. Unauthorized digital lending apps and P2P platforms, which mimic genuine apps and platforms, intrusively obtain customer data and offer

desperate customers hassle-free but expensive digital loans. Agents then use abusive debt collection practices, such as social shaming, to pressure customers to repay their loans. Due to inadequate redress mechanisms, customers are unable to renegotiate their loans and must resort to negative coping strategies such as obtaining additional loans to repay existing loans or reducing food purchases.

There is an urgent need for proactive measures that maintain customer trust in DFS and ensure positive outcomes. Regulators and supervisors can develop systems to detect and monitor risks. They can also collect disaggregated data and develop coordination mechanisms to engage other sector regulators. Donors and investors can integrate consumer risk analysis in DFS project design. DFS providers can design customer-centric services that promote financial health and positive customer outcomes. Consumer groups can raise customer awareness and alert supervisors about risks while researchers can continue to fill the gaps this research has identified. For further information, see CGAP's [Market Monitoring Toolkit](#), [Collective Consumer Voice](#) research, and [Customer-Centric Guide](#).

I. BENEFITS OF DIGITAL FINANCIAL SERVICES (DFS)

DFS UNLOCK LIFE-CHANGING OPPORTUNITIES FOR CONSUMERS

DFS help consumers save, borrow, and receive remittances – reducing negative coping mechanisms

Positive impacts DFS have on consumers

- ✓ Improve saving behavior
- ✓ Empowerment through greater privacy
- ✓ Spend less money and time
- ✓ Better prepared to deal with shocks and recover faster
- ✓ Consumption smoothing

Source: Mastercard Foundation Evidence Gap Map.

A study in Uganda found that the probability of saving, borrowing, and receiving remittances increased by 25, 22, and 82 percentage points, respectively, in households that had a mobile money user (Munyegera and Matsumoto 2017). Another study found that women who received a microfinance loan on their mobile money account experienced 15 percent higher business profits and 11 percent higher levels of business capital (Riley 2019).

In Mexico, when the Oportunidades program switched its payment system from cash to electronic disbursements, remittance reception frequency increased and participation in informal saving decreased. The change also reduced the use of negative coping strategies such as reduced food consumption (Masino and Niño-Zarazúa 2014).

A randomized controlled trial in Bangladesh that introduced electronic wage payments to a population of salaried factory workers increased saving levels and the ability to cope with unanticipated shocks (Breza et al. 2017).

An assessment in Kenya of the uptake and impact of M-shwari, one of the world's most popular digital credit products, revealed that households that used M-shwari were 6.3 percent less likely to forego expenses due to negative shocks (Bharadwaj et al. 2019).

In Ghana, Tigo Family Care (Tigo), a “freemium” mobile insurance cover launched in 2010, facilitated the doubling of Ghana's insurance market in less than three years. By early 2013, Tigo had extended its basic life cover to 978,000 people, much higher than the 540,000 Ghanaians (5.4 percent of the country's adults) who had formal insurance in 2010 (Zetterli 2013).

DFS CAN EVEN INCREASE ACCESS TO ESSENTIAL SERVICES

But all these benefits can be undermined by risks. If ignored, risks are likely to erode consumer trust in DFS

Our research shows promising ways for digital finance to address development challenges.

Digital finance can foster efficiency and enable new business models, such as pay-as-you-go (PAYGo), which expand access by low-income households to essential services such as lighting, water, and cooking fuel (Waldron and Sotiriou 2019).

In Cote d'Ivoire, a pilot survey to assess the impact of a short-term digital education loan product delivered through cooperatives revealed it helped increase the rate of children starting school from 49 to 73 percent (Vidal and Barbon 2018).

However, the benefits of DFS may be undermined by risks which, if ignored, are likely to erode consumer trust in DFS.

Consumers have a lot to gain from DFS, but the opportunities they present are not without risks. Perceived consumer risks may discourage nonusers from embracing DFS. For users, risks that materialize may cause direct financial losses and other harms that erode their trust and confidence in DFS.

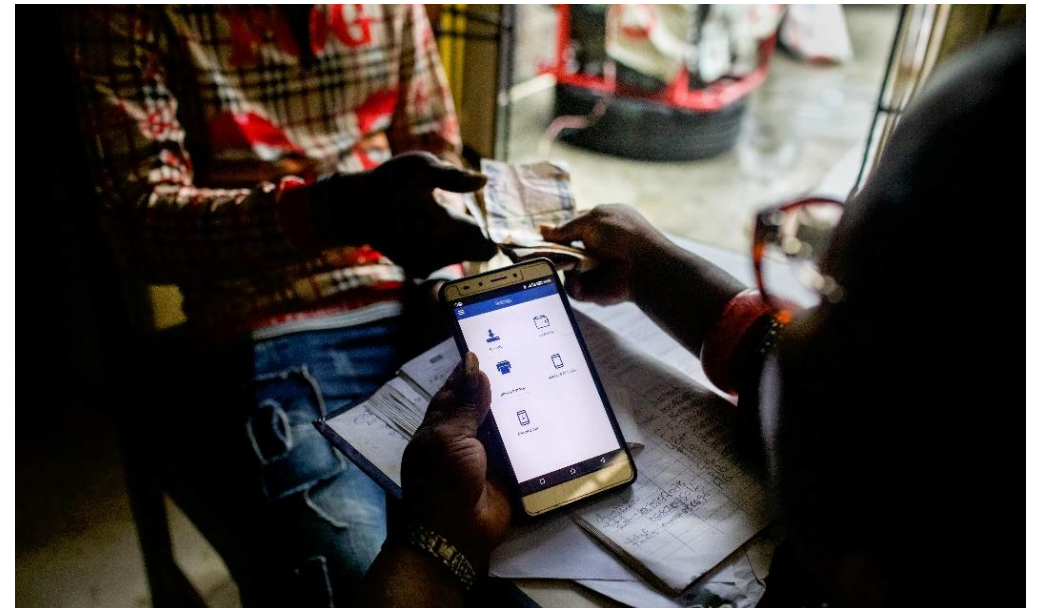


Photo for CGAP by Temilade Adelaja via Communication for Development Ltd.

II. A NEW DFS CONSUMER RISK TYPOLOGY

EXISTING RISKS HAVE BECOME MORE COMPLEX

DFS consumer risks have worsened over time

SIM swap fraud. While SIM swap fraud is a global issue, it is more frequently observed in developing countries (Farooq 2019). Although currently there is no global evidence to show the evolution of this risk, evidence from South Africa shows the increase in SIM swap fraud was higher than the mobile adoption growth rate (SABRIC 2019; World Bank DataBank).

Data breaches. There has been a massive increase in the number of records exposed over the past several years, associated with increased data generated from the use of social media and the internet of things. Based on available data, the increase in records exposed is growing at a faster rate than the rate of data creation.

Social engineering scams. Social engineering tactics are not solely limited to phishing (fraudulent emails that induce people to reveal personal information, which is then used to commit fraud), but also include smishing (phishing via text message) and vishing (phishing via voice call). Smishing and vishing are the main fraud vectors used to target low-income earners

who predominantly use mobile-based DFS platforms. Social engineering scams have been more prevalent over the past few years, especially during the COVID-19 pandemic (Medine 2020). Another growing social engineering scam that affects smartphone users is Quick Response (QR) code fraud, which happens when scammers temper with legitimate QR codes to steal customers' information and money.

Unlicensed digital investment/Ponzi schemes. The advent of cryptocurrencies has led to the emergence of cryptocurrency-based Ponzi schemes. These schemes usually persuade low-income earners who do not have the skills to use complex crypto platforms to transfer their funds to unscrupulous actors promising to invest in crypto assets on their behalf. Such schemes win the trust of low-income earners because they operate similarly to mutual aid networks (saving groups low-income people are used to).

Other risks include liability allocation risk, mis-selling, undisclosed fees, and abusive debt collection practices.

NEW DFS CONSUMER RISKS HAVE EMERGED

We identified five relative “newcomer” risks since since CGAP conducted DFS consumer risk research in 2015

1. Mobile app fraud. Given the increased adoption of smartphones, mobile app fraud is globally on the rise (RSA 2020; Fu and Mishra 2020a). Mobile app fraud occurs when a fraudster uses a malicious mobile application to deceive a customer. [Google’s Next Billion Users research](#) estimates that by 2025, there will be a billion more first-time smartphone users who likely have lower incomes and less formal education, live in less developed areas with more unreliable internet, possess limited exposure to technology, and have low confidence in how to use it. If deliberate actions are not taken to protect inexperienced users, more people will be exposed to mobile app fraud.

2. Biometric identity fraud. Biometrics are useful for risk mitigation. However, fraudsters can obtain copies of fingerprints or high-resolution pictures to access customer accounts, biometric data storage can be breached,

and legal limitations may lead to data misuse (Stolba 2020; Medine 2017). Europol (2020a) notes that “[in] the future, law enforcement and industry should expect to see an increased use of voice biometrics to commit impersonation fraud.”

3. Authorized push payment (APP) scams. An APP scam occurs when a fraudster tricks a consumer into sending money to a criminally controlled account. KPMG’s Global Banking Fraud Survey (2019b) notes that APP scams increased between 2015 and 2018 in every region of the world ([see slide 22](#)). The United Kingdom reported a 15 percent increase in the number of APP scam cases in 2020 (Michael and Smith 2021).

NEW DFS CONSUMER RISKS HAVE EMERGED

Five relative “newcomer” risks identified since CGAP’s 2015 research

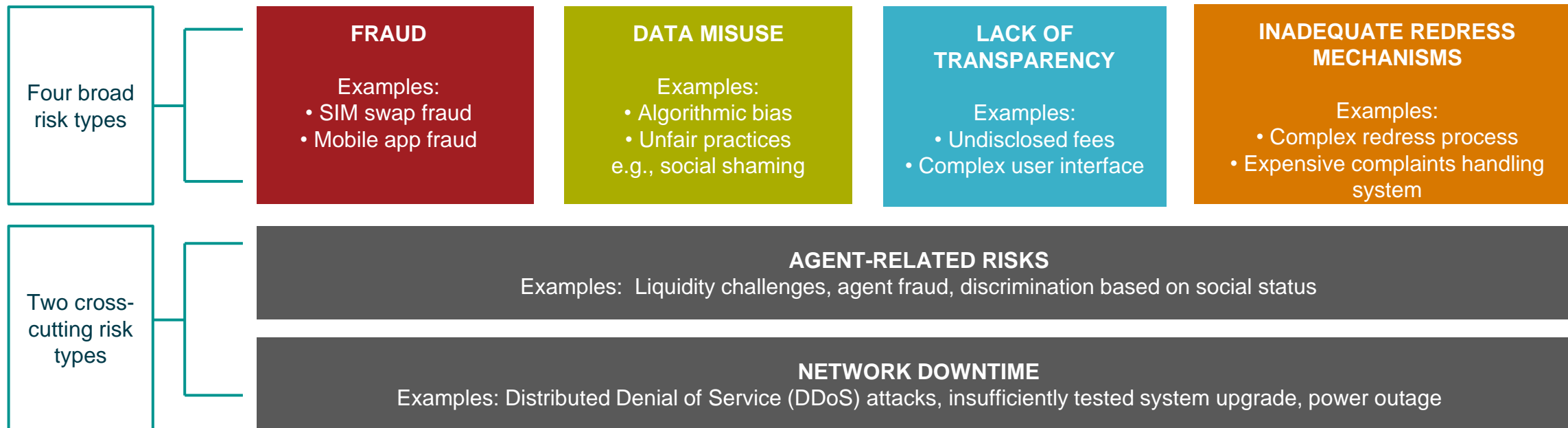
4. Synthetic identity fraud. Synthetic ID fraud happens when “new identities are made by blending elements from multiple individuals, making the uncovering of fraudulent transactions more complicated” (FICO 2018). This type of fraud is a problem that is growing in sophistication, intensity, and frequency (Aite Group 2021; FICO 2018). The Federal Reserve Banks (2021) recently developed a common definition to better equip financial services providers (FSPs) to identify and mitigate synthetic ID fraud. Synthetic fraud is worrying because unlike other types of fraud, it can simultaneously affect several customers but make it difficult to identify who has been impacted.

5. Artificial intelligence (AI)-related risks. While AI is not new, autonomous learning in AI has introduced newer risks for DFS users such as algorithmic bias/discrimination, mis-selling, privacy intrusion, and opaque decision-making (World Bank 2021; OECD 2020a, 2020b; Sahay et al.; Dvara Research 2020; Chugh 2019; Francis et al. 2017; Hurly and Adebayo 2017; European Commission 2016). Unfortunately, consensus currently does not exist on benchmarks that can be used to measure or assess AI’s relationship with broader societal discussions (Zhang, et al. 2021; Mishra et al. 2020).

THIS RESEARCH HAS ENABLED CGAP TO DEVELOP A NEW DFS CONSUMER RISK TYPOLOGY

CGAP categorization of identified DFS risks

Given the changing nature of DFS consumer risks, CGAP has identified **66 risks** and grouped them into **four broad risk types** and **two cross-cutting risk types**.












We also found that fraud and data misuse are directly linked to cybersecurity while lack of transparency and inadequate redress mechanisms have no direct link to cybersecurity. The two cross-cutting risks also share some elements with all four broad risks. Please refer to the annex for a detailed list of the 66 old and new risks identified, as well as definitions of the four broad risk types and two cross-cutting risk types.

III. EVOLUTION OF THE SCALE OF DFS RISKS*

* See further examples in Annex

THE SCALE OF DFS CONSUMER RISKS HAS INCREASED IN MOST CASES

Available evidence and data since 2015 show an increase in scale for most risk types identified by CGAP

Risk type	Global	Regions*	Country
1. Fraud*			
2. Data misuse			
3. Lack of transparency			N/A
4. Inadequate redress mechanisms**	N/A	N/A	

Red arrow: Available data show an **overall** increase in value or volume.

Orange arrow: Literature suggests an increase in value or volume without supporting data.

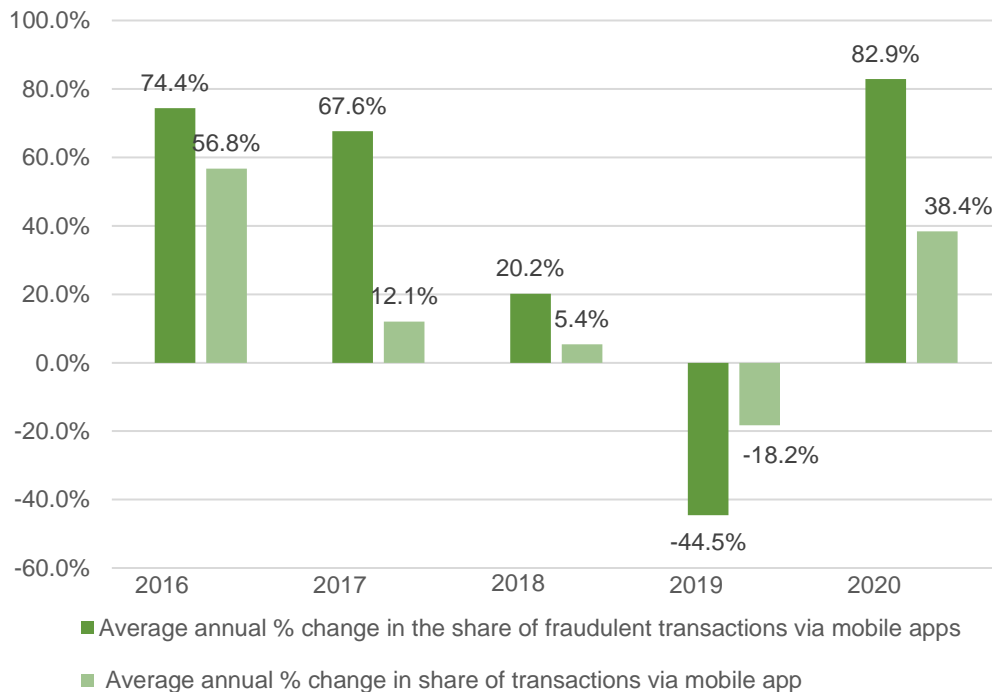
N/A: Reliable information and data are not available or sufficient to determine increase or decrease of the risk.

*Regions: Africa, East Asia & Pacific, Europe & Central Asia, Latin America & the Caribbean, Middle East & North Africa, South Asia.

**In some countries, there is evidence of improvements after government intervention (e.g. China and India).

MOBILE APP FRAUD* IS RISING FASTER THAN MOBILE APP USAGE

Percentage change in share of fraudulent mobile app transactions and share of mobile app transactions (globally)



Source: Adapted from the Outseer Fraud and Payments Report, Q2 2021, and RSA Quarterly Fraud Reports, Q1 2018 and Q3 2020.

Based on exploratory work using high-frequency mobile app data for 71 countries, Fu and Mishra (2020) note an increase in the scale and scope of fraudulent and predatory finance mobile apps over the past several years, especially during the COVID-19 pandemic.

Analysis of data from Outseer's** quarterly fraud reports indicates that between 2016 and 2020, the share of fraudulent transactions via mobile apps **increased by 104 percent** while the share of transactions via mobile apps **increased by 34 percent**. Consistent with Fu and Mishra's study, the increase in the share of fraudulent transactions and the increase in transactions via mobile apps were both more pronounced during the COVID-19 pandemic. Between 2019 and 2020, the share of fraudulent mobile app transactions **increase by 83 percent** while the share of transactions via mobile apps **increased by 38 percent**.

In the third quarter of 2020, rogue mobile apps became the primary source of fraud, overtaking phishing which had previously been the predominant attack vector (Spajić 2021; RSA 2018, 2020; Outseer 2021).

* RSA defined mobile app fraud as "mobile applications using an organization's brand without permission."

** Outseer is a new company created by RSA. The formal transition of RSA's fraud and intelligence business was officially announced on June 9, 2021. Before the new company was created, all the fraud reports were published by RSA.

MOBILE APP FRAUD IS RISING FASTER THAN MOBILE SMARTPHONE USAGE

An in-depth analysis of Android mobile money apps across 246 mobile money providers revealed that some branchless Android banking apps put users at greater risk than legacy systems do (Reaves et al. 2015).

Mobile app fraud incidents in South Africa's banking sector increased by over 90 percent between 2017 and 2018 while the number of smartphone users increased by 10.3 percent (Accenture 2020; SABRIC 2018; Statista 2021).

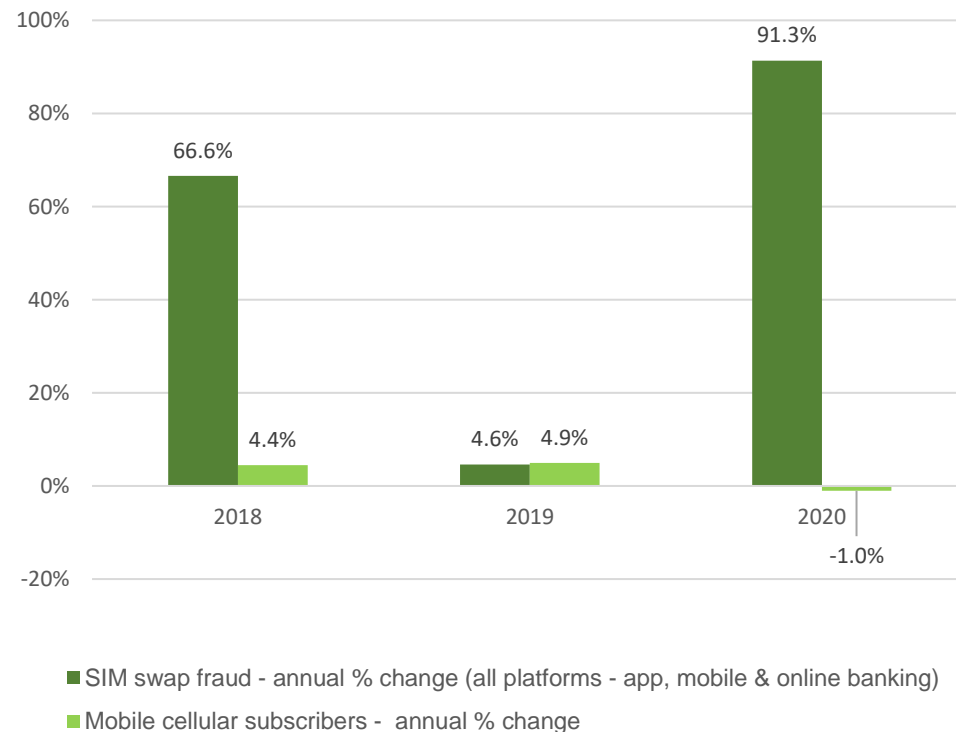
In India and Kenya, reports indicate that fraudulent and predatory lending apps have exposed digital credit customers to abusive lenders (Duflos et al. 2021; Mukharji 2021; Palepu 2021; Singh 2021a, 2021b; Faux 2020).



Photo for CGAP by Saiyna Bashir via Communication for Development Ltd.

ANECDOTALLY, SIM SWAP FRAUD IS INCREASING FASTER THAN MOBILE ADOPTION

Percentage change in SIM swap fraud incidents in South Africa (SA)'s banking sector and mobile cellular subscribers in SA: 2018–2020



Source: South African Banking and Risk Information Centre (SABRIC) 2018, 2019, and 2020 annual stats (SIM swap fraud); World Bank DataBank (mobile cellular subscribers).

SIM swap is a legitimate service offered by mobile network operators, enabling customers to move mobile details from one mobile device to another when changing or upgrading devices or changing service providers. SIM swap fraud occurs when a scammer initiates a porting request and takes control of a customer's mobile account, including services linked to the account such as mobile money or mobile banking. However, most countries do not publish SIM swap fraud statistics and published figures are sometimes unreliable (Priezkalns 2021).

“While SIM swap fraud is a global phenomenon, it is most frequently observed in developing countries.”

–Farooq (2019)

Between 2017 and 2020, SIM swap fraud incidents in South Africa (SA) increased by 233 percent while the number of mobile cellular subscribers increased by 8.4 percent (SABRIC annual reports 2018 & 2020; World Bank DataBank). In annual percentage terms, two of the three years analyzed recorded a larger increase in SIM swap fraud incidents than the change in mobile cellular subscribers. Of the three SIM swap fraud channels, mobile (i.e., via USSD) - often used by low-income earners - accounted for more than 90 percent of SIM swap fraud incidents in 2018 and 2019 and 88 percent in 2020 of all digital banking fraud incidents in SA.

SIM swap fraud has been reported in other countries, such as Mozambique, where the largest bank had a monthly average of 17.2 SIM swap cases, and Brazil, where 5,000 people fell victim to an organized SIM swap gang (Assolini and Tenreiro 2019).

THE RISE OF DIGITAL PONZI SCHEMES MAY IMPEND THE EXISTENCE OF GENUINE INVESTMENT SCHEMES

One of the most notable Ponzi schemes perpetuated in the last decade was Ezubao, a Chinese peer-to-peer (P2P) scheme that collapsed in 2015 after collecting over US\$9 billion from more than 900,000 investors. A recent study by Cheng et al. (2021) shows that Ezubao's collapse indirectly impacted other legal P2P companies.

Impact of the Ezubao P2P scheme (Cheng et al. 2021)

Indirect impact

- Exogenous shock to a legal P2P company, Renrendai.
- Loan amounts reduced while interest rates rose.
- All players (lenders, borrowers, and the firm) were affected.

The volume of digital Ponzi schemes continues to increase (ITU 2020). In developing and emerging markets, new schemes leverage cryptocurrencies, claiming to be mutual aid networks that mimic the informal savings groups and village banks that people in such markets are used to. Fund managers convince consumers who do not know how to operate crypto platforms to hand their funds over so the managers can invest in crypto assets on their behalf.

MMM, a scheme that originated in Russia, is another example. The scheme collapsed in 1994 but reemerged in 2011 with a global reach of 80 countries. It mainly targeted developing and emerging countries such as Colombia, Ghana, India, Indonesia, Nigeria, Ghana, and Zimbabwe (Solli 2019; Boshmaf et al. 2019; Chalwe-Mulenga and Duflos 2021). Other schemes include Africrypt "hack," which emerged in South Africa and involved approximately \$3.6 billion; Mirror Trading International (MTI), another South African scheme involving \$588 million and affecting over 260,000 investors globally; and Dunamiscoin Resources, which emerged in Uganda and closed in 2019 after collecting US\$2.7 million from 4,000 investors (Mureithi 2021; Henderson and Prinsloo 2021).

OTHER FRAUD TYPES HAVE ALSO INCREASED IN VOLUME AND VALUE, ESPECIALLY DURING THE COVID-19 PANDEMIC

Regional fraud trends between 2015 and 2018

Fraud Type	Americas	Europe, Middle East and Africa	Asia-Pacific
Authorized Push Payments (APP) scams*	↑ Increased	↑ Increased	↑ Increased
Card not present fraud	↑ Increased	↑ Increased	↑ Increased
Identity theft/impersonation/account takeover	↑ Increased	↑ Increased	↑ Increased

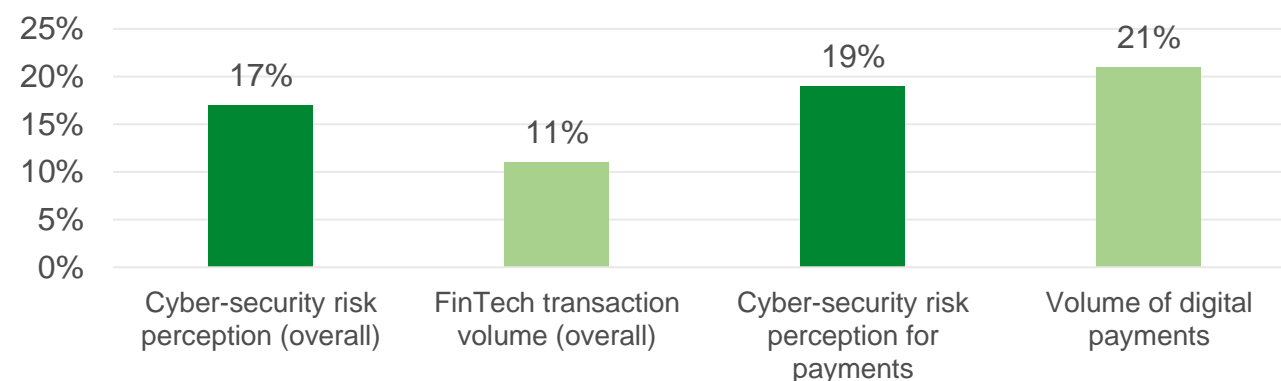
Source: KPMG Global Banking Fraud Survey, conducted across 43 retail banks between November 2018 and February 2019.

*APP scams happen “when a customer is coerced into transferring their money to an account controlled by the fraudster, on the pretext of them being a legitimate payee.”
Source: KPMG Global Banking Fraud Survey.

KPMG’s Global Banking Fraud Survey (2019b) notes that over half of survey respondents globally experienced increases in external fraud such as APP scams, card not present fraud, and identity theft.

The Global COVID-19 FinTech Market Rapid Assessment Study indicates that for all products surveyed, cyber security risk perception grew at a higher rate than transaction volumes (except for payments). The study further notes that cyber security risk perception was higher in emerging and developing economies (21 percent) than in advanced economies (16 percent).

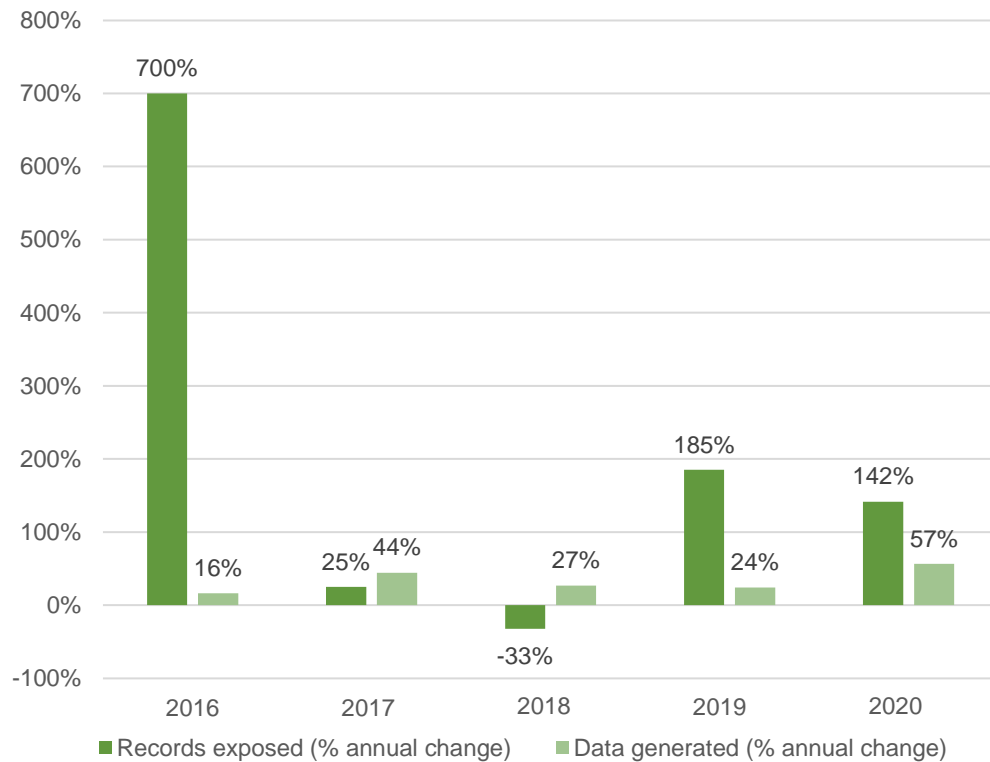
Fintech industry growth vs cyber risk perception, YoY percent change: July 2019/July 2020



Source: CCAF, World Bank Group, and WEF, 2020, The Global COVID-19 FinTech Market Rapid Assessment Study, a survey of 1,385 fintech firms operating in 169 jurisdictions.

INCREASE IN DATA BREACH INCIDENTS IS SURPASSING INCREASE IN DATA CREATED

Global data created and records exposed, annual percentage changes, 2016–2020



Source: Data adapted from Risk Based Security 2020 Year End Report (global number of records exposed) and Statista (global data created).

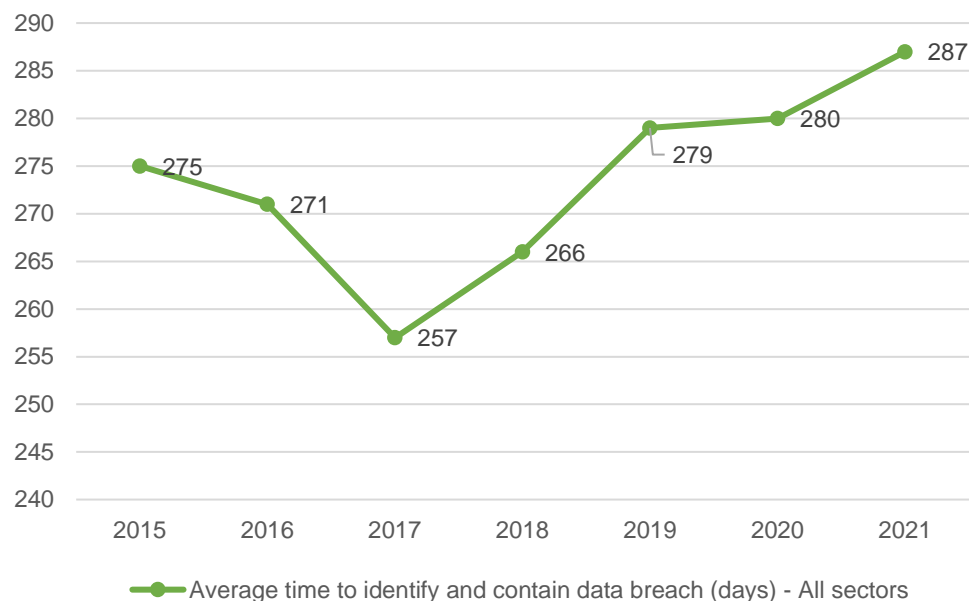
Between 2016 and 2020 the number of records exposed increased by 481 percent while data created increased by 257 percent. Between 2017 and 2020, the average annual increase in total number of records exposed globally was 80 percent and the annual increase in volume of data created was 38 percent (Risk Based Security 2020). Records exposed increased from 0.8 billion in 2015 to 37.2 billion in 2020, the highest-ever number recorded in the history of the Risk Based Security report; global data created during the same period increased from 15.5 zettabytes to 64.2 zettabytes (Statista 2021). Between 2016 and 2020, three out of five years recorded a larger annual percentage increase in number of records exposed than increase in the amount of data generated (also check Chalwe-Mulenga and Duflos 2021). It is worth noting that the severity score* steadily increased throughout 2020 to an average of 5.71 in Q4 compared to 4.75 in Q1.

KPMG's Consumer Loss Barometer (2019a) indicates that consumers in the Americas (43 percent) reported the highest level of information compromise, followed by Asia Pacific (39 percent), then Europe, Middle East, and Africa (35 percent). It is worth noting that data breaches have been identified as among the top risks for users of emerging open banking systems (Carr et al. 2018; Korobov 2020).

* Measured on a scale from zero to 10, breach severity is derived from number of records lost, how the incident occurred, type of data exposed, and a variety of other factors.

ORGANIZATIONS ARE TAKING LONGER TO IDENTIFY AND CONTAIN A DATA BREACH

Average time required to identify and contain a data breach, 2015–2021



Source: Adapted from IBM's global Cost of a Data Breach Reports, 2016 to 2021.

While consumers may not be aware that their data has been exposed, a data breach can carry extreme consequences for them.

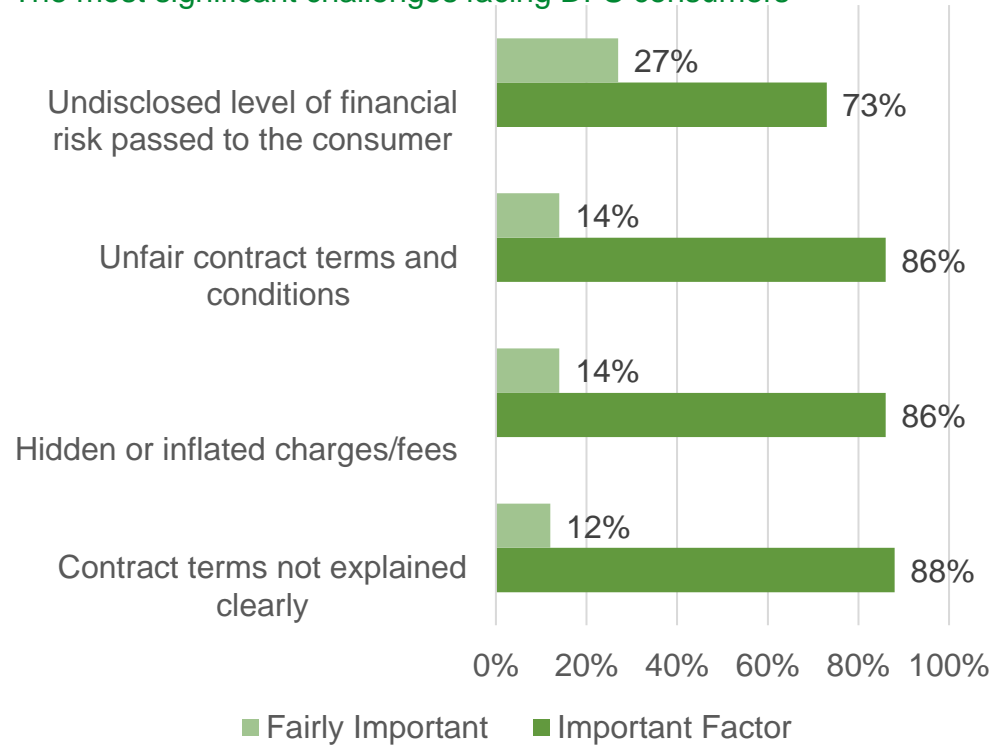
The average time to identify and contain a data breach increased from **257 days in 2017** to **287 days in 2021** due to the increased sophistication of cyber attacks that expose customer data.

IBM (2020) notes that the financial and health sectors had the longest data breach lifecycles: 233 and 326 days, respectively. Since the average time to identify and contain a data breach is linked to the total cost of the breach, the average cost of a data breach is projected to rise in the coming years.

IBM (2021) notes that for companies operating in industries with stricter regulatory environments (e.g., the financial sector), more costs accrue in the years following a breach.

ANECDOTAL EVIDENCE SHOWS TRANSPARENCY HAS WORSENERD OVERALL

The most significant challenges facing DFS consumers



Source: Adapted from the Consumers International survey, The Role of Consumer Organisations to Support Consumers of Financial Services in Low- and Middle-Income Countries, conducted in 2020.

A global survey of 36 Consumers International members from 32 low- and middle-income countries revealed that the top-four most significant challenges DFS consumers faced in 2020 were related to lack of transparency (Consumers International 2021).

In the digital credit space, evidence suggests a correlation between lack of transparency and default or late repayment of digital loans (Izaguirre et al. 2018a; Izaguirre et al. 2018b; Kaffenberger et al. 2018). This implies that worsening transparency may be a contributing factor in countries where consumers have experienced increasing levels of default or late repayment. For example, in countries such as Kenya, India, Indonesia, and Philippines, users of mobile app and P2P loans have experienced higher levels of loan default in the recent past – partly attributed to a lack of understanding of loan pricing and terms/conditions (Faux 2020; Singh 2021a; Singh 2021b; Prakarsa 2020; CNN Philippines 2021). Worsening transparency issues may also be due to the increased complexity of user interfaces, given that more people with low digital and financial skills now use smartphones (Google Next Billion Users research).

Improvements in transparency were noted in Kenya, however, after introduction of a regulation that required mobile providers to display pricing via mobile phone – as evidenced by an increase in the number of customers who knew the cost of mobile money (Mazer 2018).

FORMAL REDRESS CHANNELS ARE UNKNOWN OR EXPENSIVE, BUT DATA ARE LIMITED

Global and regional data and evidence on the evolution of risks related to inadequate redress mechanisms are limited.

Based on qualitative consumer research in Bangladesh, Colombia, and Uganda, on average, only 11 percent of customers who experienced difficulties with mobile money reported it via a formal complaints channel such as a customer care center (McKee et al. 2015).

In Tanzania and Kenya, only 5 percent and 10 percent of digital borrowers, respectively, ever contacted customer care with a question, concern, or complaint about a digital loan (Kaffenberger et al. 2018).

In Cambodia, a survey of client perspectives on consumer protection revealed that “many consumers are unaware of how to access FSPs’ complaint resolution mechanisms, and some are unlikely to use them even if the process is clear” (Kumari 2020).

A study in Indonesia revealed that call centers were the most expensive channel for dispute resolution. A majority of consumers (82 percent), therefore, used agents as the main complaints channel. Moreover, 84 percent of users preferred to incur costs at agents for dispute resolution compared to 57 percent who contacted call centers (Mohammad and Pelupessy 2017).

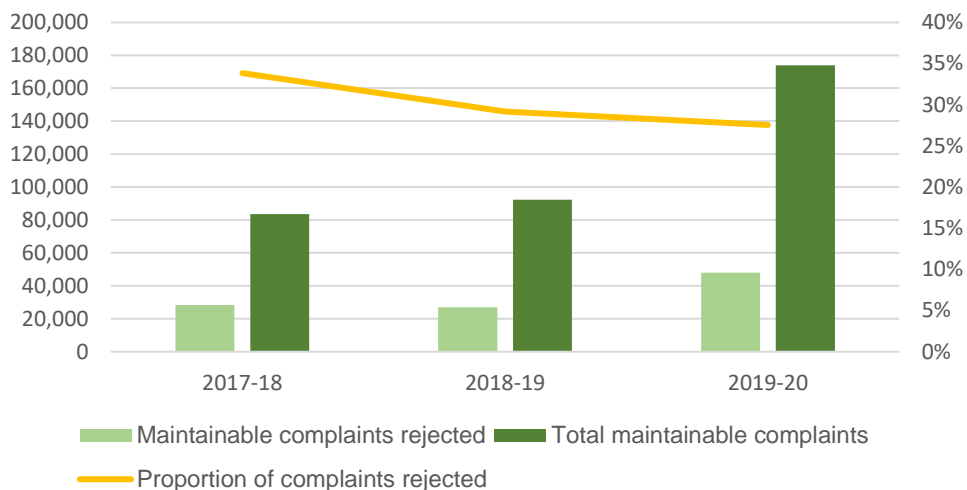
Experian’s 2021 Global Identity and Fraud survey in 10 countries shows that 50 percent of companies surveyed increased their customer support in 2020. However, only about 25 percent of consumers indicated that they received quicker responses from customer service and were able to connect with customer service if they got stuck online.

REDRESS IS A COMPLEX AND CUMBERSOME PROCESS FOR CONSUMERS

India is an example of a country where this is the case

In India, the proportion of complaints related to digital transactions (e.g., mobile/electronic banking, ATM/debit cards, credit cards) reported to the banking ombudsman (BO) rose from 33 percent (64,607) in 2018–2019 to 45 percent (137,823) in 2019–2020, accounting for the largest proportion of all complaints.

Analysis of maintainable complaints related to digital transactions rejected by India’s banking ombudsman



Between February 2019 and June 2020, a total of 2,951 complaints were reported to the Ombudsman Scheme for Digital Transactions (OSDT) – a new scheme launched in 2019 to cover digital complaints from customers of nonbank system participants regulated by the Reserve Bank of India (RBI).

An analysis of maintainable complaints* indicates that between 2017–2018 and 2019–2020, the total number of maintainable complaints and total rejected maintainable complaints increased. However, the rejection rate dropped from 34 percent to 28 percent, indicating that the quality of complaints reported improved. The slight improvement in the quality of complaints may be attributed to sensitization programs undertaken by the RBI.

Nonetheless, in 2019–2020, 72 percent of all complaints received by the BO were from metropolitan and urban areas, while rural and peri-urban areas accounted for 10 percent and 18 percent, respectively. A full 98 percent of rejected complaints were due to filing on wrong grounds and not following the procedure, indicating that people do not understand the complaints filing system. Despite a few improvements, reports indicate that overall, the redress system in India is complex and burdensome, particularly for low-income earners in rural areas who, in most cases, do not even know that the BO exists. The complexity is aggravated by the modularization of the financial sector (Sane 2021; Chivukula 2021).

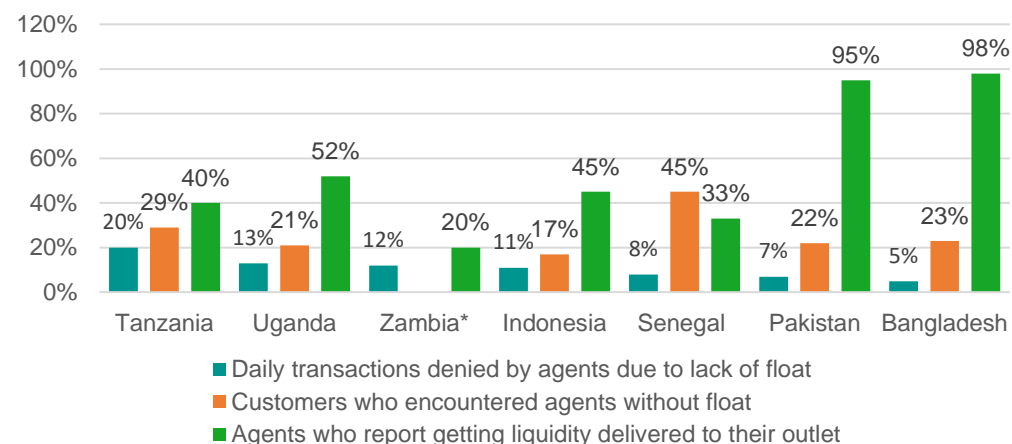
* Maintainable complaints are those made to the BO, relating to the grounds of a complaint specified in Clause 8 of the Banking Ombudsman Scheme (BOS) of 2006 and in line with the requirements laid down in the scheme. Complaints that do not meet the set standards are rejected.

Source: Compiled by the authors based on information from RBI’s 2020 Banking Ombudsman Scheme, 2006, Ombudsman Scheme for NBFCs, 2018, and Ombudsman Scheme for Digital Transactions, 2019: Annual Report – July 1, 2019, to June 30, 2020.

LACK OF AGENT LIQUIDITY PREVENTS CONSUMERS FROM TRANSACTING

Although new agent liquidity management solutions such as super-agents, overdraft facilities, and predictive algorithms for agents (Rodriguez et al. 2019; Wright and Bersudskaya 2017) may help improve agent liquidity, lack of agent liquidity is still a persistent problem in some countries (Genga et al. 2018; Kiarie et al. 2018; Harihareswara et al. 2019; Holly et al. 2020).

Customer and agent liquidity challenges



Source: Genga et al. 2018 and Kiarie et al. 2018, based on data from ANA surveys.

* Data were not available on customers who encountered agents without float (Zambia).

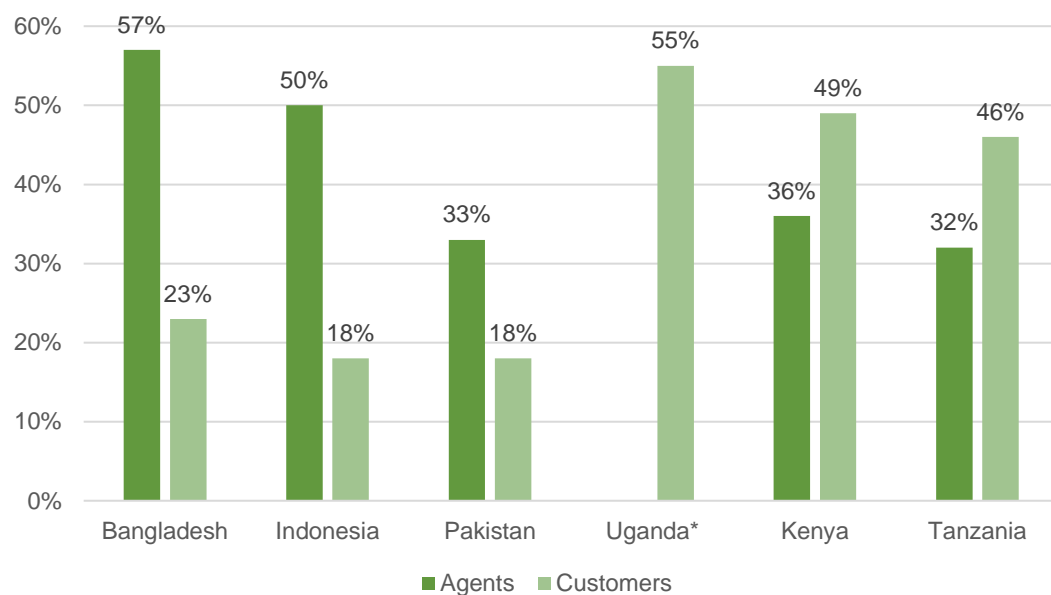
This is common where agents are in remote locations far from DFS provider branches. In Zambia, lack of agent liquidity has been noted as “a recurring and critical issue that impacts the spread of agent businesses in rural and hard-to-reach places” (Holly et al. 2020; Harihareswara et al. 2019).

Supply-side evidence shows that some countries have recorded improvements in agent liquidity management. In India, the proportion of agents who had liquidity (always/sometimes) delivered to them increased from 6 percent in 2015 to 22 percent in 2017. Over that same period, the number of agents who travelled (sometimes/always) to rebalance float reduced from 94 percent to 81 percent (Mehrotra et al. 2018).

However, due to the paucity of demand-side evidence, it is hard to establish if the improved liquidity management reported by agents has benefitted consumers. For example, 48 percent of Indian customers in urban areas and 36 percent in rural areas reported float or cash unavailability as an issue when transacting (CGAP and MSC 2020). Additionally, based on data reported by Genga et al. (2018) and Kiarie et al. (2018), in all countries surveyed, the proportion of customers who encountered agents without float was higher than the proportion of transactions agents denied due to lack of liquidity.

NETWORK DOWNTIME MAY RESULT IN RISKY CUSTOMER BEHAVIOR AND LOSS OF CONFIDENCE IN THE FINANCIAL SECTOR

Proportion of agents and customers who reported experiencing downtime



In 2015, DFS customers identified network downtime as a top concern (McKee et al. 2015; Ahmed and Gomez 2015; Zimmerman and Baur-Yazbeck 2016). Although data to show the evolution of network downtime issues at agent outlets are not available, recent evidence shows that network downtime issues have worsened globally ([see slide 30](#)).

Network downtime may lead to risky behavior, for example, a customer leaving cash, their PIN, or their phone with an agent who would complete the transaction once the network is restored. Network downtime can interrupt the day-to-day activities of customers and lead to their loss of confidence in formal financial services.

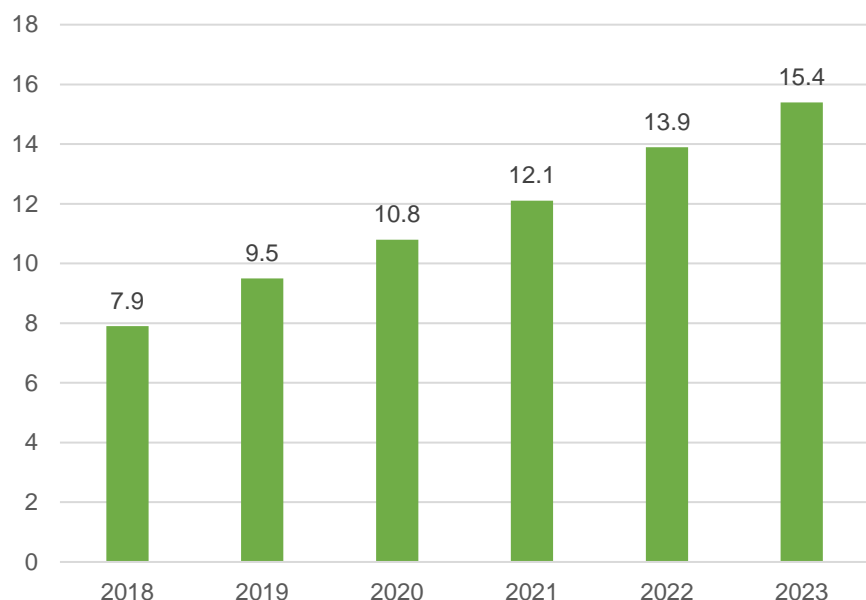
In 2016, an abrupt four-day shutdown of mobile money services in Uganda left millions without access to funds and utilities such as water and electricity (Zimmerman and Baur-Yazbeck 2016).

Source: Genga et al. 2018, based on data from ANA surveys.

* Data were not available for agents who reported experiencing downtime (Uganda).

DDoS ATTACKS – A NETWORK DOWNTIME RISK – ARE INCREASING IN SIZE AND FREQUENCY

Global distributed denial of service attacks (millions)



Source: Cisco Annual Internet Report, 2020–2023.

Refer to the annex for additional examples of the evolution of DFS consumer risks.

Network downtime is a broad issue which may be attributed to problems such as poor infrastructure, power outages, or malicious attacks such as distributed denial of service (DDoS) attacks. A DDoS attack occurs when multiple systems flood the bandwidth or resources of a targeted system. It may happen if hackers attempt to flood a network with unusually high volumes of data traffic in order to paralyze it. Estimates show that while mobile cellular speed will more than triple by 2023 to 43.9 Mbps from 13.2 Mbps in 2018, the number of DDoS attacks will double to 15.4 million by 2023 from 7.9 million in 2018 (Cisco 2020).

Cisco's Annual Internet Report (2020–2023) indicates that between 2018 and 2019, the global frequency of DDoS attacks rose by 39 percent while attacks between 100–400 Gbps grew by 776 percent. Over the same period, the average DDoS attack size was 1 Gbps – enough to take most organizations completely offline.

A 2020 security breach on a consumer finance aggregator, mainly affecting bank-to-mobile-wallet transfers, led to an indefinite suspension of mobile money transactions by the largest mobile money provider in Uganda (Kafeero 2020).

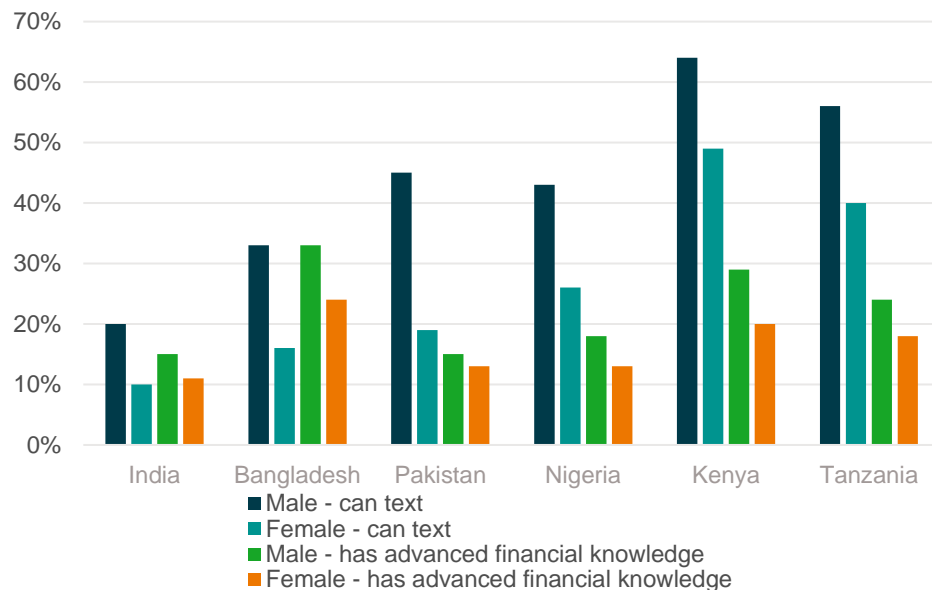
IV. VULNERABLE CONSUMERS AND DFS RISKS

LOW-INCOME WOMEN ARE MORE VULNERABLE TO DFS CONSUMER RISKS

Low digital, financial, and literacy skills amplify DFS consumer risks for women

There is limited disaggregated data to assess the evolution of DFS consumer risks that affect women. Anecdotal evidence suggests that women are more vulnerable to DFS consumer risks than men.

Financial and digital skills of rural women and men



Source: IDEO.org and the Bill & Melinda Gates Foundation, 2019, Women and Money: Insights and a Path to Close the Gender Gap.

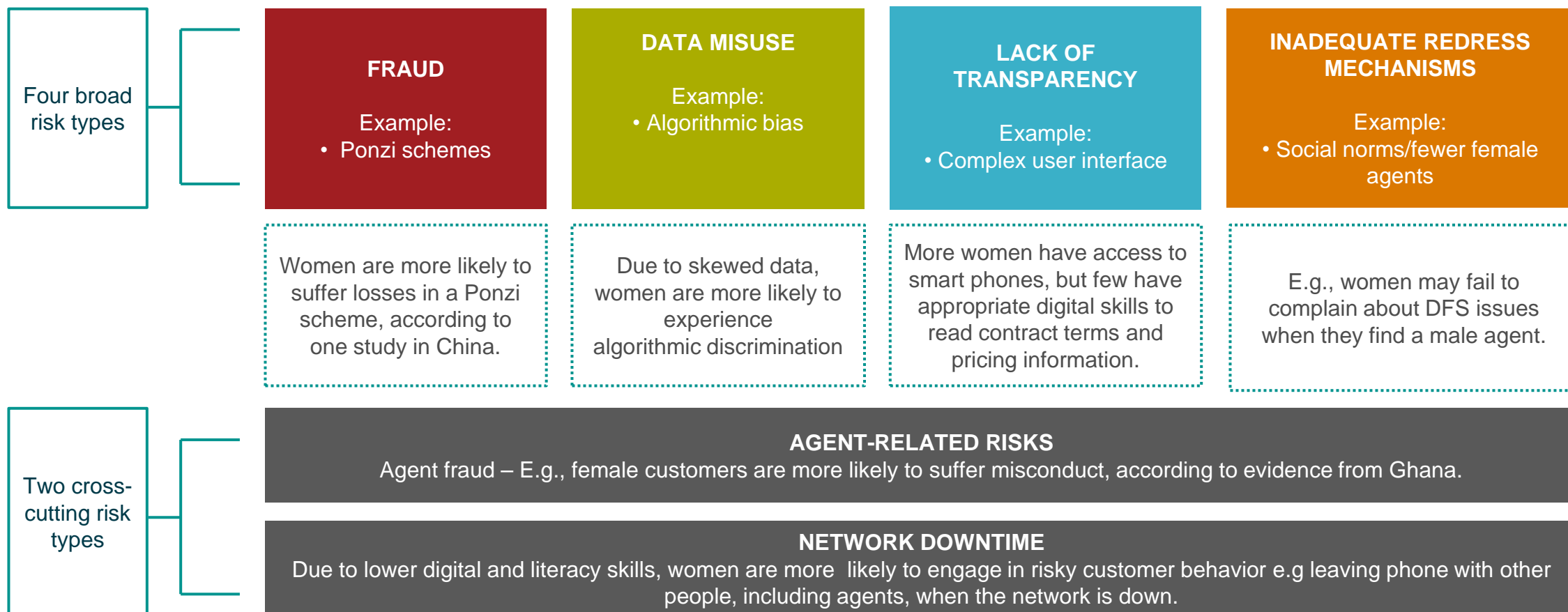
This is mainly because women generally have lower digital, financial, and literacy skills than men (GPII 2020; GSMA 2020; Toronto Centre 2018; Wechsler and Siwakoti 2020). There is need for financial inclusion and consumer protection stakeholders to collect more gender-disaggregated data. When women with low financial and digital skills are given access to DFS, they are exposed to various risks as they may not understand DFS terms and/or prices and often become victims of fraud.

In Indonesia, after the digitalization of the Program Keluarga Harapan (PKH) – a government-to-person (G2P) program that benefited about 10 million people – it was found that nearly half (44 percent) of women surveyed relied on ATM security guards, agents, and family members to help them withdraw money from their accounts. Additionally, many women reported that they preferred to access their money via an agent rather than an ATM because agents completed the full transaction on their behalf.

Studies also show that women may not change their default PIN or may use the same PIN as others in the community to reduce errors. They also sometimes hand their phone over to an agent (Theis et al. 2020; IDEO.org and the Bill & Melinda Gates Foundation 2019; Wright et al. 2018).

EXAMPLES OF DFS CONSUMER RISKS FOR LOW-INCOME WOMEN

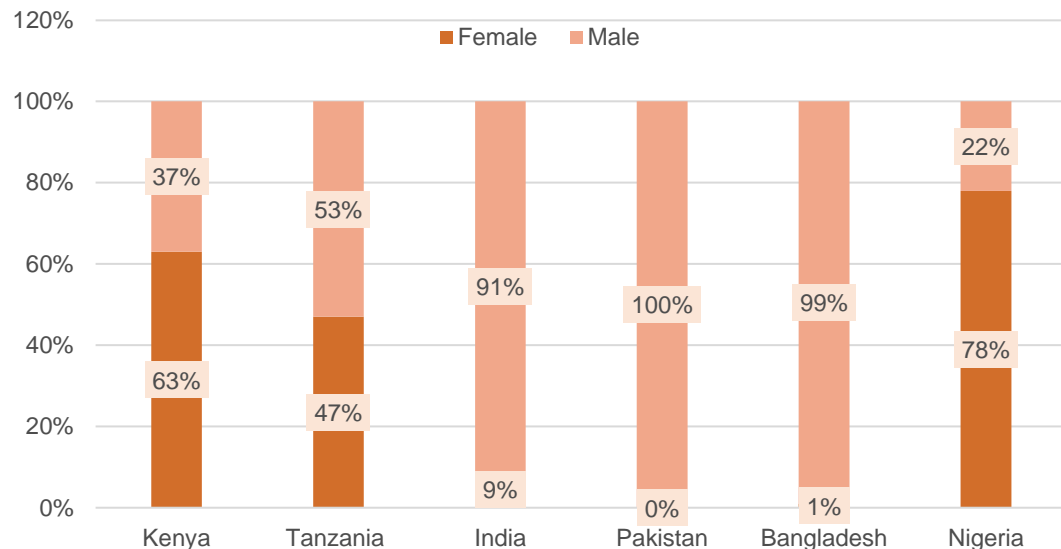
Several DFS risks affect low-income women but evidence of the evolution of risks is limited



SOCIAL NORMS AND AGENT MISCONDUCT POSE CHALLENGES FOR WOMEN

Women prefer female agents, but they are less available and more likely to overcharge

Proportion of female and male agents



Source: IDEO.org and the Bill & Melinda Gates Foundation, 2019, Women and Money: Insights and a Path to Close the Gender Gap.

In the Democratic Republic of the Congo, Chamboko et al. (2020) found evidence of “assortative gender matching in agent banking transactions, as clients prefer to transact with agents of their own gender.” They also note that women prefer female agents even when they are less available, especially “when making high-value transactions and when they have higher account balances.”

In Bangladesh, IFC (2018) found that 52 percent of women expressed a clear preference for female agents despite a 99 percent chance of finding male agents.

Women prefer to stand side-by-side with agents, which is considered improper in most cultures, especially in Pakistan and Bangladesh (IDEO.org and the Bill & Melinda Gates Foundation 2019; Kabir and Klugman 2019). Female agents are also perceived to be more patient, making them better candidates for the teaching role of agents. Unfortunately, most women do not aspire to become agents.

However, disturbing evidence in Ghana shows that female agents are more likely to engage in “misconduct.” Based on a census of the mobile money market across 166 low-income communities in Eastern Ghana, Annan (2021) found evidence of a “gender misconduct gap.” Overall, 25 percent of mobile money transactions are overcharged and while both male and female agents overcharge clients, female agents are 37 percent more likely to overcharge both male and female clients.

WOMEN ARE TARGETS OF FRAUDULENT SCHEMES AND ONLINE ABUSE

Anecdotal evidence reveals that women are more likely to experience social shaming and higher losses in Ponzi schemes

Female Ponzi investors are more susceptible to investor affinity

A study in China sought to examine how investor affinity (in terms of gender and age) affects the propagation of a Ponzi scheme and how investors suffer losses. The study found that female investors who are introduced into a Ponzi scheme by other female investors are more likely to suffer losses when the scheme – whether digital or not – collapses (Huang et al. 2021).

According to recent journalistic reports in Argentina, a high-profile celebrity allegedly lured several women into a feminist “telares de abundancia” (“abundance looms”) pyramid scheme. Marketed through social media and WhatsApp solidarity groups, the scheme leveraged feminist activism due to worsening economic conditions and injustices perpetrated against women (Schwartz and Herrera 2020; Bleszynska 2021; Gibbings 2020; Fahsbender 2019). Reports further indicate that such schemes are increasingly common in other parts of Latin America.

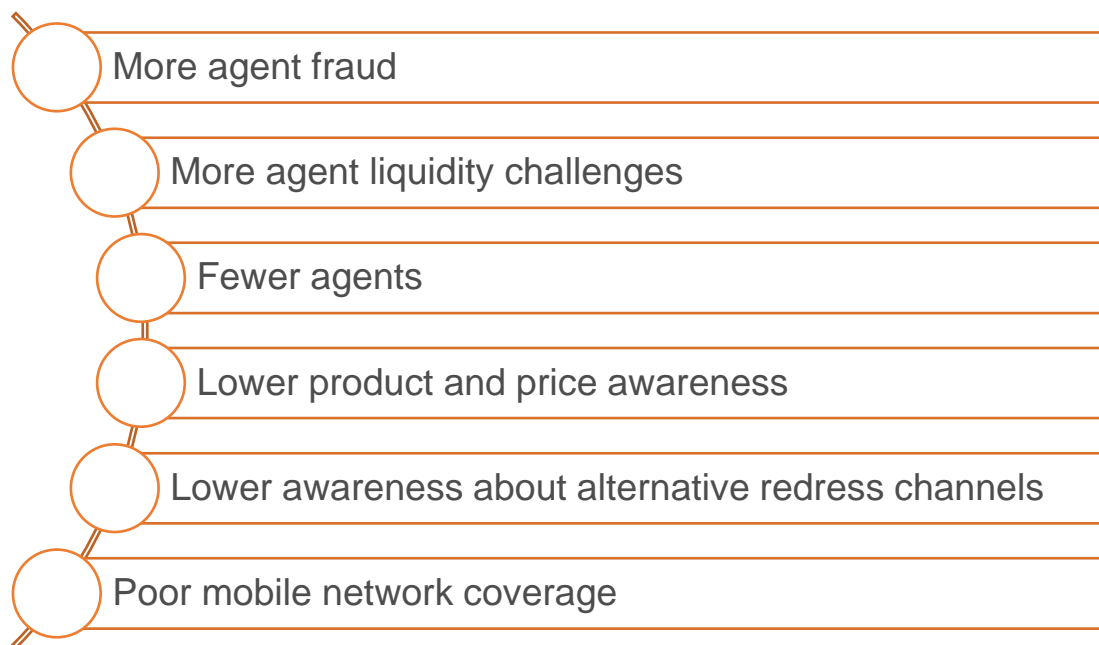
Female DFS users may be asked to provide “naked collateral”

In 2016 and 2017, media reports in China indicated that female students were told to submit images of themselves naked or performing lewd acts as collateral for app-based digital loans. The lenders then threatened to post the photos on social media if the women failed to repay their debt. One media house found a “naked collateral” file with over 160 female college students holding identity cards (Zhang and Woo 2017; Bradsher and Tang 2017). These activities happened in the unregulated digital credit market, which was booming in China at the time. It is worth noting that women are more likely to be victims of online abuse (Sambasivan et al. 2019).

There is need for proactive measures to ensure that aggressive debt collection practices do not happen, especially in markets where app-based digital credit is new.

RURAL POPULATIONS ARE MORE VULNERABLE TO DFS RISKS

Like women, rural populations have low digital, financial, and literacy skills, which amplifies DFS consumer risks



Due to the low usage of DFS in rural areas, evidence of actual risks that affect rural population areas is anecdotal.

Rural areas generally have fewer DFS options and agents than urban areas (Mustafa et al. 2017; Unnikrishnan et al. 2019). Therefore, scant evidence is available on the scale of DFS consumer risks.

The few people in rural areas who use DFS face similar or, in some cases, the same risks as low-income women. Risks are also compounded when rural consumers are female. A study in Indonesia found that awareness about transaction charges for payment accounts was 15 percent, and consumer ignorance enabled agents to overcharge clients. The study also revealed that rural customers faced other challenges, such as inadequate redress mechanisms, transaction delays, and denials more than urban customers (Mohammad and Pelupessy 2017).

According to the [2019 FinAccess Survey](#), in Kenya, more people in rural areas (42.2 percent) depend on their own financial knowledge than those in the urban areas (35.8 percent).

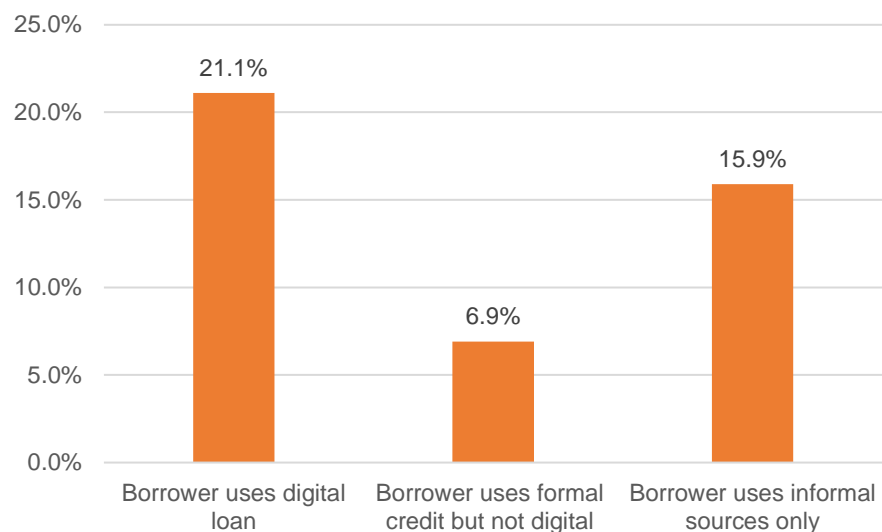
In some countries, agent liquidity challenges are more prevalent in rural areas (Harihareswara et al. 2019; White 2020; Kiarie et al. 2018).

V. SPECIAL FOCUS:
OVERINDEBTEDNESS OF DIGITAL
CREDIT USERS

DIGITAL LENDERS ARE MORE LIKELY TO FUEL UNHEALTHY BORROWING THAT RESULTS IN HIGHER DEFAULT RATES

Consumers are also more likely to default on banking apps

Borrowers who defaulted at least once on a loan in the past year



Source: FSD Kenya, Digital Credit in Kenya: Facts and Figures from FinAccess, 2019.

* Loan stacking refers to a borrower having multiple loans outstanding at the same time, which thereby affects their ability to afford timely repayment. It is also an indicator of identity fraud.

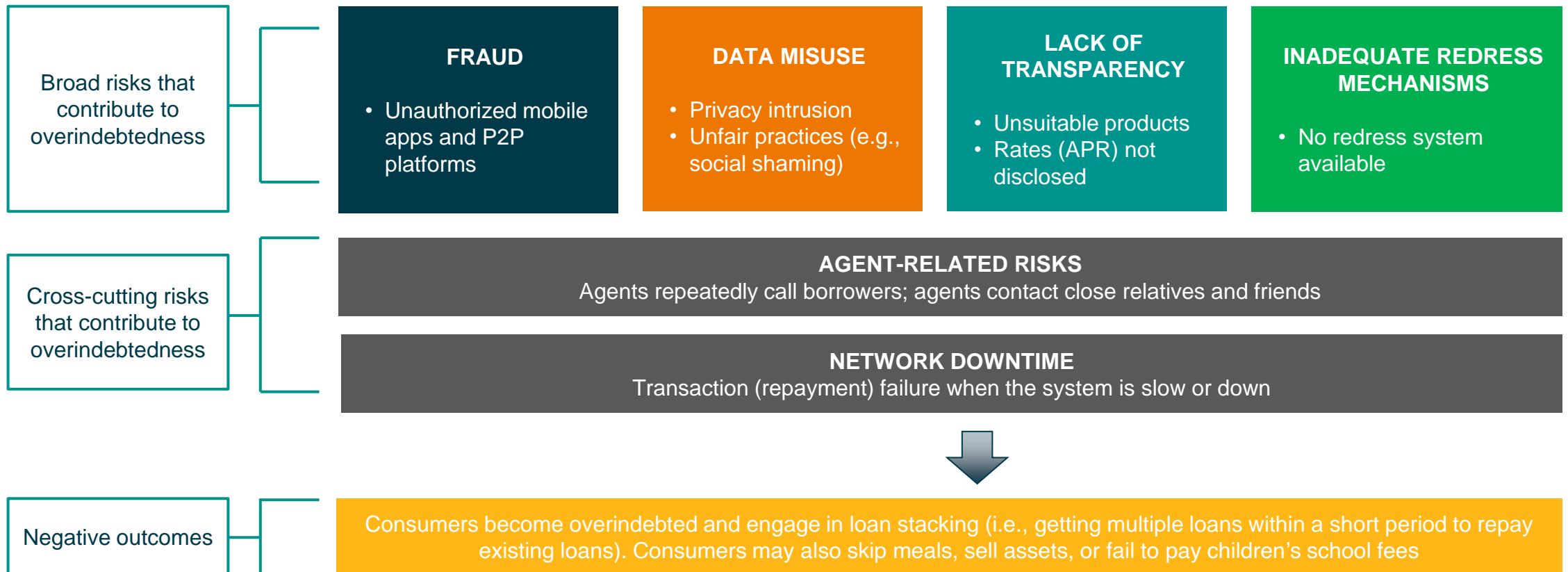
More consumers can access digital credit products via mobile applications and peer-to-peer lending platforms. But these delivery channels expose them to numerous risks that lead to overindebtedness. Based on data from the 2019 FinAccess Survey, digital borrowers (21.1 percent) are more likely to default than informal borrowers (15.9 percent) and formal non-digital borrowers (6.9 percent). Additionally, 14 percent of digital borrowers reported specifically defaulting on a mobile banking or digital app loan (FSD Kenya 2019).

A study to evaluate the progress and challenges of digital credit in Kenya found that the proportion of digital loans (91.2 percent in 2018) not only increased but far surpassed that of traditional loans (8.8 percent in 2018). However, about 2.2 million people who obtained digital loans between 2016 and 2018 had non-performing loans (NPLs) and 49 percent of these digital borrowers had outstanding balances of less than US\$10.

Consistent with other studies, poor transparency was evident as customers have low understanding of pricing and terms and conditions. Additionally, customers did not understand how their personal data was shared.

OVERINDEBTEDNESS IS AN OUTCOME OF A COMBINATION OF SEVERAL DFS CONSUMER RISKS

Overindebted digital credit consumers face multiple risks

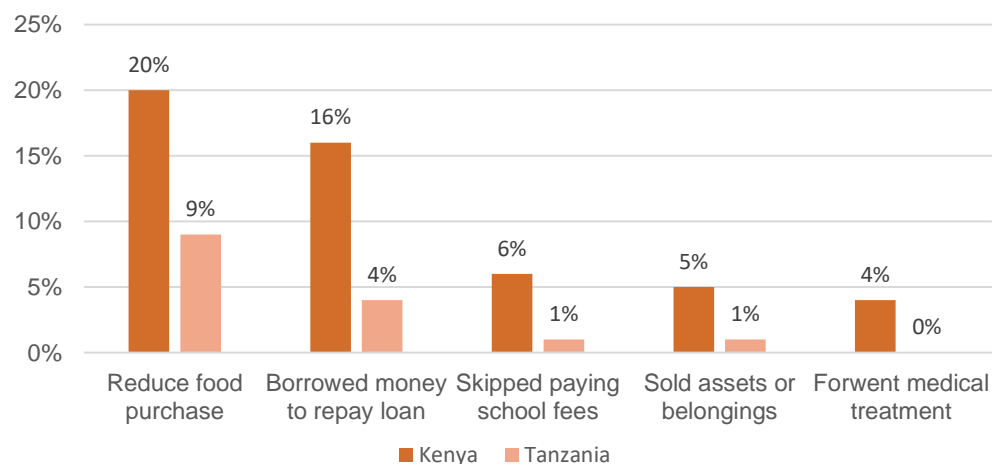


OVERINDEBTEDNESS HAS CONCERNING IMPACTS ON PEOPLE'S LIVES AND LIVELIHOODS

It affects consumers' ability to weather shocks and leads to negative coping mechanisms

Overindebtedness may lead people to take detrimental actions which affect their ability to weather shocks and stresses. In Tanzania and Kenya, a study found that people reduced their food purchases or borrowed more money to repay existing debt.

Actions taken to repay digital loans in Kenya and Tanzania



Source: Kaffenberger, Totolo, and Soursourian, 2018, A Digital Credit Revolution: Insights from Borrowers in Kenya and Tanzania.

Another study in Kenya found that using digital credit increased the probability of selling household assets to repay a loan and increased the likelihood of having more loans, which reduced household welfare (Wamalwa et al. 2019).

Indicators of repayment distress (e.g., reducing food purchases, overborrowing, taking a child out of school) for digital borrowers resemble those of informal borrowers more than those of other formal borrowers (FSD Kenya 2019).

According to media reports in China, Kenya, and India, some overindebted people who experienced social shaming committed suicide (Zhang and Woo 2017; Faux 2020; Mashal and Kumar 2021; Singh 2021a, 2021b).

Evidence from Sweden shows that over-indebted people are nine times more likely to be ill and seven times more likely to be hopeless than those not affected by overindebtedness (Political Economy Research Centre 2015; Ferreira et al. 2021; Ahlström and Tjulander 2020).

VI. THE PATH FORWARD: A CALL TO ACTION

WHAT THIS MEANS FOR REGULATORS AND SUPERVISORS

There is an urgent need for proactive measures that maintain consumer trust in DFS and ensure positive outcomes

If the growth of DFS consumer risks is not reversed, vulnerable consumers may lose trust in digital finance. **Regulators and supervisors** have a critical role to play in mitigating these risks.

Regulators and supervisors can implement tools and measures for timely monitoring and intervention to mitigate DFS risks and minimize customer harm, including:

- Adopting market monitoring tools to get a better understanding of the situation on a timely and continuous basis, especially for women and vulnerable segments.
- Including regulatory requirements that relate to specific topics such as cyber security, transparency, data management, complaints handling, etc.
- Ensuring strong enforcement of supervisory rules.
- Developing coordination mechanisms to engage nonfinancial-sector regulators (e.g., competition, telecom, and data protection authorities; law enforcement agencies).
- Helping to refocus financial inclusion on customer outcomes rather than access and usage.
- Lobbying government to expand support to consumer protection frameworks.



Photo for CGAP by Lorena Velasco via Communication for Development Ltd.

WHAT THIS MEANS FOR DONORS AND INVESTORS

Donors and investors can help promote responsible DFS practices

Donors can include assessment of consumer risks in DFS project design and evaluations. They can also support financial and digital literacy of vulnerable consumers to build customer awareness around risks. Donors can also facilitate and support:

- Coordination among financial, data, and telecoms regulators.
- Dialogue between policymakers, regulators, supervisors, DFS providers, and consumer associations.
- Governance frameworks.
- Enabling infrastructure (e.g., ID systems, etc.).
- The funding of research on consumer risks.

Investors can analyze risk management mechanisms and consumer protection policies of investees during due diligence. They can also promote responsible finance standards among DFS providers (e.g., by signing up to [investor guidelines](#) on responsible DFS investing). They can also influence investee companies to empower consumers through better digital financial literacy.



Photo for CGAP by Temilade Adelaja via Communication for Development Ltd.

WHAT THIS MEANS FOR DFS PROVIDERS

DFS providers have a critical role to play since they deal directly with customers

To help customers identify and mitigate risks, **DFS providers** are encouraged to imbed financial literacy into business models and develop industry-wide mechanisms to promote responsible DFS practices. Providers can also measure financial health of their clients and develop customer-centric business models that focus on providing positive outcomes for their customers (UNSGSA 2021; [CGAP Customer-Centric Guide](#)). Additionally, they can strengthen and continuously improve their cyber resilience.

Other measures providers can take include improving:

- Complaints-handling processes.
- Product design to minimize risks.
- Transparency of products.
- Agent liquidity management.
- System availability via frequent upgrades to information technology systems.



Photo by Chara Lata Sharma, CGAP Photo Contest

WHAT THIS MEANS FOR CONSUMER GROUPS AND RESEARCHERS

Consumer groups and researchers also have roles to play

Consumer groups can help raise consumer awareness on DFS risks and mitigation strategies. They can also:

- Help affected consumers, especially vulnerable consumers, to file complaints.
- Provide consumers with information about risks.
- Provide consumers with legal and other support.
- Offer compensation funds.
- Notify supervisors and regulators of emerging consumer concerns.

Researchers can continue to fill the gaps identified in this research, such as the lack of gender disaggregated data and the lack of evidence on the impact of risks on consumers – particularly vulnerable consumers.



Photo for CGAP by Nicolas Réméné via Communication for Development Ltd.

CGAP'S SOLUTIONS FOR PROTECTING VULNERABLE CUSTOMERS

CGAP promotes an approach where regulators, supervisors, providers, and market facilitators focus on ensuring **positive outcomes to customers in their financial journeys**.

We offer three types of solutions:

The CGAP Market Monitoring Toolkit (MMT)

CGAP has developed a toolkit for market conduct authorities and other actors that includes regulatory report analysis, complaints analysis, mystery shopping, and phone surveys. The toolkit enables supervisors to assess risks affecting consumers and take corrective action as needed.

Mechanisms to elevate the collective consumer voice (CCV)

CGAP identified three mechanisms to empower consumers to share their experience and influence regulation: consumer groups/associations, regulatory consultative bodies, and technology and social media. CGAP is currently working on pilots to illustrate how these mechanisms can empower consumers.

Showcasing responsible DFS providers

CGAP is showcasing and promoting customer-centric DFS providers that adopt responsible business models and distribution channels (e.g., agents) that protect consumers and their data from risks.

Related CGAP Resources:

Working Paper: [Elevating the Collective Consumer Voice in Financial Regulation](#)

Working Paper: [Making Consumer Protection Regulation More Customer-Centric](#)

Leadership Essay: [It's Time to Change the Equation on Consumer Protection](#)

Blog Series: [Cybersecurity and Financial Inclusion: Protecting Customers, Building Trust](#)

Blog Post: [Analyzing Social Media to Spot Digital Consumer Credit Risks in India](#)

Please consult the Annex for solutions implemented by other organizations.

ANNEXES

DETAILED LIST: RISKS IN THE FOUR BROAD RISK TYPES

FRAUD	DATA MISUSE	LACK OF TRANSPARENCY	INADEQUATE REDRESS MECHANISMS
<ul style="list-style-type: none"> • SIM swap/account takeover fraud • Internal fraud (e.g., unauthorized access to customer information, unauthorized fees) • Synthetic identity fraud • Card fraud (e.g., card not present fraud, counterfeit card) • Biometric ID fraud • Mobile app fraud/smartphone espionage • Unlicensed digital investment/Ponzi scheme • Social engineering fraud (i.e., phishing, smishing, vishing, impersonation) • Social media scam (e.g., Facebook, Twitter, etc.) • Money transfer fraud (e.g., advance fee scam, extortion, sympathy scam, purported wrong transfer) • Mobile browser fraud/pharming • Counterfeit device • Infrastructure compromise (e.g., ATM/mobile money) • Mobile device theft/sharing of devices • Authorized push payment scam 	<ul style="list-style-type: none"> • Algorithmic bias • Unfair practice (e.g., selling unsuitable product, aggressive marketing/cross-selling, abusive debt collection practice such as social shaming) • Privacy intrusion • Opaque decision making • Data breach (+ amplified cyber risk) • Uninformed consent • Inaccurate profiling and no data integrity • Matthew effect • Liability allocation risk • DFS provider failure to safeguard customer personal data • Customer failure to safeguard personal data • Data handling practices not disclosed 	<ul style="list-style-type: none"> • Incomplete/unclear pricing information • Unfair practice (e.g., selling unsuitable product, aggressive marketing/cross-selling, abusive debt collection practice such as social shaming) • Complex/confusing interface/menu • Inaccessible terms/fees, including complicated disclosure format • Inability to compare products • Unexplained/hidden/undisclosed fees • Data handling practices not disclosed • Complex legal language and excessive information that overloads/confuses consumers • No notice regarding referrals • Product's inherent risks not communicated to customer • Misleading advertisement 	<ul style="list-style-type: none"> • Unclear complaints procedure • Expensive complaints-handling system • Time-consuming complaints procedure • Slow redress process • Unresponsive or poorly trained staff • Lack of appropriate channels to report issues • Difficulty settling cross-border disputes • Incomplete or unsatisfactory dispute resolution • Untrained and unmonitored agents • Social norms

DETAILED LIST: RISKS IN THE TWO CROSS-CUTTING RISK TYPES

AGENT-RELATED RISKS	NETWORK DOWNTIME
<ul style="list-style-type: none">• Fewer female agents• Social norms• Fewer rural agents• Fraud/overcharging/fee markup/unauthorized fees• Access to customer PIN (theft/compromise)• Poor dispute resolution by agents• Limited product awareness• Manipulation of customers• Unfair treatment of customers/discrimination based on social status• Insufficient agent liquidity that may lead to transaction splitting, denial of transactions, or bulk payments• Untrained and unmonitored agents	<ul style="list-style-type: none">• Distributed denial of service (DDoS) attacks• Inadequate DFS infrastructure• Insufficiently tested system upgrade• Power outages• Inadequate disaster recovery and business continuity plans• Risky customer behavior (e.g., leaving cash, PIN, or phone with others)• Incomplete and interrupted transactions/inaccessible funds• No confirmation message – may lead to duplicate transactions• Unresolved complaint (e.g., agent/service provider fails to check transaction status or connect with DFS provider)

GLOSSARY OF TERMS

Agent risks Risks emanating from a DFS user’s interactions with the designated agent of a DFS provider.

Cybersecurity The practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

Data misuse The risk that an entity or person uses a DFS customer’s data or information for purposes it is not intended for.

Digital financial services (DFS) All financial services provided through digital channels such as mobile phones, ATMs, point-of-sale (PoS) terminals, near field communication (NFC)-enabled devices, chips, electronically enabled cards, biometric devices, tablets, phablets, and other digital channels – whether savings, payments, credit, insurance, remittances, investment, or variations of these. Includes services accessed via agents and third-party networks.

DFS consumer risk A condition or factor that exposes a consumer to potential or actual harm or loss (both financial and nonfinancial) while using DFS.

Fraud The risk that intentionally deceptive actions by an entity or person will cause a DFS consumer financial loss.

Lack of transparency The risk that terms, conditions, fees, and other DFS features are not understood by a customer.

Inadequate redress mechanisms The risk that a DFS user has no channel for complaints or complaints are not appropriately addressed.

Network downtime The risk that technological failure prevents a customer from using DFS.

Overindebtedness* An individual or household is overindebted when their existing and expected resources are insufficient to meet their financial commitments without lowering their standard of living.

Vulnerable customers** Low-income customers as well as groups that are less served, such as youth, elderly people, women, rural populations, refugees, etc. CGAP’s consumer protection program has a particular focus on women and rural segments.

* Adapted from Giovanni D’Alessio and Stefano Iezzi’s [Household Overindebtedness Definition and measurement with Italian Data](#).

** CGAP acknowledges that vulnerability can be defined differently. For example, the [Financial Conduct Authority](#) defines a vulnerable customer as someone who, due to their personal circumstances, is especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care.

RESEARCH METHODOLOGY

Reviewed 175 publications/articles

- 94 publications mentioned an increase or decrease in risk; 81 only mentioned the nature of risks
- 40 additional publications and articles (DFS benefits, solutions, etc.)
- Please refer to References section for a list of publications and articles

Consulted 74 global, regional, and national experts from 33 institutions

- Think tanks/research institutions
- Funders/investors
- Industry associations
- Providers
- Policy/supervisory entities
- Please refer to slides 52-54 for a list of institutions and individuals consulted

Incorporated expert feedback

- Initial findings resonated with most experts
- Updated some sections
- Added several new sections

CONSULTATIONS

Organization	Individuals Consulted	Designation
Alliance for Financial Inclusion (AFI)	Ghiyazuddin Mohammad	Senior Policy Manager for Digital Financial Services
	Luis Trevino Garza	Senior Policy Manager, Data and In-Country Implementation
	Sulita Levaux	Policy Specialist, Consumer Empowerment and Market Conduct
Bank for International Settlements (BIS)	Jon Frost	Senior Economist, Fintech and Digital Innovation, Digital Economy Unit
Better than Cash Alliance	Camilo Tellez	Head, Digital Innovation
	Keyzom Ngodup	Head, Asia region
Bill & Melinda Gates Foundation	Anna Wallace	Head, Consumer Protection and Regulatory Technology
	Deon Woods Bell	Senior Advisor, Policy
	Pawan Bakhshi PhD	India Lead, Financial Services for the Poor
Caribou Digital	Marissa Dean	Digital Investments Lead
CDC Group	Machal Karim	Manager, Development Impact-Investments
Center for Effective Global Action	Marisa McKasson	Senior Program Associate
	Leah Bridle	Associate Director of Research
Center for Financial Inclusion	Alexandra Rizzi	Senior Research Director, Consumer Data Opportunities and Risks
Consumer Financial Protection Bureau (CFPB), USA	Mary Griffin	Executive Director - Cooperative Development Foundation, formerly Senior Advisor - Office of Community Affairs at CFPB
Consumers International	Antonino Serra Cambaceres	Advocacy Manager
	Matthew Jones	Project Specialist
Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ)	Klaus Prochaska	Head, Financial Sector Development and Insurance, GIZ Headquarters
	Florian Berndt	Senior Advisor, Financial Systems Development, Financial Inclusion and Responsible Finance
	Saliya Kanathigoda	Program Advisor, Digital Finance
	Marian Engelbarts	Advisor for Financial System Development
Dvara Research	Indradeep Ghosh	Executive Director
	Deepti George	Deputy ED and Head of Strategy
	Beni Chugh	Research Manager

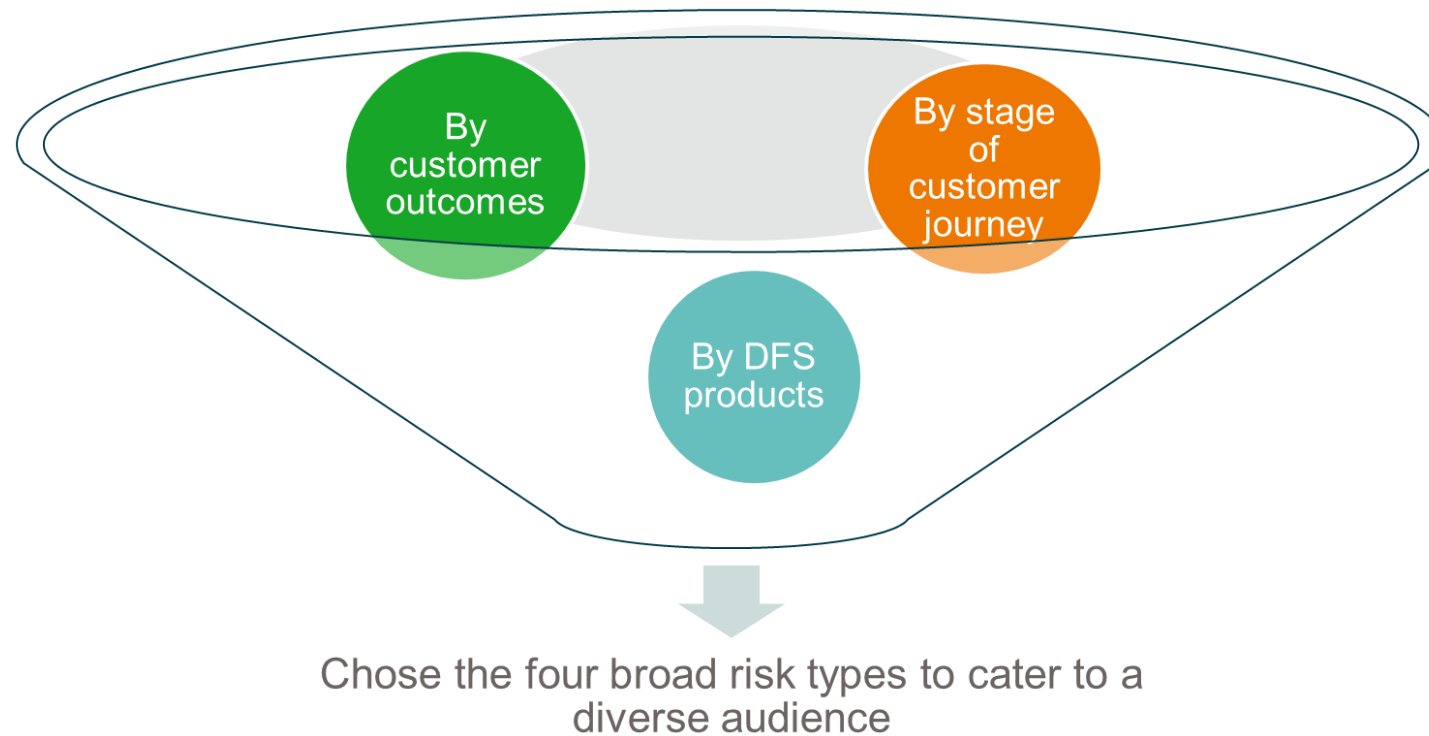
CONSULTATIONS *(continued)*

Organization	Individuals Consulted	Designation
Enhancing Financial Innovation and Access (EFInA) Nigeria	Henry Chukwu	Program Specialist, Digital Financial Services
Financial Sector Deepening (FSD) Zambia	Betty Wilkinson	Chief Executive Officer
	Charity Chikumbi	Director, Policy and Digital Financial Services
	William Sichombo	Head, Policy and Digital Financial Services
Financial Sector Deepening (FSD) Africa	Shakila Kerre	Digital Economy Specialist
Flourish Ventures	Stella Klemperer	Strategy Manager
	Tina Moran	Senior Investment Analyst
GSM Association (GSMA)	Saad Farooq	Senior Manager, Advocacy (Mobile Money)
	Ashley Olson Onyango	Head of Financial Inclusion and Agritech
	Julianne Mweheire	Data and Insights Director, Mobile Money Program
	Brian Muthiora	Policy and Regulatory Workstream Lead, Mobile Money Program
	Claire Sibthorpe	Head of Connected Women, Connected Society and Assistive Tech
	Daniele Tricarico	Director Research and Insights Research, Agritech
Innovation for Poverty Action (IPA)	Sonia Pietosi	Insights Manager, Agritech
	Rafe Mazer	Project Director, Consumer Protection
	Daniel Putman	Postdoctoral Fellow, Consumer Protection Initiative
International Finance Corporation (IFC)	Rebecca Rouse	Program Director, Financial Inclusion Program
	Lory Camba Opem	Operations Officer and Responsible Finance Lead
International Telecommunication Union (ITU)	Venkatesen Mauree	Program Coordinator, Study Groups Department, Standardization Bureau
	Bilel Jamoussi	Chief, Study Groups Department
Mastercard Center for Inclusive Growth	Daniel Barker	Vice President for Research and Knowledge
	Ali Schmidt-Fellner	Manager for Knowledge and Insights
	Leslie Meek-Wohl	Director for Global Programs
MicroSave Consulting (MSC)	Elizabeth Berthe	Associate Director
	Graham Wright	Founder and Group Managing Director of MSC

CONSULTATIONS *(continued)*

Organization	Individuals Consulted	Designation
Observatory of the Quality of Financial Services (Senegal)	Habib Ndao	Secrétaire Exécutif
	Dr Aliou Diop	Expert financier
Orange	Anne Catherine Tchokonté	Head of Mobile Financial Services Diversification, Middle East and Africa
Peruvian Financial Regulatory Authority	Elias Roger Vargas Laredo	Deputy Assistant Superintendent of Market Conduct and Interest Rates
	Mariela Zaldivar	Deputy Superintendent of Market Conduct and Financial Inclusion
Social Performance Task Force (SPTF)	Anton Simanowitz	Director for Customer Centricity
	Laura Foose	Executive Director
	Amelia Greenberg	Deputy Director of Responsible Inclusive Finance Facility for Africa and Middle East
	Katie Hoffman	Director of Responsible Inclusive Finance Facility for Southeast Asia
United Nations Capital Development Fund (UNCDF)	Ahmed Dermish	Lead Specialist, Policy and Government Advocacy, Inclusive Digital Ecosystems
	Alexis Ditekowsky	Agile Delivery Specialist
	Naomi Bourne	Policy Analyst, Digital Finance
	Jeremiah Grossman	Digital Policy Specialist
United Nations Secretary-General's Special Advocate for Inclusive Finance for Development (UNSGSA)	Pia Tayag	Director
	Peter McConaghy	Policy Advisor - Financial Sector
	David Symington	Policy Advisor - Fintech & Digital Payments
	Nancy Widjaja	Policy Advisor - Financial Health & Private Sector Engagement
United States Agency for International Development (USAID)	Paul Nelson	Senior Digital Finance Advisor
Visa	Amina Tirana	Head of Policy and Measurement, Social Impact
World Bank Responsible Financial Access (RFA) Team	Jennifer Chien	Senior Financial Sector Specialist
	Gian Boeddu	Senior Financial Sector Specialist
World Bank G2PX	Vjayanti T. Desai	Practice Manager
	Georgina Marin	Program Officer
	Minita Mary Varghese	Consultant
Women's World Banking	Sonja Kelly	Research and Advocacy for Women's Economic Inclusion

OTHER RISK TYPOLOGIES CONSIDERED



OTHER EXAMPLES: THE EVOLVING SCALE OF DFS CONSUMER RISKS

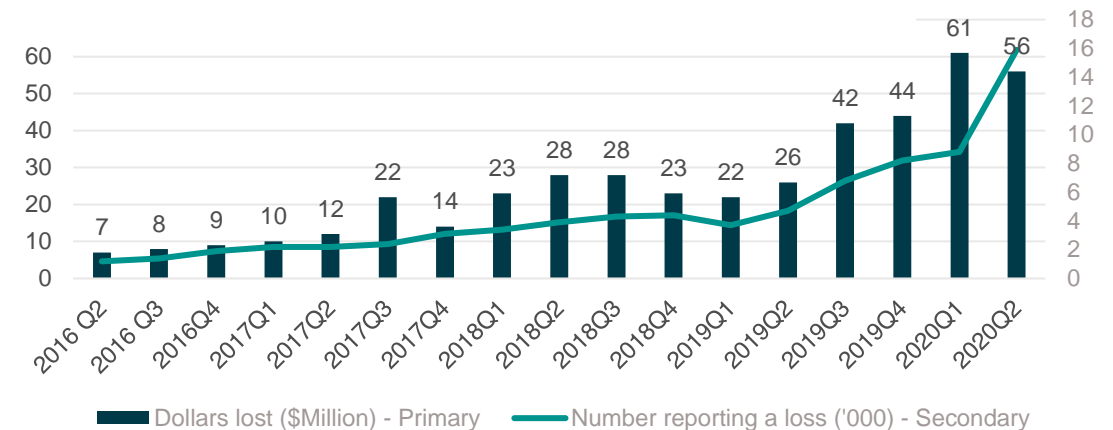
The volume and impact of social media scams is rapidly rising

A study by Consumers International (2019) in nine countries identified investment scams and imposter scams as the top two scams perpetrated through social media.

Approximately 4 billion people (about 50 percent of the global population) use social media platforms such as Facebook, Twitter, WhatsApp, and Instagram (Statista 2021). Social media presents a great opportunity for fraudsters to trick unsuspecting DFS users. Consumers International also reports that the Swedish Consumer Agency found that consumers with physical or cognitive impairments, low incomes, low levels of education, and poor language skills were more likely to become victims of subscription traps.

Consumers International further notes that data from the Australian Competition and Consumer Commission show that the amount of money lost through social media scams quadrupled between 2015 and 2018 – from AUS\$3.8 million to AUS\$13.1 million.

Scams started on social media, 2016–2020



Source: Federal Trade Commission Consumer Protection Data Spotlight, October 2020.

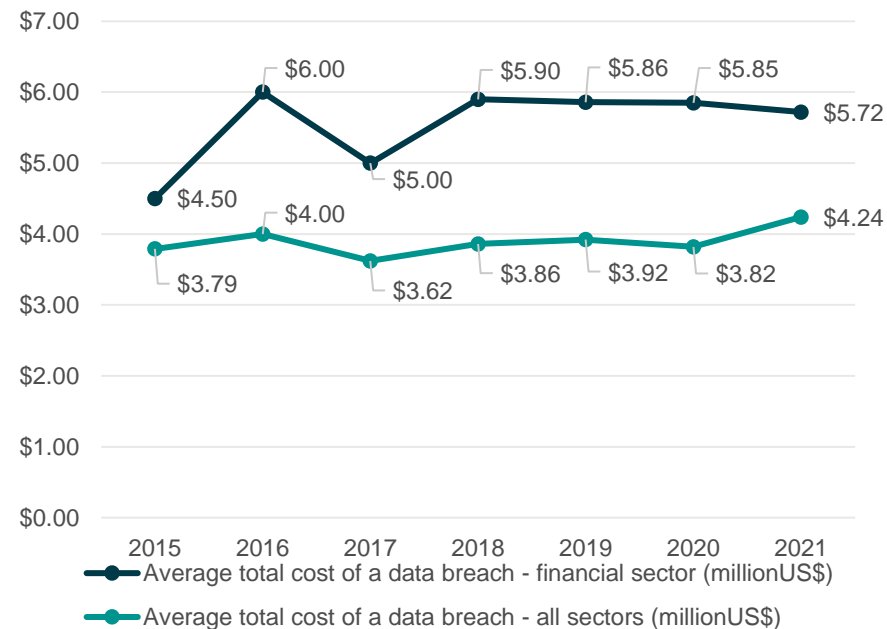
In the United States, data from the Federal Trade Commission (2020) show that reports of scams started on social media and money lost through such scams rose massively between 2016 and 2020.

In developing and emerging countries, there have been several media reports about people being defrauded through social media scams. But data to assess the evolution of scams are not readily available.

OTHER EXAMPLES: THE EVOLVING SCALE OF DFS CONSUMER RISKS

Lost business accounted for the largest proportion of breach costs, indicating that data breaches may lead to a loss of confidence in the formal financial sector

Average total cost of a data breach, 2015–2021



Source: Adapted from IBM's Cost of a Data Breach reports, 2016 to 2021.

Although the average total cost of a data breach has not massively increased since 2015, the financial sector has persistently recorded a higher average total cost than all other sectors. However, it is worth noting that between 2020 and 2021, the average cost of a data breach for all sectors increased by 11 percent while the average cost in the financial sector reduced by 2.2 percent. This slight improvement in the financial sector may be attributed to improved cyber security measures adopted by players involved.

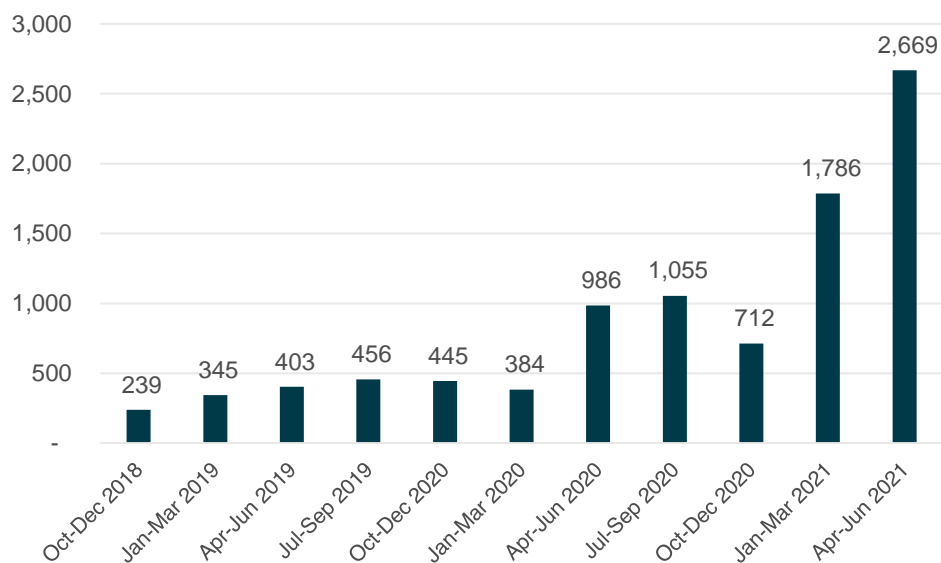
To calculate the total cost of a data breach, IBM considers expenses such as providing full credit monitoring subscriptions, discounts for future products/sales, and lost business/customers.

In 2020–2021, at 38 percent, lost business accounted for the largest proportion of breach costs. This may indicate to the financial inclusion community that exposing customer data would result in loss of confidence in the financial sector and ultimately contribute to financial exclusion.

OTHER EXAMPLES: THE EVOLVING SCALE OF DFS CONSUMER RISKS

Complaints about digital wallets and mobile payments are on the rise but consumer protection measures are not keeping up

Mobile or digital wallet complaints in the United States, 2017–2021



Source: Compiled by the authors based on data from CFPB's consumer complaints database.

An analysis of mobile/digital wallet complaints received by the Consumer Financial Protection Bureau (CFPB 2021)* shows a massive increase in complaints after March 2020, coinciding with the first wave of the COVID-19 pandemic. Of 9,480 complaints received between October 2018 and June 2021, 76 percent (7,208) were reported after March 2020. Complaints linked to managing/opening/closing a mobile wallet account made up the largest proportion (45 percent), followed by fraud/scams (23 percent) and unauthorized transactions (22 percent).

Mierzwinski et al. (2021) notes that while payment app websites warn consumers about scams, [they provide very little recourse](#) for fraud victims. Furthermore, unlike credit cards – which are regulated under the Truth In Lending Act and the Fair Credit Billing Act – and debit cards – which are covered under the Electronic Fund Transfer Act (EFTA) – there are no regulations for P2P transactions. Although the EFTA extends to P2P transactions, it may not always apply.

Considering that a developed country like the United States has such redress issues, we infer that problems may be worse in developing and emerging countries.

* An independent entity in the United States, CFPB is responsible for consumer protection in the financial sector. CFPB deals with complaints that FSPs fail to resolve.

EXAMPLES: SOLUTIONS TO MITIGATE DFS CONSUMER RISKS

Most emerging solutions involve the application of technology.

Please note: Examples in this section are anecdotal as the research did not focus on solutions.

Artificial intelligence (AI) fraud detection systems may help detect and mitigate fraud (Experian 2020; FSB 2017; Calzolari 2021). Additionally, supervisors can use AI to monitor fraud in the financial sector.

For example:

- The Australian Securities and Investments Commission (ASIC) uses natural language processing (NLP) and other technologies to identify and extract entities of interest.
- The Monetary Authority of Singapore (MAS) is exploring the use of AI and machine learning for analysis and identification of suspicious transactions that warrant further attention.
- The United States Securities and Exchange Commission (SEC) uses big data analytics and machine learning algorithms to detect possible fraud and misconduct.

Sensitization by financial sector supervisors and law enforcement agencies has helped mitigate fraud in some cases. For example, 2020 media reports* indicate that United Arab Emirates experienced a drop in SIM swap fraud after the country's Central Bank and police launched a major nationwide awareness campaign.

* Reports including [Emirates News Agency](#), [WAM](#), [Emirati News](#), and [Gulf News](#).

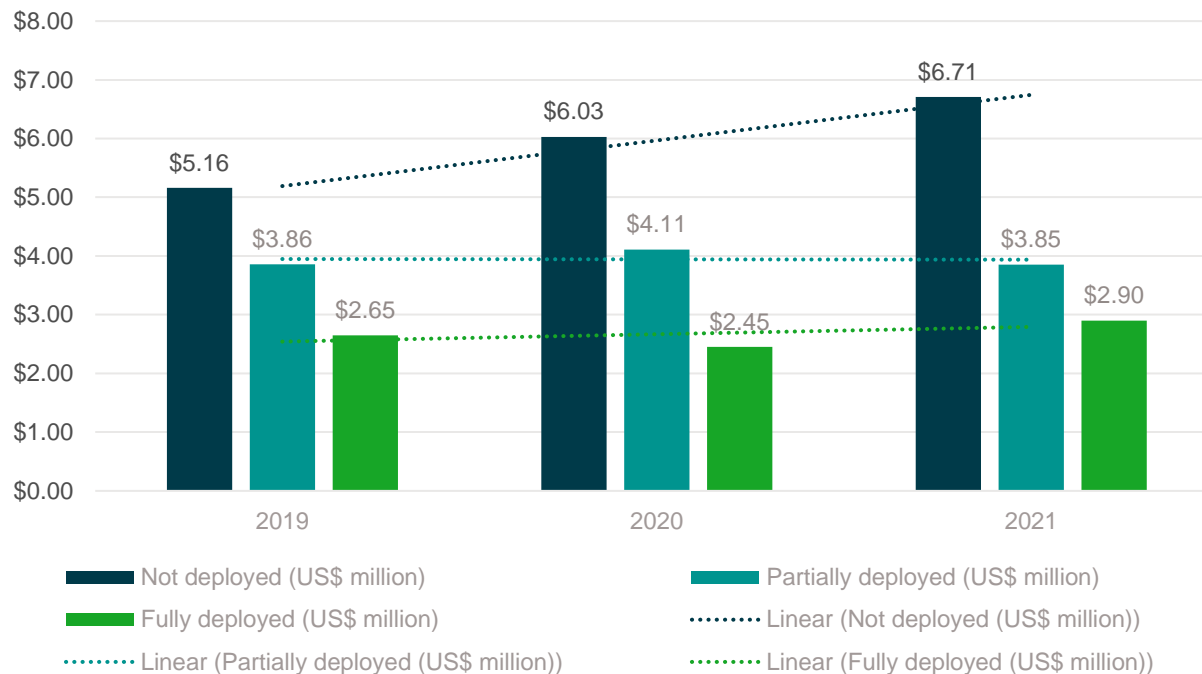
Based on research by [Buku and Mazer \(2017\)](#), CGAP recommends the following measures to mitigate fraud in mobile financial services:

- Comprehensive fraud management programs
- Compliance monitoring and agent recruitment, training and management programs
- Incorporating product risk assessment into risk management programs
- Comprehensive agent fraud prevention measures (e.g., training and sensitization)
- Provision of an effective complaints channel
- Effective staff recruitment

EXAMPLES OF SOLUTIONS TO MITIGATE DFS CONSUMER RISKS

Investment in security AI and automation can significantly reduce the average time to identify and respond to a data breach

Average cost of a data breach by security AI deployment level



IBM's [Cost of a Data Breach Report 2021](#) shows that companies with security AI (e.g., fraud detection systems) and automation take fewer days to identify and contain a data breach. For example, in 2021 it took companies with security AI and automation an average of 247 days to detect and contain a data breach, compared with 324 days for those that had not deployed a system.

Additionally, companies that deployed security AI and automation experienced 80 percent lower average costs associated with a data breach in 2021 (US\$2.91 million) than those with no system in place (US\$6.71 million).

Companies without security AI and automation also experienced a larger increase in the cost of data breaches over a three-year period.

Source: Adapted from IBM's Cost of a Data Breach Report 2021.

EXAMPLES OF SOLUTIONS TO MITIGATE DFS CONSUMER RISKS

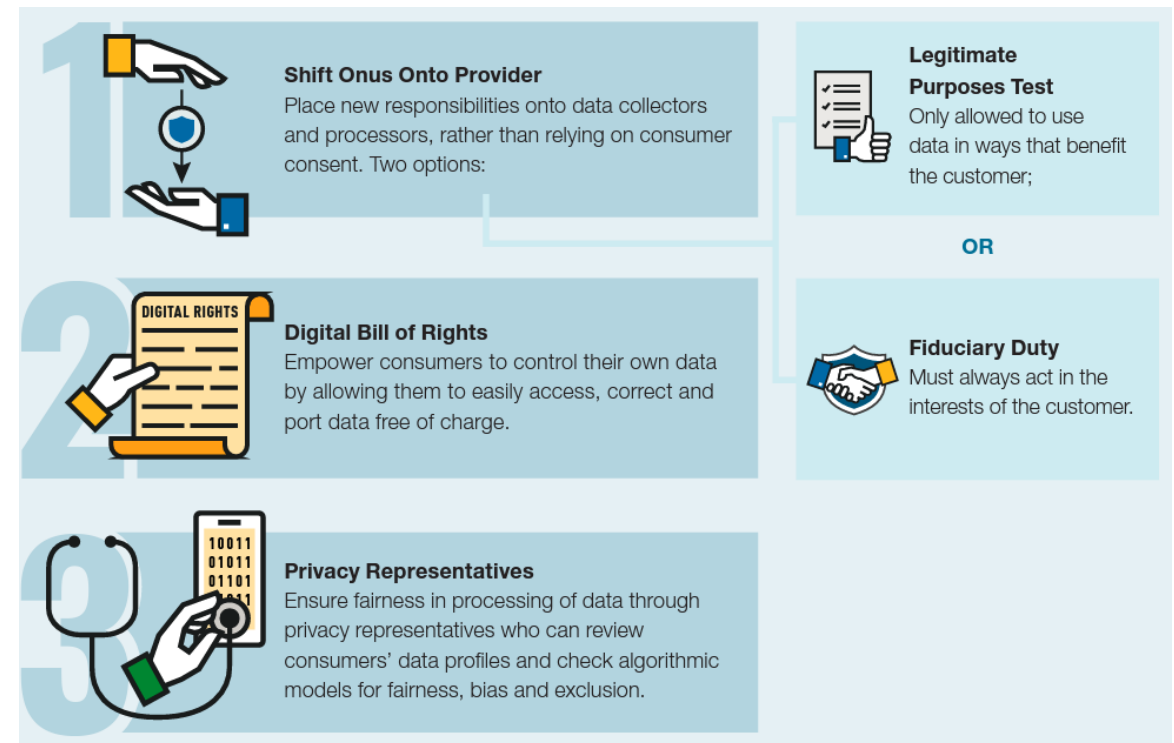
Other solutions to mitigate data misuse

Approaches to mitigate algorithmic bias

Adopt national AI strategies that incorporate ethical considerations. In 2017, Canada became the first country to publish a national AI strategy. By December 2020, more than 30 additional countries, including China, Japan, France, Germany, India, Mexico, Estonia, the United States, Russia, and Indonesia, had published similar strategies. Others, including Brazil, Argentina, Kenya, and Malaysia, have announced plans to develop AI strategies (Daniel et al. 2021).

Conduct algorithmic audits. In 2020 a U.S. federal court ruled that “independent research aimed at uncovering whether online algorithms result in racial, gender, or other discrimination does not violate the Computer Fraud and Abuse Act” (Rizzi et al. 2021; Deloitte 2020; Kassir 2020; Calzolari 2021; Andrews 2021, FSB 2017). However, algorithmic audits require skills and expertise that most auditors and financial supervisors currently do not have.

Based on research by [Medine and Murthy \(2020\)](#), CGAP recommends:



EXAMPLES OF SOLUTIONS TO MITIGATE DFS CONSUMER RISKS

Consumers, DFS providers, and supervisors can leverage social media for complaints management and to identify key consumer protection issues

Examples of “social listening” tools: analytics dashboards within social media platforms and commercial tools

Innovation for Poverty Action (IPA) and Citibeats (2021) collected social media data in Nigeria, Kenya, and Uganda from Twitter, Facebook, and the Google Play Store to understand problems faced by DFS consumers.

Using 4.5 million social media messages collected from commercial banks, telecommunication companies, fintech startups, and microfinance institutions between July 1, 2019 and July 1, 2020, text analysis and human input identified key issues consumers faced. Inter alia, they found that:

- Twitter and Facebook are mainly used by DFS users to report consumer protection issues, particularly those related to customer care. Google Play is used to report operational failures.
- Service providers respond when customers post issues on social media, but response rates vary considerably. Provider response rates are higher on Facebook (5 to 46 percent) and Google Play (8 to 58 percent) than on Twitter (0.04 to 1.2 percent).

In the Philippines, a chatbot solution called BSP’s Online Budd allows customers to file complaints via social media and other communications platforms. The chatbot uses AI technologies, such as machine learning and NLP, to process complaints and directly respond or escalate to a call center that files complaints to a central database (Duflos, Griffin, and Valenzuela 2021).

According to a survey by the American Bankers Association, 63 percent of banks already use social media to monitor complaints for risk management purposes while 12 percent intend to do so within one or two years (World Bank 2019).

However, using social media may introduce other risks for DFS providers and consumers (see the Federal Financial Institutions’ Examination Council’s 2013 social media guidance). Additionally, social media is not effective for less tech-savvy consumers, such as low-income women and rural populations who normally do not use it.

CGAP recently conducted a study and used social media data from Twitter and the Google Play Store to identify key issues that affect digital credit borrowers in India.

The study employed NLP and applied the consumer risk typology discussed in this paper to categorize consumer issues in India (Duflos et al. 2021a, 2021b).

EXAMPLES OF SOLUTIONS TO MITIGATE DFS CONSUMER RISKS

Financial education programs may mitigate some risks, but this depends on the mode of delivery

According to the OECD (2017), few DFS-focused financial education programs address the needs of vulnerable groups.

Armenia (rural)

Impact of two-day financial education workshops

- In the short term, the workshops had a positive and significant impact on financial literacy and trust (AFI 2018).
- After six months, short-term positive and significant impact diminished, implying negligible long-term impact (AFI 2020).

Malawi (urban)

Impact of financial literacy-focused interactive voice response (IVR) module informing customers of the importance of understanding loan terms, repayment, and fees

- The IVR module improved knowledge of loan fees and loan repayment in the short term and increased borrowing.
- There was also some evidence of improvements in borrowers' well-being (Robinson and Dupas 2020).

Tanzania (rural)

Impact of interactive SMS-customized learning content based on consumers' preferences and responses

- Farmers who accessed the learning platform saved at rates over five times greater than those who did not access the platform.
- Farmers who accessed the learning platform took out larger loans and had a higher repayment than those who did not.
- Farmers who viewed more screens had more financial activity (Mazer 2016).

REFERENCES

REFERENCES

Accenture. 2018. “[Unmask Digital Fraud. Today. Boosting Customers’ and Companies’ Defense Against Digital Fraud.](#)” White paper.

AFI. 2017. “[Digitally Delivered Credit: Consumer Protection Issues and Policy Responses to New Models of Digital Lending.](#)” AFI Consumer Empowerment and Market Conduct (CEMC) Working Group, Responsible Lending Sub-Group. Policy Guidance Note and Results from Regulators Survey.

AFI. 2018. “[The Effectiveness of Short-term Financial Education Workshops in Rural Areas: The Case of Armenia.](#)” Case study.

AFI. 2020. “[The Long-term Effectiveness of Financial Education Classroom Workshops in Rural Areas: The Case of Armenia.](#)” Case study.

Ahlström, Richard, and Fredrik Tjulander. 2020. “[Insolvency Syndrome: When Over-indebtedness Affects Health and Wellbeing.](#)” Finance Watch blog post.

Ahmed, Wajiha, and Natalia Gomes. 2015. “[Papayas and Digital Finance: Emerging Consumer Risks in Colombia.](#)” CGAP blog post.

Aite Group. 2021. “[Synthetic Identity Fraud: Diabolical Charge-Offs on the Rise.](#)” Report.

American Bankers Association. 2019. “[Social Media in Banking 2019 Report.](#)” Report.

Andrews, Dorothy. 2021. “[Algorithmic Accountability.](#)” National Association of Insurance Commissioners.

Annan, Francis. 2021. “[Gender and Financial Misconduct: A Field Experiment on Mobile Money.](#)” Georgia State University research paper.

Assolini, Fabio, and Andre Tenreiro. 2019. “[Large-scale SIM Swap Fraud.](#)” Securelist research.

Baur-Yazbeck, Silvia, and Jean-Louis Perrier. 2020. “[Regional Centers Can Help Low-Income Countries Build Cyber Resilience.](#)” CGAP blog post.

Baur-Yazbeck, Silvia, David Medine, and Jean-Louis Perrier. 2020. “[Cybersecurity Resource Centers for the Financial Sector: A Proposed Business Concept.](#)” CGAP FinDev Gateway slide deck.

BBC. 2020a. “[Chinese Phones with Built-in Malware Sold in Africa.](#)” Article.

BBC. 2020b. “[U.S.-Government-issued Phones Run ‘Chinese Malware.’](#)” Article.

Better than Cash Alliance. 2021. [UN Principles for Responsible Digital Payments: Building Trust, Mitigating Risks and Driving Inclusive Economies](#)

Bharadwaj, Prashant, William Jack, and Tavneet Suri. 2019. “[Fintech and Household Resilience to Shocks: Evidence from Digital Loans in Kenya.](#)” NBER Working Paper 25604.

Biallas, Margarete, Momina Aijazuddin, and Lory Camba Opem. 2019. “[The Case for Responsible Investing in Digital Financial Services.](#)” IFC EMCompass Note 67.

BIS. 2019. “[Welfare Implications of Digital Financial innovation.](#)” Remarks by Luiz Awazu Pereira da Silvaat, Santander International Banking Conference, Madrid. Speech.

Bleszynska Katya. 2021. “[Ponzi and Pyramid Schemes Spread Across Caribbean.](#)” InSight Crime article.

Bold, Chris, and Rashmi Pillai. 2016. “[The Impact of Shutting Down Mobile Money in Uganda.](#)” CGAP blog post.

REFERENCES

Boshmaf, Yazan, Charitha Elvitigala, Husam Al Jawaheri, Primal Wijesekera, and Mashael Al Sabah. 2019. “[Investigating MMM Ponzi Scheme on Bitcoin](#).” Technical Report.

Boyd, Mark. 2020. “[Digital Finance APIs Come with Risks – Here’s One Way to Manage Them](#).” CGAP blog post.

Bradsher, Keith, and Ailin Tang. 2017. “[China to Debtors: Pay Up or Be Shamed](#).” New York Times article.

Breza, Emily, Martin Kanz, and Leora Klapper. 2017. “[The Real Effects of Electronic Wage Payments: First Results](#).” International Growth Centre paper F-31407-BGD-1.

Buguroo. 2019. “[Online Banking Fraud in Latin America: An Emerging Regional Threat](#).” White paper.

Buku, Mercy, and Rafe Mazer. 2017. “[Fraud in Mobile Financial Services](#).” CGAP Brief.

Calzolari, Giacomo. 2021. “[Artificial Intelligence Market and Capital Flows](#).” Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament, Luxembourg. Study.

Carnegie Endowment for International Peace. 2020. “[Timeline of Cyber Incidents Involving Financial Institutions](#).”

Carr, Brad, Pablo Urbiola, and Adrein Delle-Case. 2018. “[Liability and Consumer Protection in Open Banking](#).” Institute of International Finance report.

CCAF, World Bank Group, and WEF. 2020. “[The Global COVID-19 FinTech Market Rapid Assessment Study](#).” Report.

CEGA. 2016. “[Access to Digital Credit and Its Spillover Effects in China](#).” Digital Credit Observatory (DCO) Results Brief.

CEGA. 2020. “[Can Digital Credit Work for Agriculture? Lessons from Kenya and Uganda](#).” CEGA interview.

Central Bank of Kenya, Kenya National Bureau of Statistics, and FSD Kenya. 2019. “[FinAccess Household Survey: Access, Usage, Quality and Impact](#).” Report.

CGAP and MSC. 2020. “[Cash-in Cash-Out Cross-Country Analysis India](#).” Slide deck.

CGAP. 2018. “[Financial Inclusion Insights Analytics: Côte D’Ivoire](#).” FinDev Gateway slide deck.

CGAP. [Cybersecurity and Financial Inclusion: Protecting Customers, Building Trust](#). CGAP blog series.

Chalwe-Mulenga, Majorie, and Eric Duflos. 2021. “[The Evolving Nature and Scale of Consumer Risks in Digital Finance](#).” CGAP blog post.

Chamboko, Richard, Robert Cull, Xavier Gine, Soren Heitmann, Fabian Reitzug, and Morne Van Der Westhuizen. 2020. “[The Role of Gender in Agent Banking: Evidence from the Democratic Republic of Congo](#).” IFC and World Bank Policy Research Working Paper 9449.

Chen, Greg, and Rafe Mazer. 2016. “[Instant, Automated, Remote: The Key Attributes of Digital Credit](#).” CGAP blog post.

Cheng, We Geng, Rodrigo de Oliveira Leite, and Fabio Caldieraro. 2021. “[Financial Contagion in Internet Lending Platforms: Who Pays the Price?](#)” Finance Research Letters.

REFERENCES

Chinese Academy of Financial Inclusion (CAFI). 2018. [“Growing with Pain: Digital Financial Inclusion in China.”](#) FinDev Gateway. Report.

Chivukula, Chinmayanand. 2021. [“Consumer Grievance Redress in Financial Disputes in India.”](#) Dvara Research.

Chugh, Beni. 2019. [“Financial Regulation of Consumer-facing Fintech in India: Status Quo and Emerging Concerns.”](#) Dvara Research Working Paper Series No. WP-2019-01.

Cisco. 2020. [“Cisco Annual Internet Report \(2018–2023\).”](#) White paper.

CNN Philippines. [“SEC Shuts Down 11 More Online Lenders.”](#) Article.

Coetzee, Gerhard. 2019. [“It’s Time to Change the Equation on Consumer Protection.”](#) CGAP Leadership Essay.

Consumer Financial Protection Bureau (CFPB). 2021. [“Consumer Complaint Database: Complaints by Sub-products, by Date Received by the CFPB.”](#) Database.

Consumers International. 2017. [“Banking on the Future: An Exploration of FinTech and the Consumer Interest.”](#) Report.

Consumers International. 2019. [“Social Media Scams: Understanding the Consumer Experience to Create a Safer Digital World.”](#) Report.

Consumers International. 2021. [“The Role of Consumer Organisations to Support Consumers of Financial sServices in Low and Middle Income Countries.”](#) Consumers International and CGAP report.

Dabo, Mohamed. [“Mobile Banking Statistics: The Future of Money Is in the Palm of Your Hand.”](#) DataProt Retail Banker International Report.

Deloitte. 2020. [“Algorithm Assurance: Ensuring that Algorithms Are Working as Needed.”](#) Deloitte Malta report.

Duflos Eric, Daryl Collins, Jayshree Venkatesan, and Juan Carlos Izaguirre. 2021b. [“Analyzing Social Media to Spot Digital Consumer Credit Risks in India.”](#) CGAP blog post.

Duflos, Eric, Jayshree Venkatesan, Amulya Neelam, and Sarah Stanley. 2021a. [“Digital Consumer Credit in India – Time to Take a Closer Look.”](#) CGAP blog post.

Duflos, Eric, Mary Griffin, and Myra Valenzuela. 2021. [“Elevating the Collective Consumer Voice in Financial Regulation.”](#) CGAP Working Paper.

Dvara Research. 2020. [“Future of Finance Initiative Conference Series 2019: Regulating Data-driven Finance.”](#) Conference proceedings.

ESMA, EBA, and EIOPA. 2016. [“Joint Committee Discussion Paper on the Use of Big Data by Financial Institutions.”](#) Joint Committee of the European Supervisory Authorities Discussion Paper.

European Commission. 2016. [“Assessment of Current and Future Impact of Big Data on Financial Services.”](#) Financial Service User Group paper.

Europol. 2020a. [“Internet Organised Crime Threat Assessment \(IOCTA\) 2020.”](#) European Union Agency for Law Enforcement Cooperation document.

Europol. 2020b. [“The SIM Hijackers: How Criminals Are Stealing Millions by Hijacking Phone Numbers.”](#) European Union Agency for Law Enforcement Cooperation article.

Experian. 2020. [“2020 Global Identity and Fraud Report.”](#)

Experian. 2021. [“2021 Global Identity and Fraud Report.”](#)

REFERENCES

Fahsbender Frederick. 2019. "[A WhatsApp Audio Links Actress Jasmine Stuart with the Loom of Abundance.](#)" Infobae article.

Farooq, Saad. 2019. "[Mitigating Common Fraud Risks: Best Practices for the Mobile Money Industry.](#)" GSMA paper.

Faux, Zeke. 2020. "[Tech Startups Are Flooding Kenya with Apps Offering High-Interest Loans.](#)" Bloomberg Businessweek article.

Federal Financial Institutions Examination Council. 2013. "[Social Media: Consumer Compliance Risk Management Guidance.](#)" Press release.

Federal Reserve Banks. 2021. "[Synthetic Identity Fraud Defined.](#)" Blog post.

Federal Trade Commission. 2020. "[Scams Starting on Social Media Proliferate in Early 2020.](#)" Consumer Protection Data Spotlight.

Ferreira, Mário, Filipa de Almeida, Jerônimo Soro, Márcia Maurer Herter, Diego Costa Pinto, and Carla Sofia Silva. 2021. "[On the Relation Between Over-Indebtedness and Well-Being: An Analysis of the Mechanisms Influencing Health, Sleep, Life Satisfaction, and Emotional Well-Being.](#)" Frontiers in Psychology paper.

FICO. 2018. "[FICO Survey: 6 in 10 APAC Banks Say Use of Fraudulent 'Synthetic Identities' on the Rise.](#)" Survey.

National Financial Inclusion Strategy (SNKI). 2018. [Financial Inclusion Insights \(FII\) Indonesia.](#) Report

Francis, Eilin, Joshua Blumenstock, and Jonathan Robinson. 2017. "[Digital Credit: A Snapshot of the Current Landscape and Open Research Questions.](#)" Centre for Effective Global Action and Bill & Melinda Gates Foundation research report.

Frost, Jon, Leonardo Gambacorta, and Romina Gambacorta. 2020. "[The Matthew Effect and Modern Finance: On the Nexus Between Wealth Inequality, Financial Development, and Financial Technology.](#)" BIS Working Paper No 871.

FSB. 2017. "[Artificial Intelligence and Machine Learning in Financial Services.](#)" Report.

FSD Kenya. 2019. "[Digital Credit in Kenya: Facts and Figures from FinAccess 2019.](#)" Focus Note.

Fu, Jonathan, and Mrinal Mishra 2020b. "[Fintech in the Time of COVID-19: Trust and Technological Adoption During Crises.](#)" Swiss Finance Institute Research Paper No. 20–38.

Fu, Jonathan, and Mrinal Mishra. 2020a. "[Combating the Rise in Fraudulent Fintech Apps.](#)" Center for Financial Inclusion blog post.

Garz, Seth, Xavier Giné, Dean Karlan, Rafe Mazer, Benjamin N. Roth, Rebecca Rouse, Caitlin Sanford, and Jonathan Zinman. 2021. "[Consumer Financial Protection in Lower-Income Countries: A Review of the Evidence and Directions for Future Research.](#)" NBER Working Paper 28262.

Genga, Kevin, Wanjiku Kiarie, and Vera Bersudskaya. 2018. "[Measuring Risk in Agent Networks: What Risks Are Inherent in Agency Business and How to Track Them.](#)" MicroSave Helix Institute of Digital Finance paper.

Gibbins Wesley. 2020. "[The Caribbean's Pandemic Pyramids and Ponzis.](#)" The Caribbean Investigative Journalism Network article.

Google Next Billion Users. 2021. "[New Internet Users: Similar and Very Different.](#)" Research.

REFERENCES

GPFI. 2020. “[Advancing Women’s Digital Financial Inclusion.](#)” BTCA, Women’s World Banking, and World Bank Group report.

GSMA. 2020. “[MTN MoMo Pay Merchant Payments: Expanding Female Mobile Money Usage in Ghana.](#)” Connected Women Case Study.

Harihareswara, Nandini, Zerubabel Junior Kwebiiha, Brian Katimbo, Anne Duijnhouwer, and Moira Favrichon. 2019. “[State of the Digital Financial Services Market in Zambia, 2018.](#)” UNCDF and BoZ report.

Hayes, Marianne. 2020. “[The Many Different Forms of Identity Theft.](#)” Experian blog post.

Henderson, Roxanne, and Loni Prinsloo. 2021. “[South African Brothers Vanish, and So Does \\$3.6 Billion in Bitcoin.](#)” Bloomberg Wealth article.

Holly, Isaac, Kilyelyani Kanjo, Brian Katimbo, Anne Duijnhouwer, Moira Favrichon, and Mali Kambandu. 2020. “[State of the Digital Financial Services Market in Zambia, 2019: Results from the UNCDF Annual Provider Survey.](#)” UNCDF and BoZ report.

Huang Li, Li Oliver Zhen, Lin Yupeng, Xu Chao and Xu Haoran. 2021. “[Gender and Age-based Investor Affinities in a Ponzi Scheme.](#)” Article.

Hurly, Mikella, and Julius Adebayo. 2017. “[Credit Scoring in the Era of Big Data.](#)” Yale Journal of Law and Technology article.

IBM. 2020. “[Cost of a Data Breach Report 2020.](#)” IBM Security and Ponemon Institute report.

IBM. 2021. “[Cost of a Data Breach Report 2021.](#)” IBM Security and Ponemon Institute report.

IDEO.org and the Bill & Melinda Gates Foundation. 2019. “[Women and Money: Insights and a Path to Close the Gender Gap.](#)” Report.

IDEO.org. 2020. “[Measuring and Designing for Women’s Financial Empowerment. Increasing Women’s Voice, Influence, and Control of Money.](#)”

IFC. 2018. “[Closing the Gender Gap: Opportunities for the Women’s Mobile Financial Services Market in Bangladesh.](#)” Report.

IMF. 2020. “[Digital Financial Services and the Pandemic: Opportunities and Risks for Emerging and Developing Economies.](#)” IMF Special Series on COVID-19.

Institute and Faculty of Actuaries (UK) 2017. “[Data Science in Insurance: Opportunities and Risks for Consumers.](#)” Policy Briefing.

Interpol. 2021. “[ASEAN Cyberthreat Assessment 2021: Key Cyberthreat Trends Outlook from the ASEAN Cybercrime Operations Desk.](#)”

IPA and Citibeats. 2021. “[Social Media Usage by Digital Finance Consumers: Analysis of Consumer Complaints in Kenya, Nigeria, and Uganda. July 2019–July 2020.](#)” IPA study.

IPA and Competition Authority of Kenya. 2021. “[Kenya Consumer Protection in Digital Finance Survey.](#)”

IPA and Uganda Communications Commission. 2021. “[Uganda Consumer Protection in Digital Finance Survey.](#)”

IPA. 2021. “[Nigeria Consumer Protection in Digital Finance Survey.](#)”

ITU. 2016. “[Commonly Identified Consumer Protection Themes for Digital Financial Services.](#)” ITU-T Focus Group Digital Financial Services.

REFERENCES

ITU. 2020. “[Unlicensed Digital Investment Schemes \(UDIS\)](#).” Financial Inclusion Global Initiative (FIGI) Security, Infrastructure, and Trust Working Group report.

Izaguirre, Juan Carlos, Denise Dias, Eric Duflos, Laura Newbury Brix, Olga Tomilova, and Myra Valenzuela. 2022. “[Market Monitoring for Financial Consumer Protection](#).” CGAP toolkit.

Izaguirre, Juan Carlos, Michelle Kaffenberger, and Rafe Mazer. 2018. “[It’s Time to Slow Digital Credit’s Growth in East Africa](#).” CGAP blog post.

Izaguirre, Juan Carlos, Rafe Mazer, and Louis Graham. 2018. “[Digital Credit Market Monitoring in Tanzania](#).” CGAP slide deck.

Izaguirre, Juan Carlos. 2020. “[Making Consumer Protection Regulation More Customer-Centric](#).” CGAP Working Paper.

Jenik, Ivo, Timothy Lyman, and Alessandro Nava. 2016. “[Will Crowdfunding Help Financial Inclusion of Unserved Crowds?](#)” CGAP blog post.

Kabir, Raiyan, and Jeni Klugman. “[Women’s Financial Inclusion in a Digital World: How Mobile Phones Can Reduce Gender Gaps](#).” Georgetown Institute for Women, Peace and Security report.

Kafeero, Stephen. 2020. “[Uganda’s Banks Have Been Plunged Into Chaos by a Mobile Money Fraud Hack](#).” Quartz Africa article.

Kaffenberger, Michelle, Edoardo Totolo, and Matthew Soursourian. 2018. “[A Digital Credit Revolution: Insights from Borrowers in Kenya and Tanzania](#).” CGAP Working Paper.

Kaffenberger, Michelle. 2018. “[Digital Credit in Tanzania: Customer Experiences and Emerging Risks](#).” CGAP.

Kassir, Sara. 2020. “[Algorithmic Auditing: The Key to Making Machine Learning in the Public Interest](#).” IBM Center for the Business of Government Viewpoints article.

Kelly, Sonja, and Mehrdad Mirpourian. 2021. “[Algorithmic Bias, Financial Inclusion, and Gender](#).” Women’s World Banking.

Kiarie, Nancy, Ian Odongo, and Vera Bersudskaya. 2018. “[Fitting the Pieces of the Liquidity Management Puzzle](#).” MicroSave Helix Institute of Digital Finance paper.

Korobov Gustav. 2020. “[Open Banking as a World of Open Opportunities and Hidden Risks](#).” Finextra blog post.

KPMG. 2019a. “[Consumer Loss Barometer: The Economics of Trust](#).” Survey.

KPMG. 2019b. “[Global Banking Fraud Survey](#).” Survey.

Kumari Tanwi. 2020. “[Client Perspectives on Consumer Protection: Analysis of a Client Survey in Cambodia](#).” Center for Financial Inclusion Brief.

Levi, Michael, and Russell Smith. 2021. [Fraud and Its Relationship to Pandemics and Economic Crises: From Spanish flu to COVID-19](#). Australian Institute of Criminology research report.

LexisNexis Risk Solutions. “[What Is Synthetic Fraud?](#)” LexisNexis article.

REFERENCES

Mashal, Mujib, and Hari Kumar. 2021. [“Using Shame, Lending Apps in India Squeeze Billions Out of the Desperate.”](#) New York Times article.

Masino, Serena, and Miguel Niño-Zarazúa. 2014. [“Social Service Delivery and Access to Financial Innovation. The Impact of Oportunidades’ Electronic Payment System in Mexico.”](#) World Institute for Development Economics Research Working Paper, Series No. 2014/034.

Maynard, Nick, and Susan Morrow. 2021. [“Online Payment Fraud: Emerging Threats, Segment Analysis, Market Forecasts – 2021–2025.”](#) Juniper research.

Mazer, Rafe, and Dan Onchieku. 2019. [“Did You See My Tweet: Monitoring Financial Consumer Protection Via Social Media.”](#) FSD Kenya.

Mazer, Rafe, and Kate McKee. 2017. [“Consumer Protection in Digital Credit.”](#) CGAP Focus Note.

Mazer, Rafe. 2016. [“Interactive SMS Drives Digital Savings and Borrowing in Tanzania.”](#) CGAP blog post.

Mazer, Rafe. 2018. [“Kenya’s Rules on Mobile Money Price Transparency Are Paying Off.”](#) CGAP blog post.

McKee, Katharine, Michelle Kaffenberger, and Jamie M. Zimmerman. 2015. [“Doing Digital Finance Right: The Case for Stronger Mitigation of Customer Risks.”](#) CGAP Focus Note.

Medine David. 2020. [“Financial Scams Rise as Coronavirus Hits Developing Countries.”](#) CGAP Blog Series: Coronavirus (COVID-19): Financial Services in the Global Response.

Medine, David, and Gayatri Murthy. 2020. [“https://www.cgap.org/research/publication/making-data-work-poor.”](https://www.cgap.org/research/publication/making-data-work-poor) CGAP Focus Note.

Medine, David. 2017. [“India Stack: Major Potential but Mind the Risks.”](#) CGAP blog post.

Mehrotra, Aakash, Akhand Tiwari, Karthick Morchan, Mimansa Khanna, and Vivek Khanna. 2018. [“State of the Agent Network, India 2017.”](#) MicroSave Helix Institute of Digital Finance, India Country Report.

Mierzwinski, Ed, Teresa Murray, and Mike Litt. 2021. [“Virtual Wallets, Real Complaints: How Digital Payment Apps Put Consumers’ Cash At Risk – An Analysis of CFPB Complaints.”](#) U.S. PIRG Education Fund Report.

Mishra, Saurabh, Jack Clark, and C. Raymond Perrault. 2020. [“Measurement in AI Policy: Opportunities and Challenges.”](#) Research report.

Mohammad, Ghiyazuddin, and Alfa Pelupessy. 2017. [“Emerging Risks and Customer Protection in Digital Financial Services in Indonesia.”](#) MicroSave research.

Mondato. 2019. [“The Inclusion Illusion: Financial Health In Kenya.”](#) Blog post.

Mondato. 2019. [“The Inclusion Illusion: Financial Health In Kenya.”](#) Blog post.

Mondato. 2021. [“Digital Lending’s Self-regulation: A Redemption Story?”](#) Blog post.

Mukharji, Arunoday. 2021. [“The ‘Saviour’ Loan Apps That Trapped Pandemic-struck Indians.”](#) BBC article.

Munyegera, Ggombe Kasim, and Tomoya Matsumoto. 2017. [“ICT for Financial Access: Mobile Money and the Financial Behavior of Rural Households in Uganda.”](#) Review of Development Economics article.

Mureithi, Carlos. 2021. [“Inside Africa’s Biggest Cryptocurrency Scams.”](#) Quartz Africa article.

REFERENCES

Mustafa, Zeituna, Mercy Wachira, Vera Bersudskaya, William Nanjero, and Graham A.N. Wright. 2017. "Where Credit Is Due: Customer Experience of Digital Credit in Kenya." MicroSave report.

Mustafa, Zeituna, Mercy Wachira, Vera Bersudskaya, William Nanjero, and Graham A.N. Wright. 2017. "Where Credit is Due Customer Experience of Digital Credit in Kenya." MicroSave.

Ndauti, Hildah. 2018. "Cyber Security in Emerging Financial Markets." CGAP FinDev Gateway publication.

Niño, Jonas Lopez, Jan Langthaler, Marcos Fabian, and Joaquin Mayorga. 2017. "An Overview of FinTechs: Their Benefits and Risks." Association of Supervisors of Banks of the Americas.

OECD. 2017. "G20/OECD INFE Report: Ensuring Financial Education and Consumer Protection for All in the Digital Age." Report.

OECD. 2019. "Good Practice Guide on Consumer Data." OECD Digital Economy Paper No. 290.

OECD. 2020a. "Personal Data Use in Financial Services and the Role of Financial Education: A Consumer- Centric Analysis." Report.

OECD. 2020a. "Personal Data Use in Financial Services and the Role of Financial Education: A Consumer- Centric Analysis."

OECD. 2020b. "The Impact of Big Data and Artificial Intelligence (AI) in the Insurance Sector." Report.

OECD. 2020b. "The Impact of Big Data and Artificial Intelligence (AI) in the Insurance Sector."

OECD. 2020c. "Financial Consumer Protection Policy Approaches in the Digital Age: Protecting Consumers' Assets, Data, and Privacy."

Outseer. 2021. "Outseer Fraud and Payments Report: Digital Transaction Insights from the Outseer Global Data Network," Q2 2021.

Owens, John. 2018. "Responsible Digital Credit: What Does Responsible digital Credit Look Like?" Center for Financial Inclusion.

Palepu, Advait. 2021. "Troves of Data Stolen by Fake Digital Lending Apps." Menianama article.

Parkin, Benjamin, and Mercedes Ruehl. 2021. "Asian Authorities Clamp Down on Digital Lenders." Financial Times article.

Pazarbasioglu, Ceyla, Alfonso Garcia Mora, Mahesh Uttamchandani, Harish Natarajan, Erik Feyen, and Mathew Saal. 2020. "Digital Financial Services." World Bank Group report.

Political Economy Research Centre. 2015. "Financial Melancholia – Mental Health and Indebtedness." Report.

Prabhakar, Tarunima. 2020. "A New Era for Credit Scoring: Financial Inclusion, Data Security, and Privacy Protection in the Age of Digital Lending." UC Berkeley Centre for Long-term Cybersecurity.

Prakarsa Policy Brief. 2020. "The Risk of Over-indebtedness Amid COVID-19 Pandemic."

REFERENCES

Prakarsa. 2020. [“The Risk of Over-indebtedness Amid COVID-19 Pandemic.”](#) Policy brief.

Priezkalns, Eric. 2021. [“Are SIM Swaps Rising? Freedom of Information Disclosure Shows UK Police Figures Are Unreliable.”](#) CommsRisk blog post.

Ramanathan, Arundhati. 2021. [“India’s Instant Loan App Crisis Is Made in China.”](#) The Ken article.

Reaves, Bradley, Nolen Scaife, Adam Bates, Patrick Traynor, and Kevin R.B. Butler. 2015. [“Mo\(bile\) Money, Mo\(bile\) Problems: Analysis of Branchless Banking Applications.”](#) University of Florida paper.

Reitzug, Fabian, Richard Chamboko, Xavier Gine, and Bob Cull. 2020. [“Does Agent Gender Matter for Women’s Financial Inclusion?”](#) World Bank blog post.

Reserve Bank of India. 2020. [“Banking Ombudsman Scheme, 2006, Ombudsman Scheme for NBFCs, 2018, and Ombudsman Scheme for Digital Transactions, 2019: Annual Report - July 1, 2020 to March 31, 2021.”](#) Annual Report. Annual Report.

Responsible Finance Forum. 2017. [“Opportunities and Risks in Digital Financial Services: Protecting Consumer Data and Privacy.”](#)

Responsible Finance Forum. 2020. [“Preventing Over-Indebtedness in Digital Credit Markets: Investors’ Checklist.”](#) Discussion Paper Investor Guideline 9: Prevent Over-Indebtedness, Strengthen Digital Literacy and Financial Awareness Prepared by Incofin Investment Management April 2020. Draft Working Paper for Comments.

Responsible Practices Working Group. 2020. [“Responsible Practices to Address Seven Major Risks in COVID-19 Digital Financial Transfers.”](#) COVID-19 Global Situation Room convened by the Bill & Melinda Gates Foundation.

Riley, Emma. 2019. [“Hiding Loans in the Household Using Mobile Money: Experimental Evidence on Microenterprise Investment in Uganda.”](#) Oxford University Economics Department paper.

Risk Based Security. 2020. [“2020 Year End Report.”](#)

Rizzi Alexandra, Isabelle Barrès, and Elisabeth Rhyne. 2017. [“Tiny Loans, Big Questions: Client Protection in Mobile Consumer Credit.”](#) Center for Financial Inclusion.

Rizzi, Alexandra, Alexandra Kessler, and Jacobo Menajovsky. 2021. [“The Stories Algorithms Tell: Bias and Financial Inclusion at the Data Margins.”](#) Center for Financial Inclusion paper.

Robinson, Jonathan, and Pascaline Dupas. [“Knowledge, Use, and Repayment of Digital Credit in Malawi.”](#) Centre for Effective Global Action research.

Rodriguez, Christian, Julia Conrad, Gisela Davico, Susie Lonie, and Lesley Denyes. 2019. [“A New Banking Model for Africa: Lessons on Digitization from Four Years of Operations.”](#) IFC report.

Rowntree Oliver. 2019. [“The Mobile Gender Gap Report 2019.”](#) GSMA.

RSA. 2018. [“RSA Quarterly Fraud Report, Q1 2018.”](#)

RSA. 2020. [“Quarterly Fraud Report, Q3 2020.”](#)

Ryan, Chris. 2021. [“Solving the Fraud Problem: What is Account Takeover Fraud?”](#) Experian blog post.

SABRIC. [“Annual Crime Stats 2018: Contact Crime, Digital Crime, Card Fraud.”](#)

SABRIC. [“Annual Crime Stats 2019: Contact Crime, Digital Crime, Card Fraud.”](#)

REFERENCES

Sahay, Ratna, Ulric Eriksson von Allmen, Amina Lahreche, Purva Khera, Sumiko Ogawa, Majid Bazarbash, and Kimberly Beaton. 2020. ["The Promise of Fintech : Financial Inclusion in the Post COVID-19 Era."](#) IMF Departmental Paper No. 20/09.

Sambasivan, Nithya, Amna Batool, Nova Ahmed, Tara Matthews, Kurt Thomas, Laura Gaytan-Lugo, David Nemer, Elie Bursztein, and Sunny Consolvo. 2019. ["They Don't Leave Us Alone Anywhere We Go': Gender and Digital Abuse in South Asia."](#) Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow.

Sane, Renuka, Srishti Sharma, and Karthik Suresh. 2021. ["Grievance Redress in the Financial Sector in India: Lessons from the Field."](#) The Leap Journal blog post.

Schwartz, Leo, and Lucia Cholakian Herrera. 2020. ["'Feminist' Ponzi Schemes Are Sweeping through Argentina."](#) Rest of World article.

Serianu. 2017. ["Africa Cyber Security Report 2017: Demystifying Africa's Cyber Security Poverty Line."](#)

Serianu. 2018. ["Africa Cyber Security Report, Botswana: Cyber Security Skills Gap."](#)

Serianu. 2018. ["Africa Cyber Security Report, Kenya: Cyber Security Skills Gap."](#)

Serianu. 2018. ["Africa Cyber Security Report, Lesotho: Cyber Security Skills Gap."](#)

Serianu. 2020. ["Africa Cybersecurity Report Kenya, 2019/2020: Local Perspective on Data Protection and Privacy Laws – Insights from African SMEs."](#)

Serianu. 2020. ["Africa Cybersecurity Report Uganda, 2019/2020: Local Perspective on Data Protection and Privacy Laws – Insights from African SMEs."](#)

Sift. 2020. ["Q3 2020 Digital Trust and Safety Index: Account Takeover Fraud and the Growing Burden on Business."](#)

Simmons, Dan. 2017. ["BBC Fools HSBC Voice Recognition Security System."](#) BBC Click investigation.

Singh, Arti. 2021a. ["A New Worry for Fintech Lenders."](#) The Morning Context article.

Singh, Arti. 2021b. ["Inside the Scramble to Cut Off Chinese Loan Apps ."](#) The Morning Context article.

Sivalingam, Isvarya, Olivia, Evelyne Matibe, Rahul Chatterjee, Karthick Morchan, Anup Singh, and Leonard Kambona. 2019. ["Making Digital Credit Truly Responsible: Insights from Analysis of Digital Credit in Kenya."](#) SPTF, MSC, and the Smart Campaign.

Solli, Jami Hubbard. 2019. ["An Intro to UDIS and the MMM Cooperation."](#) Financial Inclusion Global Initiative report.

Spencer, Shelley, Mandana Nakhai, and Jordan Weinstock. 2018. ["The Role of Trust in Increasing Women's Access to Finance through Digital Technologies."](#) USAID.

Statista. 2020. ["Volume of Data/Information Created, Captured, Copied, and Consumed Worldwide from 2010 to 2025."](#)

Statista. 2021. ["Number of Social Network Users Worldwide from 2017 to 2025 \(in Billions\)."](#)

Stolba, Stephan Lembo. 2020. ["How Can Biometrics Protect Your Identity?"](#) Experian blog post.

REFERENCES

Suryono, Ryan, Indra Budi, and Betty Purwandari. 2020. [“Challenges and Trends of Financial Technology \(Fintech\): A Systematic Literature Review.”](#)

Theis, Sophie, Giudy Rusconi, Elwyn Panggabean, and Sonja Kelly. 2020. [“Delivering on the Potential of Digitized G2P: Driving Women’s Financial Inclusion and Empowerment through Indonesia’s Program Keluarga Harapan \(PKH\).”](#) Women’s World Banking research.

Toronto Centre. 2018. [“Advancing Women’s Digital Financial Inclusion.”](#) Practical Leadership and Guidance from Toronto Centre. TC Notes.

Totolo, Edoardo. 2018. [“Kenya’s Digital Credit Revolution Five Years On.”](#) FSD Kenya report.

Traynor, Patrick. 2018. [“Digital Finance and Data Security: How Private and Secure Data Is Used in Digital Finance?”](#) Center for Financial Inclusion.

UK Finance. 2020. [“Fraud – The Facts 2020: The Definitive Overview of Payment Industry Fraud.”](#)

Unnikrishnan, Shalini, Jim Larson, Boriwat Pinradab, and Rachel Brown. 2019. [“How Mobile Money Agents Can Expand Financial Inclusion.”](#) Boston Consulting Group research.

UNSGSA. 2021. [“Financial Service Providers and Financial Health.”](#) UNSGSA Working Group on Financial Health report.

Vidal, Maria Fernandez, and Fernando Barbon. 2018. [“Digital Credit Helping to Put Kids in Classrooms in Cote d’Ivoire.”](#) CGAP blog post.

Waldron, Daniel, and Alexander Sotiriou. 2019. [“Digital Finance for the Real Economy: Introduction.”](#) CGAP slide deck.

Wamalwa, Peter, Ireen Rugiri, and Julienne Lauler. 2019. [“Digital Credit, Financial Literacy, and Household Indebtedness.”](#) KBA Centre for Research on Financial Markets and Policy Working Paper.

Warburton David. 2020. [“Phishing and Fraud Report: Phishing During a Pandemic.”](#) F5 Labs.

Wechsler, Michael, and Samikshya Siwakoti. 2020. [“Gender, Cybersecurity and Fraud in DFS.”](#) Columbia University Digital Financial Services Observatory.

Wein, Tom, Mercy Musya, Rafe Mazer, and Maria Fernandez Vidal. 2017. [“Do Peer-to-Peer Lenders Understand Risk?”](#) CGAP bog post.

White, Zachary. 2020. [“VITALITE Zambia: Learnings from Providing Pay-as-You-Go Smartphones through Pay-as-You-Go Solar.”](#) GSMA Mobile for Development blog post.

World Bank DataBank. [“Mobile Cellular Subscriptions – South Africa.”](#)

World Bank. 2019. [“Complaints Handling within Financial Service Providers Principles, Practices, and Regulatory Approaches.”](#) World Bank Group Technical Note.

World Bank. 2021. [“Consumer Risks in Fintech: New Manifestations of Consumer Risks and Emerging Regulatory Approaches.”](#) Policy Research Paper.

Wright, Graham A.N. 2015. [“A Question of Trust Mitigating Customer Risk in Digital Financial Services.”](#) MicroSave.

REFERENCES

Wright, Graham, and Vera Bersudskaya. 2017. “[More Than Hygiene – Improving Agent Network Performance to Maximise Profitability.](#)” Microsave Consulting ” Helix Institute of Digital Finance. blog post.

Wright, Graham, Nitish Narain, and Manoj Nayak. 2018. “[Consumer Protection in the Digital Age.](#)” MSC blog post.

Zetterli, Peter. 2013. “[Can Phones Drive Insurance Markets? Initial Results from Ghana.](#)” CGAP blog post.

Zhang, Daniel et al. 2021. “[The AI Index 2021 Annual Report.](#)” AI Index Steering Committee, Human-Centered AI Institute, Stanford University.

Zhang, Shu, and Ryan Woo. 2017. “[After Spate of Suicides, China Targets Predatory Student Lending.](#)” Reuters article.

Zimmerman, Jamie, and Silvia Baur-Yazbeck. 2016. “[Understanding Consumer Risks in Digital Social Payments.](#)” CGAP Brief.

