POLICY RESEARCH PAPER

Consumer Risks in Fintech

New Manifestations of Consumer Risks and Emerging Regulatory Approaches

APRIL 2021

WORLD BANK GROUP

Ministry of Foreign Affairs of the Netherlands

FINANCE, COMPETITIVENESS &
INNOVATION GLOBAL PRACTICE

POLICY RESEARCH PAPER

Consumer Risks in Fintech

New Manifestations of Consumer Risks and Emerging Regulatory Approaches

APRIL 2021

WORLD BANK GROUP

Ministry of Foreign Affairs of the Netherlands

1818 H Street NW
Washington DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org

CONTENTS

TABLES

ACKNOWLEDGMENTS

This Policy Research Paper is a product of the Financial Inclusion and Consumer Protection Team within the Financial Inclusion, Infrastructure & Access Unit of the World Bank Group's (WBG) Finance, Competitiveness & Innovation Global Practice.

This paper was prepared by Gian Boeddu, Jennifer Chien, and Ivor Istuk (Senior Financial Sector Specialists, WBG) and Ros Grady (Consultant, WBG), with valuable research and drafting assistance from Arpita Sarkar (Consultant, WBG). Mahesh Uttamchandani (Practice Manager, WBG) provided overall guidance.

The team is grateful for valuable comments received from the following WBG staff members: Sharmista Appaya (Senior Financial Sector Specialist), Patricia Caraballo (Senior Financial Sector Specialist), Ana Fiorella Carvajal (Lead Financial Sector Specialist), Julian Casal (Senior Financial Sector Specialist), Isaku Endo (Senior Financial Sector Specialist), Harish Natarajan (Lead Financial Sector Specialist), and Luz Maria Salamina (Principal Operations Officer); and from the following external reviewers: the Consultative Group to Assist the Poor (CGAP), the International Financial Consumer Protection Organisation (FinCoNet), the G20/OECD Task Force on Financial Consumer Protection (G20 Task Force), Professor Katja Langenbucher, and Alexandra Rizzi (Center for Financial Inclusion).

The team also gratefully acknowledges editorial assistance provided by Charles Hagner and design and layout assistance provided by Debra Naylor of Naylor Design, Inc.

Finally, the team gratefully acknowledges the generous financial support of the Ministry of Foreign Affairs of the Kingdom of the Netherlands and the Bill & Melinda Gates Foundation under the Financial Inclusion Support Framework (FISF) program, without which preparation of this paper would not have been possible.

ACRONYMS AND ABBREVIATIONS

AFPI	Indonesian Joint Funding Fintech Association
AI	artificial intelligence
AML/CFT	anti-money laundering/countering the financing of terrorism
APR	annual percentage rate
ASIC	Australian Securities and Investments Commission
BdP	Banco de Portugal
BIS	Bank for International Settlements
BNM	Bank Negara Malaysia
CAK	Competition Authority of Kenya
CBIRC	China Banking and Insurance Regulatory Commission
CGAP	Consultative Group to Assist the Poor
CONDUSEF	National Commission for the Protection and Defense of Users of Financial Services (Mexico)
DFSA	Dubai Financial Services Authority
EBA	European Banking Authority
FCA	Financial Conduct Authority (UK)
FCP	financial consumer protection
FinCoNet	International Financial Consumer Protection Organisation
FSP	financial service provider
G20 Task Force	G20/OECD Task Force on Financial Consumer Protection
GDPR	Regulation 2016/679—General Data Protection Regulation (EU)
GSMA	GSM Association
ICCR	International Committee on Credit Reporting
IMF	International Monetary Fund

KFS	key facts statement
MiFID	Directive 2014/65/EU—Markets in Financial Instruments Directive (EU)
MNO	mobile network operator
NBFC	non-banking financial company
OJK	Otoritas Jasa Keuangan (Financial Services Authority, Indonesia)
P2P	peer-to-peer
P2PL	peer-to-peer lending
PSD2	Directive 2015/2366 on Payment Services (EU)
RBI	Reserve Bank of India
SEC	Securities and Exchange Commission (USA)
T&C	terms and conditions
TCC	total cost of credit
TILA	Truth In Lending Act (USA)
USSD	Unstructured Supplementary Service Data
WBG	World Bank Group

All dollar amounts are US dollars unless otherwise indicated.

1

EXECUTIVE SUMMARY

Fintech[1] is increasingly recognized as a key enabler for financial sectors worldwide, enabling more efficient and competitive financial markets while expanding access to finance for traditionally underserved consumers. As noted in the Bali Fintech Agenda[2] launched in October 2018 by the WBG and International Monetary Fund (IMF), fintech can support economic growth and poverty reduction by strengthening financial development, inclusion, and efficiency. The critical challenge for policy makers is to harness the benefits and opportunities of fintech while managing its inherent risks.

Along with its benefits, fintech also poses a range of risks to consumers that need to be mitigated in order for fintech to truly benefit consumers. Some of these risks are new, but many represent new manifestations of existing risks resulting not only from the technology supporting and enabling fintech offerings but also from new or changed business models, product features, and provider types, as well as greater accessibility for consumers to sometimes unfamiliar or more complex financial products.[3] For example, a rapid expansion of the peer-to-peer lending (P2PL) market in China in the first half of the 2010s was followed by significant platform collapses and incidents of fraud and platform operator misconduct that caused significant losses to consumers.[4] While digital microcredit has expanded access to credit in some developing countries, countries such as Tanzania and Kenya have seen large numbers of borrowers who are unable to repay their loans due to irresponsible lending practices.[5] Similarly, while there has been significant uptake of electronic money (e-money) in many developing markets, the rise in usage has been accompanied by a rise in a variety of risks for consumers, including potential loss of funds due to fraud and unscrupulous fee-charging practices. Such negative experiences, in addition to causing direct harm to consumers, may also lead to greater mistrust of fintech and the financial sector overall.

The COVID-19 pandemic has further accelerated the widespread transition of consumers to digital financial services and fintech, highlighting their significant benefits while also demonstrating how risks to consumers can increase in times of crisis and economic stress. For example, reports from Indonesia indicate that individual lenders/investors are currently being adversely affected by risky loans made through P2PL platforms, as are borrowers who obtained such loans but are now struggling to have lenders/investors agree to restructure them.[6] Significant numbers of low-income consumers are facing increasing difficulty in repaying existing debts due to the pandemic.[7] Small enterprises have been severely affected by widespread closures and safety measures designed to slow the spread of COVID-19, decreasing the enterprises' profitability and impeding their ability to honor repayment obligations.[8] This in turn exposes their investors to increased risk of loss from their investments. In addition, significant increases in fraudulent app-based digital microcredit lenders have been observed during lockdowns related to COVID-19.[9]

Authorities responsible for financial consumer protection (FCP) are increasingly faced with the challenge of developing or adapting regulation to address risks to consumers generated by fintech. The task of regulators in developing countries is even more difficult if they are attempting to tackle this new challenge while having to implement a baseline FCP regulatory framework[10] at the same time. In a recent survey, regulators identified their limited internal technical expertise as the foremost impediment to regulating and supervising "alternative finance" (such as P2PL and equity crowdfunding) effectively.[11] This paper is intended to contribute to regulators' efforts to bridge the gaps in expertise and knowledge regarding emerging fintech products and their attendant FCP issues.

This paper aims (1) to identify significant new manifestations of consumer risks posed by four key fintech products (digital microcredit, P2PL, investment-based crowdfunding, and e-money)[12] and (2) to provide examples of regulatory approaches emerging internationally that regulators can consider when developing regulatory policy to target such risks. Examples of regulatory approaches are drawn from country examples and international literature.

The primary focus of this paper is informing authorities' development of regulatory policy. It is hoped, however, that the discussion of manifestations of consumer risks in a fintech context can also assist authorities with related key areas, such as market conduct supervision.

Key types of consumer risks and corresponding regulatory approaches discussed in this paper include the following:

- **Factors such as the novelty and opaqueness of fintech business models, fintech entities' responsibilities in the context of those business models, and lack of consumer familiarity with and understanding of new offerings can lead to heightened risks of fraud or misconduct by fintech entities or third parties.** Platform finance (P2PL and investment-based crowdfunding) poses risks to consumers as both lenders/investors and borrowers. Lenders/investors may face loss due to conduct perpetrated by platform operators or related parties, such as fraudulent lending or investment opportunities, misappropriation of funds, or facilitation of imprudent lending or investment to generate fee revenue for the operator to the detriment of consumers who ultimately bear potential losses. Consumers borrowing from such platforms may similarly suffer harm from the resulting imprudent lending. Holders of e-money face risks related to agent misconduct, including charging of unauthorized fees, splitting transactions to earn more commissions and "skimming" into agent accounts. Regulatory approaches to address such risks include vetting of fintech entities during the authorization stage; risk management and governance obligations for platform operators; imposing clear responsibility and liability on providers for the conduct of persons acting on their behalf; placing targeted obligations on platform operators to safeguard consumers' interests regardless of business model (such as requiring P2PL platform operators to undertake creditworthiness assessments even if they are not themselves the lender); warnings and provision of other key disclosures to consumers regarding the risks associated with fintech products; and segregation of client funds.
- **Certain characteristics of fintech business models can lead to conflicts of interests between consumers and fintech entities.** For example, lending models heavily dependent on fees generated by new business can give rise to perverse incentives for fintech entities to act in a manner inconsistent with the interests of their consumers, such as P2PL platforms or digital microcredit providers focusing on loan quantity over quality to maximize fee-related returns. Such risks can be exacerbated in markets where fintech entities are attempting to grow their revenues and size quickly. Potentially harmful conflicts can also arise where fintech entities are empowered to make key decisions affecting the risk of loss, but where that risk is borne by consumers—such as a P2PL or crowdfunding platform operator assisting with loan or investment selection and performing inadequate due diligence on these. Corresponding regulatory approaches include placing positive obligations on fintech entities to manage and mitigate conflicts of interest, to act in accordance with the best interests of their consumers, to undertake adequate assessments regardless of business model, and to prohibit certain business arrangements that encourage conflicted behavior.
- **Consumers may face a heightened risk of adverse impacts due to platform or technology unreliability or vulnerability.** Consumers may be more vulnerable to cyber fraud when acquiring fintech products than when accessing financial products through more traditional channels because interaction with providers is largely or exclusively via digital and remote means. Platform or other technology malfunctions can have adverse impacts on consumers ranging from inconvenience and poor service to monetary loss and loss of data integrity, the risk of which may be increased due to heavier reliance on automated processing of transactions. Regulatory approaches to address such

risks include specific obligations on fintech entities to address technology and systems-related risks and risks associated with outsourcing.

- **Some fintech entities may be at greater risk of business failure or insolvency than established financial service providers (FSPs) due to inexperience, untested businesses, and market factors affecting long-term viability.** This can lead to consumers whose funds are held or administered by a fintech entity facing correspondingly greater risk of loss if the provider becomes insolvent or their business ceases to operate. Consumers may risk losing their committed loan principal or investment funds, or repayments or investment returns owed them, that are being held or administered by a P2PL or crowdfunding platform whose operator becomes insolvent or fails. Insolvency of e-money issuers or banks holding an e-money float similarly puts client funds at risk, especially where there is no deposit insurance. Regulatory approaches to address such risks include requirements for client funds to be segregated from other funds held by a fintech entity and requiring that fintech entities have in place business continuity and resolution arrangements.
- **The digital environment poses inherent challenges to disclosure and transparency, amplified by the novelty of fintech product offerings and consumers' lack of experience with such products.** Information provided via digital channels may not be appropriately formatted to assist in understanding or retention by consumers. Poor design of user interfaces may hamper consumer comprehension or exploit behavioral biases by concealing or underplaying "negative" aspects such as risks and costs. Fintech can also give consumers access to products, such as P2PL or crowdfunding investment opportunities, to which they may previously have had limited or no exposure, making clear, understandable information even more essential for good decision-making. Approaches to address such issues include requirements to disclose key information in a consistent and clear format, on a timely basis, and in a manner that can be retained by consumers. Behavioral insights can also be utilized to disclose information via digital channels in a manner that aims to increase the likelihood of consumer comprehension.
- **Consumers face potentially heightened risks when acquiring fintech products due to their lack of sophistication or inexperience.** Due to the development of fintech, consumers increasingly have access to novel and complex financial products, but they may lack the knowledge or experience to assess or use these products properly. For example, platform finance enables more individuals to act as investors and lenders; this has positive implications for financial inclusion but can present enhanced risks for ordinary consumers new to assessing more complex opportunities. Potential regulatory approaches include setting limits on individual investments, such as overall caps on how much an individual may borrow through a P2PL platform or how much money a company can raise on a crowdfunding platform, or limitations on specific types of investors or exposures; targeted warnings to potential investors; requiring consumers to confirm that they understand the risks they are undertaking; and cooling-off periods. Risks may also arise with respect to digital microcredit products being offered to consumers that are unsuitable and unaffordable for such consumers. Regulatory approaches include requiring effective creditworthiness assessments and applying product design and governance principles, particularly where automated credit scoring is utilized.
- **Use of algorithms for consumer-related decisions is becoming particularly prevalent in highly automated fintech business models.** Consumers may face a range of risks as a result, such as discriminatory or biased outcomes. Emerging approaches in this context include applying fair treatment and anti-discrimination obligations to algorithmic processes; putting in place governance frameworks that require procedures, controls, and safeguards on the development, testing, and deployment of algorithms to ensure fairness; auditing requirements; and providing consumers with rights regarding how they or their information may be subjected to algorithmic decision-making.

Table 1 summarizes new manifestations of consumer risks and corresponding regulatory approaches for each fintech product discussed in this paper. While many of these risks cut across the fintech landscape, they may manifest differently in the context of different fintech products.

In terms of implementation, it is not the intent of this paper to suggest that all risk mitigants discussed herein be implemented. For any regulator contemplating implementing the kinds of regulatory measures discussed in this paper, it will be important to prioritize and take a risk-based approach, to tailor regulatory approaches to country context, and to balance the need for consumer protection with the resulting impact on industry and market development and innovation. It would not necessarily be advisable for a country to implement all of the regulatory measures discussed in this paper immediately or to transplant approaches from other jurisdictions without adjustment. This paper also summarizes a range of key implementation matters for regulators to consider.

TABLE 1: Consumer Risks and Regulatory Approaches by Fintech Product

RISKS TO CONSUMERS	REGULATORY APPROACHES	SEE PAGE
Digital Microcredit (Chapter 4)		
Disclosure and transparency **Content of disclosure** • Information about pricing is incomplete and not transparent (for example, range of different methods used to convey pricing, finance charges not disclosed separately from principal and fees for third-party charges not disclosed) • Inadequate access to complete information about terms and conditions (T&C)—for example, links to full T&C provided at separate location	• Require prominent disclosure of both total cost metrics and clear breakdown of costs • Require disclosure of key T&C in channel being used for transaction • Indicate specific T&C that must be disclosed in transaction channel • Require access to full T&C, including after transaction completed	54
Format of disclosure • Lack of standardized format for costs • Information conveyed via mobile phones in a format or manner that does not facilitate comprehension • Consumers may not be able to retain information	• Encourage greater standardization in presentation of fees/pricing • Require plain language without technical jargon or graphical elements affecting readability • Require standardized presentation of information adapted for digital channels (for example, bite-sized chunks of info provided in consistent manner) • Provide secondary layers of information for further details • Provide offline channels to obtain further info and assistance as well as the ability to access info for future reference	55
Timing and flow of information • Key information such as pricing provided after completion of a transaction • Less appealing information may be de-emphasized	• Require order and flow of info to enhance transparency and comprehension, providing an intuitive "digital journey" through a transaction process • Require disclosure of pricing and key T&C earlier in transaction process • Leverage behavioral insights to encourage consumers to engage with info (for example, require confirmation to move to next stage of transaction)	57
User interfaces • User interface may not be user-friendly, with complex menus that are difficult to navigate	• Require user interface be user-friendly and easy to navigate, including on low-end mobile devices • Encourage consumer testing of user interfaces • Require providers to provide guidance to consumers on user interfaces	58
Marketing practices via remote channels • Push marketing and unsolicited offers encourage impulse borrowing • Exploitation of behavioral biases (for example, encouraging borrowing of maximum amount possible, trivializing loans) • Misleading ads targeting vulnerable consumers (for example, emphasizing benefits, hiding risks, unrealistic offers with hidden conditions, marketing on weekend evenings) • Remote nature of digital channels and rapid speed of transactions increase consumer vulnerability	• Require explicit warnings on risks of short-term, high-cost credit, and information on alternatives to such loans and helpful resources • Ban sales practices that focus on ease of obtaining credit, trivialize credit, or target vulnerable consumers • Slow down process of transacting digitally to allow consumers more time for reflection and deliberation (for example, intermediate steps/screens, adding a review screen) or appropriate cooling-off period • Require loan options be presented in manner that is beneficial (or at least neutral) to consumers and not exploitative (for example, banning default selection of maximum loan size, pre-ticked boxes which lead customers to sub-optimal options)	59

TABLE 1, *continued*

RISKS TO CONSUMERS	REGULATORY APPROACHES	SEE PAGE
Unfair lending • High prices for digital microcredit • Mass marketing to consumers with little assessment of individual consumer circumstances or ability to repay ("lend-to-learn" model) • Certain business models based on high loss rates (for example, large late fees relative to size of loan) • Poor practices such as rolling over loans or encouraging multiple borrowing • Abusive debt collection practices utilizing mobile phone and social media data to contact relatives, friends, and colleagues	• Require providers to assess the ability of prospective customers to repay loans and grant loans only where they are affordable to potential borrowers • Impose requirements that limit rollovers and multiple borrowing to decrease risk of over-indebtedness • Require enhanced monitoring of loan portfolios, particularly where automated credit scoring is utilized • Apply product design and governance rules to digital microcredit, including designing processes and customer acquisition plans to ensure that potential harms and risks to consumers are considered and mitigated • Adapt debt collection rules to prevent abusive debt collection practices utilized by digital lenders	61
Algorithmic scoring • Biased outcomes due to poor algorithm design, incomplete or unrepresentative input data, biased input data • Discrimination based on proxies reflecting sensitive attributes • Consumers unaware or powerless regarding use of algorithm • Regulators lack technical expertise to evaluate algorithmic systems; proprietary nature of algorithms	• Apply fair treatment and anti-discrimination rules to algorithms • Require appropriate procedures, controls, and safeguards during development, testing, and deployment of algorithms to assess and manage risks related to bias and discrimination • Require regular auditing of algorithmic systems by external experts • Ensure transparency to consumers regarding use of algorithms • Provide consumers with right not to be subject solely to automatic processing and the right to request human intervention	64
Regulatory perimeter • Unlevel playing field for different types of providers, with often weaker rules for non-bank lenders • Regulatory gaps for app-based lenders, who may not be covered by any regulatory authority and/or may be based in another country	• Ideally, establish activity-based framework covering all providers of digital microcredit (banks, mobile network operators, non-bank lenders) • Where activity-based approach is not feasible, be opportunistic and build off of existing rules and power to cover non-bank microcredit providers • Coordinate with domestic and international regulatory authorities • Consider regulating domestic agents and intermediaries of foreign fintech companies • Pursue complementary, non-regulatory measures, including industry codes of conduct and working with mobile platforms to establish and enforce rules in key areas for app-based lenders • To address gaps in the coverage of cross-border fintech activities, consider range of measures—including applying a country's FCP requirements (and regulators' mandates) to fintech providers dealing with consumers in that country, regardless of where the providers are based. Also consider supporting coordination and cooperation between authorities to assist with enforcement of relevant requirements	67
Peer-to-Peer Lending (Chapter 5)		
Risks for both lenders/investors and borrowers		
Gaps in regulatory perimeter: P2PL is not adequately covered by a country's FCP regime, and borrowers and lenders/investors receive even less protection than applies to traditional lending	• Apply FCP requirements on an activities basis (lending and investment-related services), rather than by institution type • Extend existing FCP requirements to P2PL and, where necessary, introduce additional FCP rules for P2PL • Issue regulatory guidance to address uncertainty regarding the application of existing FCP requirements to P2PL *(Also, see approaches for addressing cross-border risks summarized above in the context of digital microcredit)*	78

TABLE 1, *continued*

RISKS TO CONSUMERS	REGULATORY APPROACHES	SEE PAGE
Fraud or other misconduct: Fraud or other misconduct by P2PL platform operators, related parties, or third parties	• Impose licensing/registration and vetting and competence requirements on operators and related parties • Require operators to have in place adequate risk management and governance arrangements • Require operators to segregate consumers' funds and deal with them only in prescribed ways • Consider compensation funds *(Also, see below for approaches to address platform/technology vulnerability risks that may facilitate fraud)*	81
Platform/technology unreliability or vulnerability: Platform/technology unreliability or vulnerability that causes or facilitates loss, inconvenience, or other harms	• Require operators to have in place adequate risk management and governance arrangements • Require operators to comply with targeted risk management and operational reliability requirements, including for technology-related risks and outsourcing • Impose specific competence requirements on operators in relation to matters such as information technology–related risk	82
Business failure or insolvency: Business failure or insolvency of operator, causing loss, such as of lenders'/investors' capital or future income on loans or borrowers' committed loan funds or repayments	• Require operators to segregate consumers' funds, hold them with an appropriately regulated entity, and deal with them only in prescribed ways • Require operators to have in place business continuity and hand-over/resolution arrangements • Require operators to comply with record-keeping requirements to support business continuity arrangements • Impose vetting and competence requirements on operators and related parties	83
Inadequate credit assessments: Inadequate credit assessments, increasing the risk of losses from borrower defaults for lenders/investors and over-indebtedness for borrowers	• Impose creditworthiness assessment requirements on operators regardless of whether they are the lender of record	85
Conflicts of interest: Conflicts of interest between platform operators (or their related parties) and lenders/investors or borrowers, leading to operators and related parties to engage in conduct not in the interests of their consumers: • Conflicts of interest leading to imprudent lending assessments by operators • Conflicts of interest leading to unfair or inappropriate loan pricing • Conflicts of interest from intra-platform arrangements causing operators to engage in conduct favoring related parties over consumers	• Impose general conflict mitigation obligations on operators • Require operators to comply with duties to act in consumers' best interests • Require operators to meet obligations regarding fair loan pricing and fees and charges-setting policies consistent with consumers' interests • Place restrictions or prohibitions on operators or their associates investing in loans facilitated by their platforms • Impose creditworthiness assessment requirements on operators regardless of whether they are the lender of record	86

TABLE 1, *continued*

RISKS TO CONSUMERS	REGULATORY APPROACHES	SEE PAGE
Additional risks for lenders/investors		
Inadequate investment-related information: Lenders/Investors are not provided with adequate investment-related information, including:		88
• Inadequate up-front information when considering or making investments/loans	• Require platform operators to provide/make available to consumers ahead of any transaction information highlighting key matters relating to P2PL, such as expected risks, factors affecting returns, and restrictions on early exit • Require platform operators to provide key precontractual information about individual loans to prospective lenders/investors in business models allowing individual loan selection • Mandate warnings or disclaimers in key contexts to highlight risks for consumers and assist in balancing out inappropriately optimistic perceptions	
• Information being provided in an inadequate format	• Require platform operators to give key information appropriate prominence on electronic channels • Require key information to be provided in a standardized format to assist clarity and comparability *(Also, see approaches for risks from digital disclosure summarized above in the context of digital microcredit)*	
• Unbalanced or misleading marketing regarding P2PL investment/lending opportunities	• Require platform operators to comply with general prohibitions against providing misleading information (and, when necessary, clarify via more specific regulatory guidance the application of such prohibitions to marketing of P2PL opportunities) • Impose targeted restrictions on specific P2PL circumstances presenting higher risk of misleading investors	
• Inadequate ongoing information about the performance and status of their investments/loans	• Require platform operators to provide ongoing information to lenders/investors at prescribed times or frequencies regarding matters affecting their investments/loans specifically, such as defaults and changes to borrowers' circumstances, or more generally, such as performance of the operator and adverse events	
Harm due to lenders'/investors' lack of sophistication or inexperience: Such as taking on risk of loss they cannot afford or do not understand	• Impose lending/investment caps on less sophisticated or more vulnerable lenders/investors (jurisdictions have done so on a variety of bases) • Impose caps on the amount that individual borrowers may borrow through P2PL platforms as another way to reduce risk of loss to lenders/investors • Consider compensation funds	94
Borrower fraud: Loss for lenders/investors due to borrower fraud	• Require platform operators to comply with risk management requirements referred to above, as well as targeted requirements such as to obtain appropriate identification information and implement measures against fraudulent access to their platform (know your customer requirements under anti-money laundering and countering the financing of terrorism laws would also be relevant) • Impose creditworthiness assessment requirements on platform operators regardless of whether they are the lender of record	97
Additional risks for borrowers		
Inadequate loan-related information	• Extend application of existing traditional credit disclosure requirements to platform operators even when they are not the lender of record • Address gaps in existing borrower disclosure regimes by developing requirements specific to P2PL *(Also, see approaches for risks relating to credit disclosure summarized above in the context of digital microcredit)*	97

TABLE 1, *continued*

RISKS TO CONSUMERS	REGULATORY APPROACHES	SEE PAGE
Risks from digital distribution of P2PL credit: Risks arising from digital distribution of credit summarized above in the context of digital microcredit can also affect digital distribution of P2P loans to borrowers	*See approaches summarized above in the context of digital microcredit*	98
Investment-Based Crowdfunding (Chapter 6)		
Investor inexperience and higher-risk nature of investee companies • Small business and start-up investee companies may constitute a riskier investment for retail investors • Investors are often unlikely to possess sufficient knowledge or experience, or have access to financial advice, to assess offers • Investees may have majority shareholder and management arrangements that present risks for minority shareholders such as external crowdfunding investors	• Require risk warnings and disclosures about key aspects of crowdfunding • Impose issuer caps—limitations on the size of an issue • Impose investor caps—limitations on individual investments/exposures • Require investor-suitability assessments to be undertaken by platform operators • Establish cooling-off periods for investors	108
Risks related to the nature of securities offered on crowdfunding platforms • Securities rarely traded on any kind of organized market and may have limitations on transferability—investors may not understand or be able to deal with risk of being unable to exit their investment • Creation of complex hybrid securities by incorporating rights and restrictions for security holders to match issuer's needs	• Prescribe disclosure requirements focused on emphasizing the illiquid nature of issued securities • Restrict the types of securities that can be issued • Impose targeted product intervention • Require targeted warnings • Introduce rules facilitating information exchanges and secondary trading	112
Consumers are not provided with adequate information • Crowdfunding issuers often tend to be small businesses or in their start-up phase with a limited track record, limiting the availability of information • High separation between ownership by crowdfunding investors and parties that control issuers—potential lack of information provided to crowdfunding investors • Retail investors in crowdfunding securities are also at risk of misleading marketing practices, potentially exacerbated as a result of issuers being new to making public offers	• Introduce investment-related disclosure requirements • Introduce regulation of bulletin boards and crowdfunding trading facilities (including secondary market) to assist information accuracy • Apply fair marketing rules to investment-based crowdfunding activities	115
Platform operator misconduct or failure • Platform operators and related parties may engage in misconduct under a range of circumstances that affect investors, from outright fraud to incompetent administration to undertaking unfair conflicted behavior • Failure of a platform can leave investors without services essential to the continued integrity of their investment	• Introduce authorization and vetting requirements • Require business-/service-continuity arrangements • Require segregation of client funds • Impose rules and require policies for mitigating conflicts of interest • Apply risk management requirements of the kinds summarized above in the context of P2PL	119
Issuer fraud: Consumers investing on crowdfunding platforms may suffer losses due to issuer fraud, such as sham offers or concealing or providing misleading information	• Require platform operators to undertake due diligence	122

TABLE 1, *continued*

RISKS TO CONSUMERS	REGULATORY APPROACHES	SEE PAGE
E-Money (Chapter 7)		
Gaps in regulatory perimeter: Current requirements may not apply to all entities offering e-money products, and even if the licensing rules are activities based, consumer protection rules may not apply to e-money as a product given innovative differences.	• Allow e-money activities to be undertaken only by licensed entities (that may include non-banks) • Ensure consumer protection rules also apply on an activities basis to providers of e-money • Ensure that e-money is covered by any relevant definition of financial product or service	131
Fraud or other misconduct resulting in consumer loss • Fraud or misconduct by issuers or related parties, including agents • Fraud by third parties	• Impose licensing/registration and vetting and competence requirements on providers and related parties • Impose rules specifically for agents, including requirements for agent due diligence, requirements for agency agreements, requirements for agents to be trained and monitored, and clear provider responsibility and liability for agent conduct • Require operators to have in place adequate risk management and governance arrangements • Mandate transaction-authentication standards and require transaction-specific fraud-prevention methods to be applied—for example, limits on transaction attempts • Limit consumers' liability for an unauthorized transaction, except, for example, in case of fraud or gross negligence by the consumer • Require warnings and information about security risks to be provided to consumers • Require consumers to advise providers of matters relevant to potential fraud, such as lost or stolen devices or security credentials • Place the burden of proof on providers to show transactions were unauthorized • Require reporting of large-scale fraud/security breaches • Prohibit agents from charging unauthorized fees *(Also, see below for approaches to deal with platform/technology vulnerability risks that may facilitate fraud)*	132
• Conflicts between interests of providers or agents and consumers (such as perverse incentive arrangements for agents), leading to consumer harms	• Impose conflict mitigation obligations on providers to avoid conduct to their advantage inconsistent with consumers' interests, or equivalent conduct engaged in by agents	
E-money platform/technology vulnerability or unreliability: Platform/technology unreliability or vulnerability that causes or facilitates loss, inconvenience, or other harms	• Mandate technology risk and cybersecurity-management requirements • Place obligations on operators to ensure appropriate/minimum levels of operational reliability • Require notice to users of anticipated/actual service interruptions • Make a payer institution liable for transactions not being completed as instructed	136
Mistaken transactions: A consumer's funds are misdirected to an incorrect account/recipient as a result of error, rather than fraud	• Require a mechanism that enables the consumer to view transaction details before transaction completion • Require providers to explain how to stop transfers • Require FSPs involved in a transaction to assist in resolving mistakes • Place the burden of proof on providers to show a transaction was authenticated and recorded accurately	137
Provider insolvency or liquidity risks • A provider may become insolvent with insufficient funds to meet the demands of e-money holders • E-money may also not be covered by deposit insurance schemes • A provider or their agents may not have enough liquid funds to meet consumer demand, such as for cash-out transactions	• Require an e-money issuer to isolate and ring-fence funds equal to e-money balances outstanding • Limit activities e-money issuers can carry out to minimize insolvency risk • Mandate initial and ongoing capital requirements • Require issuers to maintain sufficient liquidity and to ensure agents have sufficient liquidity to honor cash-out obligations	138

TABLE 1, *continued*

RISKS TO CONSUMERS	REGULATORY APPROACHES	SEE PAGE
E-money not covered by deposit insurance schemes: E-money balances may not have the benefit of deposit insurance that applies to traditional accounts, in the event of insolvency of either the e-money issuer or a custodial institution holding an e-money float (such as a bank holding a trust account)	• Deposit insurance may be extended to e-money balances or to custodial accounts holding the e-money float depending on availability of scheme in the country. An alternative policy approach is to exclude e-money balances from deposit insurance schemes. (The arguments for and against each of these options are beyond the scope of this paper but are covered in other publications referenced later in the paper)	139
E-money not permitted to be redeemed for face value: Providers may seek to apply a discount beyond transaction-processing fees	• Require funds to be redeemed at face/par/equivalent value	140
Consumers are not provided with adequate Information		140
• Key product information is not disclosed/available up front to consumers	• Require compliance with general transparency and/or disclosure • Require public up-front disclosure of T&C and fees and charges through all applicable channels, as well as provision of written agreements at contracting stage • Require consumers to be given notice of changes • Require standard form agreement to be lodged with regulator	
• Inadequate ongoing information, such as about ongoing transactions, changes to the product, or product suspension or withdrawal	• Require written notice of changes to be provided to consumers • Require transaction receipts to be issued • Require periodic statements to be issued and/or that consumers be able to access details of previous transactions	
• Disclosed information cannot be easily retained by a consumer	• Require information to be in a form the customer can access and keep for future reference	
• Disclosure format risks in a digital context	• See approaches for equivalent risks summarized above in the context of digital disclosure for digital microcredit	
• Misleading marketing	• Prohibit misleading marketing in relation to e-money account • Require disclosure of provider's details in marketing materials to assist with recourse • Impose specific rules—for example, making risk statements prominent	
Unsuitable e-money products: E-money products may not be designed to be suitable for the consumer segments they are marketed to, particularly some previously unserved or underserved consumers	• Require providers to design and distribute e-money products to meet the needs and capabilities of users in their target market • Impose individual suitability assessment requirements	144

NOTES

1 For the purposes of this paper, *fintech* refers to advances in technology that have the potential to transform the provision of financial services spurring the development of new business models, applications, processes, and products. See World Bank Group and International Monetary Fund, *Bali Fintech Agenda,* 12.

2 World Bank Group and International Monetary Fund, *Bali Fintech Agenda.*

3 For an overview of risks and benefits in a digital financial services context, see G20/OECD Task Force on Financial Consumer Protection, *Financial Consumer Protection Policy Approaches,* 12–14.

4 See, for example, Duoguang, "Growing with Pain," 42; Owens, "Responsible Digital Credit," 8–9; Huang, "Online P2P Lending," 77; Hornby and Zhang, "China's Middle Class."

5 For example, a 2017 MicroSave study found that 2.7 million Kenyans were blacklisted in credit reference bureaus in the past three years, 400,000 of these for amounts of less than $2. See MicroSave, "Where Credit Is Due."

6 See, for example, Faridi, "P2P Fintech Lending Sector in Indonesia."

7 For example, 76 percent, 80 percent, and 89 percent of low-income survey respondents in Ghana, India, and Kenya, respectively, indicated they were late in making loan repayments since the pandemic began. See BFA Global, "Dipstick Surveys."

8 See, for example, Gibbens, "Helping Small Businesses."

9 https://www.centerforfinancialinclusion.org/combating-the-rise-in-fraudulent-fintech-apps

10 For an overview of key elements of a FCP regulatory framework (as an element of a broader legal and supervisory framework for FCP), see, for example, World Bank Group, *Good Practices*, 14, 68, 102, and 140.

11 World Bank Group and CCAF, *Regulating Alternative Finance*, 63.

12 Selected as examples of fintech offerings that may address some of the most basic needs of first-time, and thus inexperienced, financial consumers—namely, making payments, borrowing, or saving or investing money—as well as representing different stages in the development of fintech product offerings and corresponding regulatory and policy frameworks that surround them. See section 2.2 below for definitions of these terms as used in the paper.

INTRODUCTION

2

INTRODUCTION

2.1 THE AIMS OF THIS PAPER

Within the broader digital financial services space, the umbrella term *fintech* (financial technology) represents particularly novel product or service offerings leveraging technology. While there is no universally accepted definition of *fintech*, a broad interpretation recently posited by the WBG and IMF describes fintech as advances in technology that have the potential to transform the provision of financial services, spurring the development of new business models, applications, processes, and products.[13]

Fintech is increasingly recognized as a key enabler for financial sectors worldwide, enabling more efficient and competitive financial markets while expanding access to finance for traditionally underserved consumers. In October 2018, the WBG and IMF launched the Bali Fintech Agenda, a set of 12 policy elements aimed at helping countries harness the benefits and opportunities of fintech while managing its inherent risks.[14] As noted in the Bali Fintech Agenda, fintech can support potential growth and poverty reduction by strengthening financial development, inclusion, and efficiency. Recent analysis by the IMF also points to the potential for digital finance to assist in mitigating economic impacts of the COVID-19 pandemic.[15]

Along with its benefits, fintech also poses a range of risks to consumers that need to be mitigated in order for fintech to truly benefit consumers. Some of these risks are new, but many represent new manifestations of existing risks resulting not only from the technology supporting and enabling fintech offerings but also from new or changed business models, product features, and provider types, as well as greater accessibility for consumers to sometimes unfamiliar or more complex financial products.[16] For example, a rapid expansion of the P2PL market in China in the first half of the 2010s was followed by significant platform collapses and incidents of fraud and platform operator misconduct that caused significant losses to consumers.[17] While digital microcredit has expanded access to credit in some developing countries, countries such as Tanzania and Kenya have seen large numbers of borrowers who are unable to repay their loans.[18] Similarly, while there has been significant uptake of electronic money (e-money) in many developing markets, the rise in usage has been accompanied by a rise in a variety of risks for consumers, including potential loss of funds due to fraud and unscrupulous fee-charging practices.

The COVID-19 pandemic has further accelerated the widespread transition of consumers to digital financial services and fintech, highlighting their significant benefits while also demonstrating how risks to consumers can increase in times of crisis and economic stress. For example, reports from Indonesia indicate that individual lenders/investors are currently being adversely affected by risky loans made through P2PL platforms, as are borrowers who obtained such loans but are now struggling to have lenders/investors agree to restructure them.[19] Significant numbers of low-income consumers are facing increasing difficulty in repaying existing debts due to the pandemic.[20] Small enterprises have been severely affected by widespread closures and safety measures designed to slow the spread of COVID-19, decreasing their businesses' profitability and impeding their ability to honor

repayment obligations.[21] This in turn exposes their investors to increased risk of loss from their investments. The COVID-19 pandemic has also increased the demand for digital payment services such as e-money in preference to using cash. Reasons for this include the impact of lockdowns on both consumers and merchants; the dissemination of emergency relief, welfare payments, and other forms of welfare support via digital platforms; reductions in fees for payment services; a disinclination to use cash because of the perceived risk of virus transmission via paper money; and central banks' encouragement of consumers to use digital payment services, and merchants to accept them.[22] With the increased momentum for digital financial services generated by the crisis, it is important that regulatory measures also address potential increases in risk. For example, prior to new P2PL rules coming into effect, Korean authorities announced a lowering of the limits they would place on how much individual lenders/investors could invest, taking into account increased levels of credit risk amid the COVID-19 crisis.[23] Recognizing the increased need for accessible funding, some regulators have introduced temporary adjustments to existing crowdfunding regulations to facilitate and speed up the process of raising funds.[24]

Authorities responsible for FCP are increasingly faced with the challenge of developing or adapting FCP regulation as may be necessary to address risks to consumers generated by fintech. Regulators are having to consider whether and what adjustments they may need to make to established FCP approaches, or whether new innovative approaches are required, to mitigate manifestations of consumer risks resulting from fintech. The task of regulators in developing countries is even more difficult if they are attempting to tackle this new challenge while having to implement baseline FCP regulatory frameworks at the same time.

In a recent survey on alternative finance such as P2PL and investment-based crowdfunding, regulators identified their limited internal technical expertise as the foremost impediment to regulating such activities effectively.[25] This paper is intended to contribute to regulators' efforts to bridge gaps in expertise and knowledge about the interaction of FCP issues and fintech.

This paper aims (1) to identify significant new manifestations of consumer risks posed by four key fintech products (digital microcredit, P2PL, investment-based crowdfunding, and e-money) and (2) to provide examples of regulatory approaches emerging internationally that are intended to address such risks. Examples of regulatory approaches are drawn from country examples and international literature. The primary focus of this paper is on informing authorities' development of regulatory policy—that is, FCP rules. It is hoped, however, that the discussion on manifestations of consumer risks in a fintech context that need to be understood for the purposes of formulating regulatory policy can also assist authorities with key related areas, such as market conduct supervision.

This paper is not intended to cover all consumer risks and corresponding regulatory approaches common to traditional and fintech products. In 2017, the WBG published the latest edition of its *Good Practices for Financial Consumer Protection* (WBG FCP Good Practices 2017),[26] which addresses this broader range of baseline, and equally important, risks and mitigants applying across financial product categories in both a traditional and fintech context.[27] This paper is intended to be a complementary publication to the WBG FCP Good Practices 2017 by assisting policy makers in developing and implementing FCP regulation that addresses new manifestations of risks affecting consumers in this context.

This paper considers fintech-related risks from a retail consumer perspective. In particular, it identifies and discusses risks that have potential adverse impacts for retail consumers (typically individuals or micro, small, or medium enterprises) when acquiring and using fintech offerings, especially the kinds of risks that authorities increasingly consider warrant regulatory intervention. Some risks, such as in relation to gaps in the coverage of FCP regulation or impacts from the use of algorithms, are discussed separately in the context of their root causes to help readers understand them, but with the ultimate aim of addressing the potential consumer harm that can result.

International practice is converging on FCP regulatory approaches to address some risks, but for other risks, measures can differ significantly or are still in the developmental stage. The recent regulator survey on alternative finance noted above indicated that wide variance remains in international adoption of various regulatory requirements, in part perhaps reflecting the limited development of relevant markets, as well as regulatory responses.[28] This paper highlights where convergence is occurring. To avoid giving an overly narrow view, however, and to assist regulators in developing their own approaches in a rapidly developing field, the paper also covers approaches that as yet may be disparate in addressing the same risks, or are still in preliminary stages of development.

This paper draws from a cross section of jurisdictions, both geographically and in terms of level of development. To identify risks and corresponding approaches, the paper draws to a large extent on findings made and initiatives implemented, or being implemented, by national and international authorities. While not all regulatory approaches or frameworks identified internationally are necessarily equally effective, and it will be some time before effectiveness of different approaches becomes clear, this is intended to assist policy makers in developing countries to draw from practical experiences. Where useful, particularly where there is still a lack of emerging approaches from authorities, the paper also draws from other international guidance and research, such as from international organizations and commentators.

2.2 KEY FINTECH PRODUCTS COVERED IN THIS PAPER

This paper covers four key fintech products: digital microcredit, P2PL, investment-based crowdfunding and e-money (as defined in Table 2 below). These fintech products were selected primarily for two reasons. First, they are examples of fintech offerings that can address some of the most basic needs of first-time, and thus inexperienced, financial consumers (of particular relevance in developing countries)—namely, making payments, borrowing, or saving or investing money. Second, they represent different stages in the development of fintech product offerings and corresponding regulatory and policy frameworks that surround them, ranging from more established examples such as e-money offerings to more recent developments such as P2PL and crowdfunding.

There are obviously many other emerging products and service offerings for which further research insights would be beneficial, such as robo-advice, 'insurtech' and 'banking as a service' offerings.

2.3 HOW THE PAPER IS STRUCTURED

This paper focuses on consumer risks arising in the context of the four selected fintech products—digital microcredit, P2PL, investment-based crowdfunding, and e-money. Chapters 4 to 7 set out a discussion of new manifestations of consumer risks and corresponding regulatory approaches in relation to each of these products. Readers interested in focusing on only some of these products may consult the relevant product chapter for a stand-alone discussion.

Chapter 3 (section 3.1) provides an overview of consumer risks identified in the product-specific chapters that are relevant to most of or all four fintech products discussed in the paper. The chapter provides examples, based on the product-specific chapters, of how relevant risks arise in connection with the various products. The section also briefly touches on some key issues related to data privacy.

Chapter 3 (section 3.2) also discusses key considerations for regulators contemplating implementation of regulatory measures to address relevant consumer

TABLE 2: Fintech Products Discussed in This Paper

FINTECH PRODUCT	DEFINITION FOR PURPOSES OF THIS PAPER
Digital microcredit	Credit products that are short term, low value, accessed via mobile devices, and typically involve automated credit scoring and fast approval.
Peer-to-peer lending (P2PL)	The provision of credit facilitated by online platforms that match borrowers with lenders, encompassing a spectrum ranging from • Platforms that facilitate consumers acting as direct lenders for individual loans; to • Platforms that allow consumers to invest in individual loans, or in pools or portfolios of loans indirectly, being exposed to the credit risk of those loans without being the lender of record.
Investment-based crowdfunding	The connecting and matching of primarily small enterprises seeking to raise investment finance by issuing securities (debt or equity) to prospective, primarily retail, investors (the crowd) through online platforms.
Electronic money (e-money)	A store-of-value product with the following characteristics: • It is a digital representation of a fiat currency (legal tender); • It is a claim against the provider; • It can be redeemed at face value on demand; and • It is accepted as a means of payment by persons other than the provider.

risks in their jurisdiction. Although the paper's focus is on regulation, not supervision, the section highlights the very important complementarity of supervision.

2.4 AREAS OUTSIDE THE SCOPE OF THIS PAPER

This paper is intended to assist authorities in considering risks that are more appropriately addressed through FCP regulation and dealt with by market conduct regulators. There are a range of other areas of risk not covered in this paper that may affect the public, and thus consumers, more broadly and can overlap with FCP—all of which governments should consider as part of a comprehensive strategic approach to fintech in their jurisdictions. These include money laundering and the financing of terrorism, prudential concerns and requirements (including capital and liquidity requirements intended to address risks that can affect consumers), gender-based and other discrimination, areas of structural disadvantage affecting consumers, and competition and monetary policy.

The paper briefly touches on credit scoring to discuss key consumer risks in connection with unfair lending in a digital microcredit and P2PL context. However, it does not set out an analysis of such issues and regimes, which warrant their own separate detailed consideration.[29]

The paper also includes a short, high-level section touching on issues related to data privacy but is not intended to be an exhaustive canvassing of privacy risks. While critical for financial consumers, data privacy risks typically involve considerations going beyond a financial consumer lens and are ideally addressed through regulatory approaches that go beyond sector-specific regulation.

NOTES

13 See World Bank Group and International Monetary Fund, *Bali Fintech Agenda,* 12.
14 World Bank Group and International Monetary Fund, *Bali Fintech Agenda*.
15 IMF, *Promise of Fintech*.
16 For an overview of risks and benefits in a digital financial services context, see G20/OECD Task Force on Financial Consumer Protection, *Financial Consumer Protection Policy Approaches,* 12–14.
17 See, for example, Duoguang, "Growing with Pain," 42; Owens, "Responsible Digital Credit," 8–9; Huang, "Online P2P Lending," 77; Hornby and Zhang, "China's Middle Class."
18 For example, a 2017 MicroSave study found that 2.7 million Kenyans were blacklisted in credit reference bureaus in the past three years, 400,000 of these for amounts of less than $2. See MicroSave, "Where Credit Is Due."
19 See, for example, Faridi, "P2P Fintech Lending Sector in Indonesia."
20 For example, 76 percent, 80 percent, and 89 percent of low-income survey respondents in Ghana, India, and Kenya, respectively, indicated they were late in making loan repayments since the pandemic began. See BFA Global, "Dipstick Surveys."
21 See, for example, Gibbens, "Helping Small Businesses."
22 See, for example, IMF, "Digital Financial Services and the Pandemic." See also Jurd De Girancourt, "How the COVID-19 Crisis May Affect Electronic Payments."
23 Bae, "S. Korea to Place Investment Cap."
24 See, for example, SEC, "Facilitating Capital Formation and Expanding Investment Opportunities."
25 World Bank Group and CCAF, *Regulating Alternative Finance*, 63.
26 World Bank Group, *Good Practices*.
27 See also OECD, *G20 High-Level Principles on Financial Consumer Protection,* and the various published *Effective Approaches to Support*.
28 World Bank Group and CCAF, *Regulating Alternative Finance*, 47.
29 For a discussion of relevant issues, including implementation and operation of credit reporting and scoring arrangements in developing countries lacking formal data sources, see, for example, World Bank Group and International Committee on Credit Reporting, *Credit Scoring Approaches Guidelines,* and ICCR, *Use of Alternative Data*.

OVERVIEW AND IMPLEMENTATION CONSIDERATIONS

3

OVERVIEW AND IMPLEMENTATION CONSIDERATIONS

This chapter provides an overview of consumer risks relevant to all or most of the four fintech products discussed in this paper—digital microcredit, P2PL, investment-based crowdfunding, and e-money—although the way relevant risks manifest may differ between those products. The chapter discusses both examples of how such risks arise in the context of the different products and examples of regulatory approaches intended to address them.

This chapter also discusses some key implementation considerations for regulators contemplating implementation of regulatory measures to address relevant consumer risks (see section 3.2). While the paper's focus is on regulation, not supervision, the important complementarity of supervision is also highlighted in this chapter.

3.1 CROSS-CUTTING RISKS AND REGULATORY APPROACHES

This section provides an overview of the following cross-cutting risks, and their corresponding regulatory approaches, relevant to most or all of the fintech products covered in this paper. The discussion draws examples from the product-specific chapters. The different contexts in which these risks may arise are discussed in more detail in chapters 4–7.

- **Gaps in regulatory perimeter:** Consumers of fintech products may receive less protection than consumers of traditional financial products if there are gaps in the coverage of their country's existing FCP regulation and financial sector oversight.
- **Fraud or other misconduct:** Factors such as the novelty, opaqueness, or complexity of certain fintech business models and fintech entities' responsibilities, as well as the lack of consumer familiarity, can lead to new or heightened risks of loss from fraud or misconduct by FSPs or third parties.
- **Platform/technology unreliability or vulnerability:** If a fintech platform or other systems underpinning a fintech offering are unreliable or vulnerable to external threats, they may expose consumers to heightened risks of loss and other harm.
- **Business failure or insolvency:** Consumers whose funds are held or administered by a fintech entity may risk losing those funds if the entity becomes insolvent or their business ceases to operate, and factors such as inexperienced entrants and riskier or novel business models can increase such risks.
- **Consumers not being provided with adequate information:** The standard risks arising from consumers not being provided with adequate product information can be heightened when new types of pricing, product features, and risks are introduced, or where digital channels for communication pose challenges to consumer comprehension.
- **Product unsuitability:** Fintech can increase access to riskier or complex financial products to consumers that may lack knowledge or experience to assess or use them properly, leading to greater risks of harm due to product unsuitability.
- **Conflicts of interest and conflicted business models:** Fintech business models may give rise to conflicts of interest under new circumstances not foreseen by regulators or expected by consumers.

- **Algorithmic decision-making:** The use of algorithms for consumer-related decisions is becoming particularly prevalent in highly automated fintech business models and some scoring decisions may lead to unfair, discriminatory, or biased outcomes.
- **Data privacy:** This is a particularly crucial consideration in relation to fintech offerings, given their highly data-driven nature.

a) Gaps in regulatory perimeter

Risks to consumers

Consumers of fintech products may risk receiving less protection than consumers of traditional financial products due to gaps in the coverage of their country's existing FCP regulation. The practical risk for consumers from such gaps is that fintech entities may not be obliged to address the range of consumer risks discussed later in this paper and that consumers do not have access to measures such as complaint-handling mechanisms because they do not extend to fintech offerings. A country's existing FCP rules may not extend to fintech products and thus may not protect their consumers due to the nature of those products or, even where a fintech product is equivalent to a traditional offering, due to the nature of the providers or their business arrangements. If a country's regulator lacks power to regulate or supervise fintech entrants in their market, this can hamper efforts to address such gaps.

Gaps in regulatory coverage frequently result from a fintech product not fitting easily within existing regulatory concepts. Even if the core nature of the product is familiar, key aspects may differ so significantly from those of traditional products that the fintech product does not fit clearly within categories contemplated by current FCP regulation. For example, in the case of P2PL, while platform operators may provide services to individual lenders/investors akin to traditional investment services (such as acting as an intermediary, operating a collective investment scheme, or providing financial advice), the novelty of P2PL arrangements has at times generated uncertainty regarding whether and how P2PL is subject to existing investor protection laws.[30]

Gaps in regulatory coverage of fintech offerings also frequently arise from regulation that covers financial products or services provided by traditional providers only, such as banks. This is sometimes referred to as institution-based regulation. In contrast, activity-based regulation focuses on the activity being undertaken, rather than the provider undertaking it. For example, in the case of digital microcredit, the core product—a loan—is the same as offered in a traditional credit context, with product differences usually relating only to distribution channel, pricing, and other features. However, the novel nature of the lender offering that digital microcredit—such as a non-financial entity or an app-based lender—may not fall within the existing authority of any financial sector regulatory body. Similarly, consumer peer-to-peer (P2P) loans are often unsecured, amortizing loans, very similar to personal installment loans provided by traditional lenders such as banks and finance companies. The key innovation in P2PL has been giving prospective borrowers access facilitated by technology—specifically by online platforms—to potential lenders that they did not have before. Although private individuals may be the lenders of record, they may not be subject to existing requirements in an institution-based framework and in any case are unlikely to be as well placed as the platform operator to meet FCP requirements. Another example arises from the challenges in regulating e-money products offered by mobile network operators (MNOs). These entities may be regulated in relation to their core business by a telecommunications regulator. However, in an institution-based model, their e-money activities are not necessarily regulated by the financial services regulator (such as the authority responsible for the payments system). A leading example of these challenges existed with the M-Pesa product in Kenya when it was initially offered by an MNO.

Gaps can still arise in regimes that adopt activity-based approaches if these are not sufficiently flexible to address differences between traditional and fintech business models. For example, the EU Directive 2008/48 on Consumer Credit Agreements, which mandates a range of FCP obligations for non-mortgage consumer lenders, applies to lenders only if undertaking lending in the course of a trade, business, or profession. In a P2PL business model where the platform operator facilitates lending by third parties, the operator would not be the regulated as the lender, given they are not the lender of record, despite controlling important aspects of the lending and being better placed to comply with relevant requirements.

A country's framework may not cover providers that offer services to consumers on a cross-border basis. A country's regulation may extend only to financial products offered by providers within the jurisdiction, rather than products offered to consumers in the jurisdiction regardless of the location of the provider. While such a gap may not affect only fintech offerings, the ease with which fintech products may be offered through digital channels increases the potential impact of this gap. For example, in a digital microcredit context, consumers may access ser-

vices of app-based lenders operating from outside their jurisdictions, making it difficult for authorities to monitor such activities. Similarly, a foreign-based crowdfunding platform could be soliciting and promoting investments to potential retail investors across borders.

Regulatory approaches

Applying FCP requirements by activity, rather than by type of institution, can help ensure that fintech entities are subject to FCP obligations regardless of their institutional type or business model. In the case of digital microcredit, countries that apply credit-related licensing and conduct regulation to all consumer credit-related activities, rather than to specific credit institutions, are better able to cover all models of digital microcredit, regardless of whether such activities are undertaken by bank or non-bank lenders, MNOs, some other kind of entity, or a combination of actors. Similarly, in the case of e-money, a range of jurisdictions apply an activities-based approach to licensing requirements for e-money issuers, allowing only licensed entities to offer such products, whether they are traditional banks or similar institutions or other kinds of entities. A few examples include Malawi,[31] the Philippines,[32] and Mexico.[33]

A focus on activities, rather than entity types, may also assist regulators in identifying and addressing consumer risks more comprehensively. An activity-based approach to regulatory policy may help regulators focus on risks that arise from each activity from a consumer perspective, regardless of the entity that engages in them.

Some countries have addressed coverage gaps by incorporating FCP rules into new frameworks for specific fintech products, separate from existing FCP requirements. There are many examples of regulatory frameworks developed for e-money that incorporate FCP rules. Under Ghana's Payment Systems and Services Act,[34] the only entities that can engage in "electronic money business" are licensed banks and licensed non-banks. The Malaysian Financial Services Act[35] takes an equivalent approach. Under that Act, no person can carry on a business of issuing a "designated payment instrument" (which includes "electronic money") unless it is approved by Bank Negara Malaysia (BNM). The Chinese authorities have issued a separate regulatory framework to cover P2PL activities.[36] Nigeria, among a range of jurisdictions that have taken a similar approach, is in the process of developing a crowdfunding-specific regulatory framework.[37]

Many countries have taken a hybrid approach, bringing fintech products within some existing FCP regulatory frameworks while also developing separate rules to address specific issues or concerns. Reasons for doing so vary; for example, adopting a hybrid approach may be considered more expedient in their domestic legal context, or more effective to address consumer issues. Mexico introduced a new overarching Financial Technology Institutions Law[38] (sometimes referred to as its Fintech Law) to cover fintech areas such as investment-based crowdfunding and P2PL. The law introduced some FCP requirements and allows regulators to issue additional FCP rules. However, Mexico already had in place a range of FCP requirements applicable to other financial institutions, such as the Law on Transparency for Financial Services.[39] Fintech entities regulated by the Financial Technology Institutions Law have also been made subject to these existing requirements. In the case of investment-based crowdfunding, while many countries' existing capital markets regulatory frameworks cover investment activities, adjustments have needed to be made to focus specifically on the nature of the participants in crowdfunding and their investment offerings.

A country's FCP regulator may lack the mandate to extend FCP rules to institutions that it does not already regulate. Until such a mandate can be extended, a short-term solution may be to leverage powers of other regulators, such as those responsible for general consumer protection. In Kenya, the Competition Authority of Kenya stepped in to issue rules on disclosure for digital financial services (including digital microcredit) for all providers, including those not regulated by financial sector authorities, to address pervasive concerns observed throughout the market.[40] Similarly, telecommunications authorities may be in a position to apply FCP requirements to MNOs entering the fintech space. While none of these approaches are necessarily ideal (and may raise difficulties in ongoing monitoring and enforcement), they could possibly be leveraged to achieve incremental progress in putting in place protections for consumers. Where such approaches are employed, close coordination will be necessary between sectoral authorities.

For activity-based coverage of FCP rules to be effective, the regulatory framework needs to incorporate concepts that are sufficiently broad and flexible to cover new and developing business models and entity roles. Some jurisdictions have found that broad concepts in existing legislation, such as relating to lending or investment activities, were effective in automatically extending regulation to new fintech offerings. Australian consumer credit legislation already regulated any "credit activities" involving consumers carried out as part of a business, including not only the provision of credit but also the provision of a range of credit-related assistance to consumers or acting as an intermediary between a lender and a consumer. It therefore was deemed to apply already to new P2PL platforms' intermediation activities.[41]

Explicit guidance may sometimes be used by regulators to clarify that existing rules already cover fintech activities. In the United States, the Securities and Exchange Commission (SEC) chose to send a strong signal to industry that the 1933 Securities Act[42] already applied to investment-related activities in a P2PL context by entering into a cease-and-desist order against a major P2PL platform on the basis it was not complying with the Act.[43]

Some authorities have considered it necessary to introduce brand-new concepts into legislation to capture fintech activities adequately. In the case of P2PL in the United Kingdom, existing rules were amended to provide for a new category of regulated firms undertaking the activity of "operating an electronic system in relation to lending."[44] Indonesia introduced a new category of activity referred to as "information technology–based loan services."[45] Regulators also started adjusting existing investor protection laws to reflect the nature of issuers and investors in the context of investment-based crowdfunding.[46] Regulators would ideally seek to avoid limiting descriptions of regulated activities to particular business models, so as to allow for further market development while avoiding the creation of new gaps. Nevertheless, these are likely to require continued monitoring and adjustment over time.

Addressing gaps in the coverage of cross-border fintech activities tends to require a range of measures. These include applying a country's FCP requirements (and regulators' mandates) to fintech entities dealing with consumers in that country, regardless of where the providers are based. In practical terms, however, measures such as cross-border coordination and cooperation between authorities (as also discussed in section 3.2 below) are usually necessary to support the enforcement of relevant requirements.

b) Fraud or other misconduct

Risks to consumers

A fundamental concern for consumers with respect to fintech products, and transacting through digital means more generally, is suffering losses from fraud or other misconduct by FSPs as well as third-party fraud. The circumstances under which such losses may arise are myriad, such as internal theft of funds, identity theft, or phishing. Potential perpetrators include FSPs themselves, their employees, agents, merchants, business partners and service providers, and external actors. These perpetrators, and the data or facilities being affected, may be located remotely (such as in the cloud) and even internationally, creating additional enforcement and evidence gathering difficulties.

Holders of e-money, for example, face the key risk of agent fraud, among other fraud risks. While not unique to e-money, agent-related fraud can be a significant risk, given the potentially extensive reliance on such agents. This can include agents charging unauthorized fees, splitting transactions or encouraging multiple accounts to earn more commissions, transferring account holders' funds to their own account, and "skimming" small extra amounts into their own accounts when processing a transaction.[47] Some of these risks can arise when consumers share their security credentials with an agent and if an agent assists a consumer with a specific transaction. They are especially likely to occur if the consumer has a low level of digital capability and needs assistance to process a transaction.

There have also been a number of significant incidents of fraud and misconduct involving P2PL and investment-based crowdfunding platforms. For example, extensive P2PL platform failures in China resulted in significant losses for many consumers,[48] with severe financial and personal impacts.[49] Some major failures were due to internal fraud, such as a platform ultimately found to be a Ponzi scheme (with most of its loan listings being fraudulent), causing almost 900,000 individual lenders/investors to lose the equivalent of $7.6 billion.[50] Investor fraud can similarly be perpetrated through crowdfunding platforms by issuers or by platform operators themselves. Issuers may try to defraud potential investors through fraudulent business proposal and plans, by concealing facts about their business history or management, or simply by using misleading promotion techniques. Consumers may also be subject to fraud from within the platform operator, such as sham or misleading offers. The extent of these risks can depend on the types of post-investment services the platform operator provides, such as whether the platform holds or receives client money, undertakes payment services (for example, channeling payments from issuers to investors), or if the platform operator represents investors through a nominee structure or runs a secondary market for issued securities. Risks also arise from crowdfunding trading platforms and bulletin boards used in secondary markets for the exchange of information about crowdfunding securities. Of course, there may also be a risk of entirely fraudulent crowdfunding sites.

Lenders/investors involved in P2PL are also at risk of losing funds provided to fraudulent borrowers, while fraudulent apps pose risks to digital microcredit borrowers. The fraud may involve a borrower (or a purported operator) absconding with the relevant funds as soon as they are provided or a borrower providing incorrect information about their ability to repay a loan (such as information about their income). For digital microcredit,

consumers face risks due to fraudulent lending apps that solicit application fees or personal data but fail to provide any credit.

Cross-cutting regulatory approaches

Authorization and vetting requirements

Requiring fintech entities to be licensed or registered and vetted prior to being granted such license or registration can be an important mechanism to filter out unscrupulous entities that are more likely to commit fraud or engage in other misconduct. Such vetting, as well as scrutinizing matters such as any prior criminal history or other history of bad conduct, may examine the ability of entities and their management to deal with the risk of internal or third-party fraud and misconduct. Ideally, such requirements are accompanied by awareness campaigns encouraging consumers to deal only with licensed or registered entities. As discussed above in the context of regulatory perimeter gaps, many jurisdictions require e-money issuers to be licensed or registered. Some countries require the licensing or authorization of all providers of consumer credit, such as in Australia[51] and Portugal, which effectively results in all digital microcredit providers being required to be licensed or authorized. Licensing or registration requirements have rapidly been adopted internationally in relation to P2PL. For example, this was recommended by the European Banking Authority (EBA) in the European Union,[52] and some European jurisdictions already had such regimes). Recent reforms in China now mean that P2PL platform operators are required to go through multiple stages of authorization, including vetting requirements.[53] As noted above, the United Kingdom introduced in its new rules the activity of "operating an electronic system in relation to lending," which requires authorization. Crowdfunding authorization approaches similarly vary across jurisdictions. Some jurisdictions, such as the European Union[54] or United States,[55] have created specific bespoke categories for crowdfunding platform operators, while others, such Australia,[56] Dubai,[57] and Nigeria,[58] apply existing categories of authorized firms as the bases for licensing crowdfunding activities.

Vetting requirements to support authorization frameworks generally focus on good reputation and adequate knowledge and experience/qualifications of fintech entities and their management as the main principles to be followed when authorizing their activities. As the EBA notes in relation to P2PL platforms, this could comprise checking that individuals managing a platform meet appropriate standards for competence, capability, and integrity.[59] This should be the case both when first applying for authorization and on an ongoing basis while they continue to be authorized. The Reserve Bank of India (RBI) requires P2PL operators to ensure that they meet fit and proper criteria at the time of their appointment as well as on an ongoing basis. In Dubai, senior managers and directors of investment-based crowdfunding platform operators must pass fit and proper criteria, including that they must have recognized knowledge and experience and be of good professional repute.[60]

Risk management and governance requirements

Regulators are increasingly subjecting fintech entities to general risk management and governance obligations that often apply to traditional providers.[61] Such obligations are generally intended to be flexible and set expectations on fintech entities that adjust to the characteristics of their business and circumstances. For example, fintech entities in the United Kingdom are subject to several overarching obligations (known as the "Principles for Business") that apply to authorized firms. One is that they must take reasonable care to organize and control their affairs responsibly and effectively, with adequate risk management systems.[62] Drawing from this principle, the UK Financial Conduct Authority (FCA) has issued more extensive general obligations and guidance with regard to risk management.[63] Mexico's Financial Technology Institutions Law similarly makes demonstrating implementation of controls for operational risk a key aspect of being authorized as a fintech operator, as well as more specifically fraud prevention.[64]

Technology-related and cyber risk management requirements are also an essential mitigant to address fraud risk that arises from vulnerabilities affecting a fintech platform or other systems. These are discussed below in the context of platform and technology unreliability and vulnerability risks.

Regulators have also been mandating the reporting of large-scale fraud and security breaches to assist their response. For example, the European Union,[65] Ethiopia,[66] and Kenya[67] require reporting to the regulator of such events in relation to payment products. The European Union's Directive 2015/2366 on Payment Services (PSD2) also requires that users be informed of any security incident that "may have an impact" on their financial interests.[68]

Liability and responsibility for staff and agents

While providers to some extent may be liable for the conduct of persons acting on their behalf under general laws (for example, on employment or agency), regulators frequently consider it necessary to impose clear responsibility and liability for such matters on the principal. For example, Ghana's Payment Systems and Services Act makes a principal liable for all acts of an agent

"in respect of the agency business" and explicitly states that this liability applies even if the acts are not authorized by the agency agreement.[69]

Warnings and information for consumers

Some jurisdictions impose requirements on providers to warn consumers about risks associated with fintech products. These requirements frequently cover more than fraud-related risks and are discussed in more detail in the section on information-related risks below.

Segregation of client funds

Requirements that consumers' funds be segregated from other funds held by a fintech entity, and held with appropriately regulated institutions, can also mitigate to some extent against risk of losses due to fraud. Such segregation can make it more difficult for funds to be misappropriated, such as in the context of fraudulent schemes internal to the entity. These regulatory measures are discussed in more detail below in the context of risks of loss that may arise due to entity insolvency or business failure.

Product-specific regulatory approaches

Regulators have also been implementing regulatory requirements seeking to address specific circumstances under which fraud may arise in relation to particular products. These are discussed in more detail in the product-specific sections of the paper.

Key examples of such mitigants in an e-money and broader payment-transactions context include requirements for authenticating transactions and limitations on consumer liability for unauthorized transactions. These are often balanced by obligations on consumers to report relevant incidents and take certain precautions within their control. For example, the European Union's PSD2 mandates "strong customer authentication" (defined in some detail to include the use of two or more independent elements—that is, two-factor authentication) as a means to mitigate the risk of fraudulent transactions. Ghana's Payment Systems and Services Act requires a provider to "ensure" that a transaction against an account is authorized by the account holder.[70] The European Union's PSD2 also places a cap on consumer liability for unauthorized transactions of €50 unless there is fraud or gross negligence by the consumer.[71] However, the provider may not be liable if notice of an unauthorized transaction is not given in a specified period.[72] Users must be advised of their obligation to report events such as lost or stolen mobile devices or compromised security credentials "without undue delay" and be provided with "appropriate means" to make such reports.[73] The European Union's PSD2 also places the burden of proof on the provider if they want to show a consumer's liability for all or part of an unauthorized transaction.[74]

In fintech business models where consumers may suffer loss due to fraud by external participants facilitated by a platform operator, such as fraud by issuers on investment-based crowdfunding platforms or borrowers on P2PL platforms, an important mitigant is requiring appropriate due diligence by platform operators. The level of thoroughness and efforts required of platform operators differ among jurisdictions. They can range from platform operators simply being expected to satisfy themselves that a fraud is highly unlikely in a particular case to expecting operators to examine the appropriateness of issuers' business plans. In the United States, a crowdfunding platform operator (funding portal) needs to deny access to an issuer if it has a reasonable basis for believing that the issuer or the offering presents the potential for fraud or otherwise raises concerns about investor protection.[75] However, there is no obligation for a funding portal to fact-check the business plan of an issuer. In the United Kingdom, the FCA does not prescribe due diligence requirements for platform operators but requires that platforms disclose to investors the level of due diligence undertaken. Platform operators are also under a general duty to exercise skill, care, and diligence as well as to act in the customers' best interests.[76] In Australia, platform operators have to check the identity and eligibility of the issuer, whether managers are fit and proper, and the completeness and legibility of the offer document.[77] Dubai and Malaysia have more stringent requirements. In Dubai, an operator must conduct extensive due diligence on each issuer before allowing it to use its service.[78] Malaysia's requirements, while less detailed, do require the platform operator to verify the issuer's business proposition in addition to conducting background checks to ensure the issuer, its management, and its owners are fit and proper.[79] Requirements for assessing prospective borrowers on P2PL platforms discussed in the section below dealing with product suitability would also be relevant in mitigating potential fraud risk by such borrowers.

FCP regulatory measures against fraud should of course be additional to a country's financial crime measures under anti-money laundering/countering the financing of terrorism (AML/CFT) laws and general criminal laws. Ideally, financial sector regulators should closely monitor the incidence of such activities in consultation with other national agencies and implement FCP mitigants particularly where risks may be more appropriately dealt with, or borne by, fintech entities, rather than consumers.

c) Platform/technology unreliability or vulnerability

Risks to consumers

If a fintech platform or other technology systems underpinning a fintech offering are unreliable or vulnerable to external threats, they may expose consumers to heightened risks of loss and other harm. When acquiring traditional financial products or services, consumers already face some level of risk of harm resulting from interruptions or failures in an FSP's processes and systems. However, the extent of these risks is likely to be particularly high in a fintech context, given the extent of reliance on technological processes that, in some cases, may be relatively new. A working group of the Bank for International Settlements' (BIS) Committee on the Global Financial System relevantly noted, for example, that fintech credit platforms may be more vulnerable than banks to certain operational risks, such as cyber risk, due to their reliance on relatively new digital processes.[80] Another aspect that can give rise to additional risk is significant reliance on third-party providers, with potential disruption of outsourced services. Lack of reliability issues can obviously also be affected by broader issues of connectivity and telecommunications infrastructure affecting a country, although measures to address these going beyond FCP are outside of the scope of this paper.

Such unreliability or vulnerability can have a range of adverse impacts on consumers, ranging from inconvenience and poor service to monetary losses due to third-party fraud or loss of data integrity. Such impacts could mean, for example, that e-money transactions cannot be initiated or completed as expected, that credit repayments due under P2PL or digital microcredit facilities are not processed in a timely manner, that there are delays in receiving loans, or that crowdfunding investors do not receive the financial returns to which they are entitled. Consumers may lose funds, incur additional charges (such as late payment fees and penalty interest), or forgo gains if transactions cannot be completed on time or correctly. Platform or technology vulnerability may also contribute to third-party fraud due to vulnerability to cyber risks. In a recent large-scale fraud in Uganda, hackers reportedly broke into the systems of Pegasus Technologies, which processes mobile money transactions for entities such as MTN Uganda, Airtel Money, and Stanbic Bank.[81]

Cross-cutting regulatory approaches

General risk management requirements

As discussed above in the context of mitigants against fraud risks, regulators are increasingly subjecting fintech entities to general risk management and governance obligations. The expectations imposed by such requirements would clearly also target the need for fintech entities to address risks related to platform and other technology unreliability and vulnerabilities.

Targeted risk management and operational reliability requirements

Regulators are increasingly making FSPs, including fintech entities, subject to specific obligations targeting technology and systems-related risks and reliability issues. In Indonesia, a P2PL platform operator must meet a range of obligations with regard to its information technology and the security of that technology, including resilience to system interference and failures.[82] Requirements include rules on the establishment of a disaster recovery center, acquisition and management of information technology, and incident management and implementation of security measures. In the case of e-money issuers, the European Union's PSD2 requires that payment service providers have appropriate mitigation measures and control mechanisms to manage operational (and security) risks, and that they report to the regulator about these risks at least annually.[83] In Malaysia, e-money issuers must comply with detailed requirements including for comprehensive and well-documented operational and technical procedures to ensure operational reliability and a robust business continuity framework, including a reliable back-up system.[84] Ghana goes so far as to specify a very specific requirement that an e-money issuer (or a payment service provider) ensure "high quality performance of at least 99.5% service availability and accessibility."[85]

Outsourcing-related risk management

Given the extent to which fintech entities may outsource a range of their activities to third parties,[86] an important risk management obligation would be to take appropriate steps to avoid additional operational risk resulting from such outsourcing. In the case of P2PL platform operators, for example, the RBI's rules set out obligations for operators to ensure sound and responsive risk management practices for effective oversight, due diligence, and management of risks arising from outsourced activities.[87] Ensuring that fintech entities remain legally responsible to consumers for outsourced functions can also assist—as contemplated, for example, by the European Union's crowdfunding regulation.[88]

Product-specific regulatory approaches

Regulators have also been implementing regulatory requirements addressing how reliability and vulnerability issues may affect specific fintech products. In the case of e-money, regulators are mandating time frames within which transactions must be processed—such as the European Union's PSD2 requirement that payments be credited to the payee by the end of the business day after the time of receipt.[89] Requirements that users be noti-

fied of service interruptions have also been introduced in a range of jurisdictions to assist consumers to mitigate the impact. For example, Ghana requires that users of e-money be notified within 24 hours of a service disruption or an anticipated disruption.[90]

d) Business failure or insolvency

Risks to consumers

Consumers whose funds are held or administered by a fintech entity may risk losing those funds if the entity becomes insolvent or their business ceases to operate. The fact that many fintech entities are relatively new entrants in the financial sector increases those risks. The nature and extent of such risk also depends on the particular fintech business model employed, as well as the fintech product and the applicable regulatory framework.

A consumer participating in P2PL as a lender/investor may risk losing their committed loan principal, or repayments owed to them, that are being held or administered by a platform operator that goes insolvent or fails. Borrowers can also face risks of losing funds under such circumstances. For example, when consulting on proposed regulatory reforms for P2PL in the United Kingdom, the FCA said it considered P2PL platform operators to present a high risk of consumer harm, given they may hold or control client funds before lending these to borrowers.[91] Likewise, a borrower may miss out on receiving funds intended for them from lenders/investors as a result of the operator's insolvency. The EBA has pointed out the risk of a lender/investor's funds not being transferred to the intended borrower if the platform is not required to hold appropriate regulatory authorizations and have in place adequate arrangements to safeguard such funds.[92] Depending on the legal relationships between the parties, borrowers may also suffer loss of funds that they are seeking to repay through the platform but fail to reach lenders/investors.

Consumers acting as lenders/investors run the risk of suffering losses in the event of a P2PL platform operator's business failure (regardless of cause) even if their assets are ring-fenced from the operator's insolvency as already discussed above. Business cessation can mean that individual loans that remain viable may not continue to be administered properly, causing corresponding loss. An investor can suffer considerable harm if a P2PL platform ceases to provide management and administration services. In practical terms, this can mean an individual lender/investor not receiving some or all of the repayments for the loans that they made or invested in through the platform, unless they retrieve payments directly from borrowers themselves.

An investment-based crowdfunding platform's failure can similarly leave investors without services essential to realizing the full value of their investment. The extent and nature of such risk depend on factors such as whether the platform holds client money, undertakes payment services (for example, channeling payments from issuers to investors), represents investors through a nominee structure, or runs a secondary market for issued securities. Loss of access to such services from the operator due to temporary or permanent platform failure can cause financial loss as well as operational detriment to investors.

If an e-money provider becomes insolvent then, depending on the way funds are held and controlled, funds may be insufficient to meet the demands of e-money holders or other unsecured creditors. This is a particular concern with e-money not considered a "deposit" protected under banking laws and without the benefit of deposit insurance. Operational failure may also make it difficult for consumers to retrieve their funds.

Regulatory approaches

Segregation of client funds

A key mechanism to address the risk of loss of funds due to operator insolvency in the case of P2PL and crowdfunding platforms, as well mishandling more broadly, are requirements for client funds to be segregated from other funds held by the platform operator. As highlighted by the EBA, for P2PL arrangements the main alternatives entail either the platform operator being appropriately authorized and regulated (such as with regard to capital requirements) to hold such funds, before being permitted to undertake money-handling activities on investors' behalf, or the operator having to ensure that a separate, appropriately regulated entity handles those funds on investors' behalf.[93] Both the RBI[94] in India and Otoritas Jasa Keuangan (OJK), the Indonesian Financial Services Authority,[95] have mandated that P2PL platform operators operate escrow accounts for this purpose. In the United Kingdom, key requirements in this regard are that the platform operator would be required to deposit such funds at an appropriate institution (that is, a bank), keep records and accounts, and conduct appropriate internal and external reconciliations so they can always distinguish been funds held for different clients.[96] Recent reforms in China mandate separation of platform owners' funds from those of lenders/investors and borrowers. Equivalent measures can be seen internationally in relation to handling of investor funds by investment-based crowdfunding platforms. In the United States, platform operators are prohibited from holding, possessing, or handling investor funds (or securities). In France, crowdfunding platforms likewise may neither receive funds directly from investors (except for payment of their own fees) nor receive securities from issuing companies.[97]

Requirements for issuers to isolate and ring-fence funds paid by e-money holders are a well-recognized core regulatory mitigant for e-money arrangements. Regulators typically also apply requirements to safeguard such funds in the holding institution. There are many country examples of such requirements. Malawi's Payment Systems (E-Money) Regulations require that an e-money service provider maintain a trust account at a bank that holds an amount no less than 100 percent of outstanding balances, and no more than 50 percent may be held in any one bank. The funds in the trust account must be unencumbered and must not be intermediated.[98] In some cases, trust account (or equivalent) obligations apply only to non-bank issuers; banks that issue e-money have lesser obligations (presumably because of the prudential regulations that already apply to them). For example, in Tanzania banks that are e-money issuers have to open a "special account" to maintain funds deposited by non-bank customers issued with e-money. In order to protect e-money customers' funds deposited in banks, some countries require safeguarded funds to be held in more than one bank when they reach a certain threshold. In Kenya, if the relevant amount is over K Sh 100 million, then the funds must be held in a minimum of two "strong rated banks" with a maximum of 25 percent in any one bank. [99]

Another approach taken by some jurisdictions is to extend deposit insurance to e-money accounts or corresponding custodial accounts at deposit-taking institutions or, if not, to make sure that consumers are aware of the fact that no deposit protection is being applied to their accounts. In Ghana, an e-money holder is eligible for protection under the Ghana Deposit Protection Act provided their balance is within the prescribed threshold.[100] In the United States, the Federal Deposit Insurance Corporation has rules to the effect that the deposit insurance scheme covering a pooled account held for the purposes of a prepaid card program will pass through to the individual card holders under certain conditions.[101]

Business continuity arrangements

Regulators have been requiring fintech entities to put in place business continuity arrangements in order to ensure the ongoing administration of consumers' funds and investments in the event of platform failure. These arrangements typically require plans to be developed that will allow orderly continuation of post-investment services in case of a wind-down of a platform. In France, P2PL platform operators are required to enter into a contract with a third-party payment institution to ensure such business continuity.[102] The EBA suggests that, to address relevant risks in the case of permanent, rather than temporary, platform failure, platform operators should be required to have resolution plans in place allowing loans to continue to be administered.[103] In Dubai, an operator must maintain a business-cessation plan that sets out appropriate contingency arrangements to ensure the orderly administration of investments in the event that it ceases to carry on its business, and the operator must review its business-cessation plan at least annually to take into account any changes to its business model or to the risks to which it is exposed.

E-money regulatory frameworks also frequently have business continuity requirements. For example, PSD2 requires an applicant for authorization as a payments institution to provide a description of business continuity arrangements including clear identification of critical operations, contingency plans, and a procedure to test and review the adequacy and efficacy of those plans regularly.[104]

Record-keeping requirements

Record-keeping arrangements are also used as a mitigant in this context, although they are obviously crucial more broadly to support the integrity of a fintech entity's business operations. P2PL platform operators in the United Kingdom are subject to general requirements, as authorized firms, to keep orderly records of their business, including all the services and transactions undertaken. Other examples in the e-money context are requirements to maintain records and accounts for e-money activities that are separate from other business activities. Malaysia has such a requirement in addition to a general requirement to have adequate information and accounting systems and a proper reconciliation process and accounting treatment for e-money transactions.[105]

Risk management requirements

Risk management and governance obligations of the kinds already discussed above of course may also reduce these risks. This would include both management of risks that may ultimately lead to business failure as well as its impacts on consumers.

e) Consumers not provided with adequate information

Fintech introduces a range of new manifestations of risks for consumers with respect to information disclosure and transparency. As is often the case with traditional offerings, information about pricing, risks, and terms of fintech products may be incomplete or insufficiently clear. These traditional risks to consumers are heightened when consumers are unfamiliar with new types of pricing and fees, product features, terms and conditions (T&C), and risks related to fintech products. Crucially, the digital format of delivery poses inherent

challenges to consumer comprehension that can require specific mitigation measures.

The risk of inadequate information being provided to consumers

Consumers often face incomplete or unclear information about pricing when obtaining fintech products. A 2015 survey of regulators in 15 developing countries found that limited disclosure of costs was the highest market conduct concern for regulators with respect to digital microcredit.[106] Disclosure of pricing for digital microcredit products is often incomplete and not transparent; different and complex methods are used to convey pricing. As a result, it is difficult for consumers to understand the full costs of a digital microcredit product or to compare across providers.

Fees and charges are often not communicated clearly. Disclosure of fees and charges for third-party services has also been found to be frequently incomplete with respect to digital microcredit. Fees and charges associated with services provided by P2PL platforms (for example, loan origination, loan servicing) and fees for e-money transactions (such as cash-in and cash-out) have also been noted to be frequently opaque.

Beyond pricing, consumers may face inadequate access to the full T&C of a fintech product. Information about e-money product features such as available transaction types and elements, points of service, and transaction and balance limits are necessary for consumers to be able to select products that best meet their needs. Full T&C are often not easily accessible over digital channels, particularly with respect to feature phones. Given the limited space available to convey information, providers may favor displaying appealing information, providing incomplete information about consumer obligations, or merely referring to T&C to be found elsewhere.

Incomplete information about risks related to fintech products poses a particular concern given the novelty of fintech products and the lack of experience of retail consumers. For example, traditional risks related to non-repayment of loans can be heightened when the typical users of digital microcredit lack understanding of borrower obligations. Similarly, in the case of P2PL, consumers acting as lenders/investors may lack understanding of loan-related risks or perceive them as equivalent to risks of other investment types. E-money users may lack understanding of the security and technology-related risks related to e-money.

For platform finance, lack of adequate information about the risks and returns of potential investments combined with overreliance on the platform can harm investors. P2PL platform operators may not have the systems to gather sufficient information about loans being offered necessary to produce appropriate disclosures regarding risks and returns. Crowdfunding issuers tend to be smaller businesses about which more limited information is available. Consumers investing in either kind of platform may not appreciate the significance of a lack of data in assessing the risk of their investments. They may be attracted to platform finance as a new form of investment but lack familiarity with the true nature of risks associated with the new types of investment products offered via such platforms. Consumers would often lack the resources necessary to analyze investments fully themselves and may also place excessive reliance on a platform operator's risk assessments or loan or investment selection, which may be of varying quality.

Inadequate information can lead consumers to choose inappropriate products that ultimately harm their welfare. For example, experiencing poor transparency, such as unexpected fees or not understanding the terms of a loan, correlated with higher levels of late repayment and default for digital microcredit in Kenya and Tanzania.[107] A lack of adequate information about key aspects of P2PL and crowdfunding, such as costs, risks, and rights and obligations, can increase the risk that investors will make decisions that are uninformed or imprudent, which may lead to unexpected losses or consumers overpaying for their investments. In the United Kingdom, the FCA expressed concern about customers being misled by comparative cost claims and missing out on services that are better suited to their needs.[108]

If information from different fintech entities cannot be compared easily, consumers may find it difficult to compare offerings or to realize differences when switching between providers. For example, methods used by P2PL platform operators to calculate risk-adjusted net returns may differ considerably between platforms due to a lack of common standards.[109] Platform operators also may not make sufficiently clear the methodology used to make such calculations.

In addition to the aforementioned risks related to inadequate up-front information, a lack of key information on an ongoing basis also poses risks to consumers. This includes lack of adequate ongoing information about the ongoing status of investments for platform finance investors, hampering their ability to adjust to changes and compounding the risks from their lack of understanding and familiarity of such investments. E-money users may not be provided with sufficiently detailed transaction receipts or periodic account information, making it difficult to track

their accounts and identify any fraudulent activity or mistaken transactions.

Regulatory approaches for inadequate information

Fundamental good practices for disclosure and transparency remain highly relevant to fintech products. Providing excessive information can easily overwhelm consumers and is not the solution. Effective disclosure requires a combination of key information provided up front, access to fuller details, and information provided in a format and manner that enhances comprehension and allows for comparison. International good practice on disclosure generally indicates that fintech entities should be required to provide clear and sufficiently comprehensive information on pricing and fees, product features, T&C, and risks and returns. Regulators may sometimes benefit from being prescriptive regarding what information is deemed the most critical for up-front disclosure for fintech products in order to ensure consistent and adequate disclosure across all providers. In the United States, the lender of record for a P2P loan is subject to the prescriptive provisions of the Truth in Lending Act[110] and its implementing Regulation Z,[111] (collectively, TILA) which apply to other lenders. Many of the e-money regulatory frameworks, such as Kenya's, also include disclosure and transparency requirements, such as to disclose fees and charges and other T&C to consumers on taking up the product and also to require public disclosure of fees and charges.[112]

Adaptations and enhancements are likely to be necessary to address unique aspects of fintech offerings. Standardized total cost indicators already in use in relation to traditional credit products, such as annual percentage rate (APR) and total cost of credit (TCC), have been shown to help consumers select lower-cost loan products.[113] Giving such indicators prominence when conveyed via digital channels could assist consumers in making borrowing decisions. Similarly, to ensure adequate access to information, e-money issuers may be required to disclose fees and charges for e-money via agents, branches, and websites[114] and to require disclosure of both up-front fees and charges and transaction-based fees.[115]

Mandating content of terms and conditions

Authorities may seek to mandate the content of contractual T&C for fintech products, but it would be important to ensure that these cover all key aspects for consumers. P2PL platform operators in Brazil must include information on the rights, obligations, and responsibilities between the investor, borrower, and platform in P2P loan agreements.[116] Countries such as Kenya[117] and the Philippines[118] require that e-money issuers provide a written agreement to each consumer covering the terms of the service and any related fees.

Requiring summaries and targeted disclosures

A summary of key T&C can be an important transparency measure (in addition to ensuring that consumers are given access to full T&C). This measure can take on added importance in the context of digital channels, where consumers may find it more difficult to review full T&C, or the speed of transacting creates less propensity to do so. For example, when conducting sales of retail banking products and services via digital channels, financial institutions in Portugal are required to "prominently present information on the basic features of the banking product or service and on other elements deemed relevant, such as fees and expenses that may be applicable, on the main screen or webpage of the marketing platform, using larger characters, information boxes, pop-ups, simulations, overviews or other similar means."[119] Additional approaches to counteract the difficulties in conveying full T&C via mobile channels include making the full T&C easily accessible to customers on an ongoing basis[120] or requiring public disclosure of standard T&C.[121]

Disclosure requirements that address and highlight key risks and their consequences, and other key aspects for consumers' decisions, are likely to be particularly important for fintech products given their novelty and consumers' lack of familiarity with such products. For digital microcredit, this includes highlighting the consequences of late payments and defaults, while e-money risks may relate to mistaken authorizations, fraud, or security. For platform finance, key matters can include risks affected by the role of platform operators and, for consumers investing through those platforms, factors affecting their returns. P2PL operators in China are required to provide a range of information to the general public (including information about the platform operator and their past and current loans) as well as to prospective lenders/investors (including information about the borrower, relevant loan, and the operator's risk assessment in relation to the loan).[122] P2PL operators in Brazil must provide prospective lenders/investors with expected rates of return, taking into account expected payment flows, taxes, fees, insurance, and other expenses.[123] Issuers on crowdfunding platforms are typically required to disclose information about the company; its ownership and capital structure; financial information; its business plan; the main risks facing the issuer's business; and the targeted offering amount and intended use of proceeds.

Warnings

Obliging fintech entities to provide warnings or disclaimers in key contexts can highlight risks for consumers and assist in balancing out inappropriately optimistic perceptions. P2PL platform operators in the United Kingdom are subject to general rules on disclo-

sure of past performance that include providing a prominent warning that past performance is not a reliable indicator of future results.[124] Brazilian authorities require that P2PL platform operators display on their website and in other electronic channels, as well as in promotional materials, a prominent warning that P2P loans constitute risky investments and are not subject to deposit insurance.[125] In some jurisdictions, warnings are also coupled with acknowledgments from lenders/investors. For example, the RBI requires P2PL platform operators to obtain explicit confirmation from a prospective lender/investor that they understand the risks associated with the proposed transaction, that there is no guarantee of return, and that there exists a likelihood of loss of the entire principal in case of default by a borrower.[126] However, it would also be important to ensure that any such warnings or acknowledgments are not seen by regulators or fintech entities (or misunderstood by consumers) as reducing the onus on fintech entities to comply with their obligations and address relevant risks where appropriate.

Ongoing disclosure requirements

Requiring the ongoing provision of key information is intended to address risks such as that consumers may lack awareness of the latest activity related to their fintech product or service, or of key changes made to contractual terms after acquisition of the product or service. For P2PL, such requirements include obliging platform operators to provide lenders/investors with ongoing information about their individual loans/investments, as well as matters relating to the circumstances of the platform that may affect those loans.[127] Lenders/investors may also benefit from periodic updates regarding the general performance of the operator, as well as notice of adverse events. Platform operators in China are required to disclose publicly within 48 hours if they have been affected by any of a range of adverse circumstances, such as bankruptcy events, cessation or suspension of business operations, or significant litigation, fraud, or other incidents affecting its operations in a manner that may damage borrowers' interests.[128] E-money providers are variously being required to provide transaction receipts;[129] to provide periodic statements and recent transaction details or make them easily accessible;[130] and to notify consumers of changes to T&C or fees and charges, a general requirement that should apply for all fintech products.[131] In addition, mobile channels do not need to pose only an obstacle to disclosure and transparency; they can also be leveraged for convenient, immediate, and direct transmission of messages and updates to consumers, such as reminders of upcoming payments or warnings about late payment penalties for digital microcredit.

The risk of information being provided in a poor format

Disclosing information in a clear and effective format is critical for consumer comprehension. As with any type of financial product, providing all relevant information but in a poorly designed format or manner can easily overwhelm consumers and make disclosure ineffective. This risk can be further heightened by lack of familiarity with the pricing and features of fintech products and services, inconsistent and incomplete methods of disclosing pricing and other T&C, and the challenges inherent in disclosing information clearly via digital channels.

Fintech entities may use inconsistent practices to disclose costs. As noted above, costs associated with digital microcredit have been found to be disclosed frequently as either rates or monetary figures and using a variety of repayment periods. The proliferation of different and sometimes complex pricing methods can be confusing for consumers and, in some cases, has been actively employed by digital microcredit providers to disguise fees.

Several unique challenges to disclosure and transparency arise due to the nature of digital channels. Particularly with respect to fintech products delivered via feature phones, practical limitations on the space to convey information as well as the ability use different design formats pose a challenge to transparency. Consumers may take a transaction on a mobile phone less seriously than a transaction in a bank branch, attention spans may be more limited, and the desire for rapid transactions may be increased. Even where consumers are provided with relevant information, the information may not be provided in a form that allows them to retain it for future reference (a particular challenge with respect to interactions via feature phones).

The timing and flow of information disclosed via digital channels can also impede transparency. Consumers may not be given sufficient time to review information on a screen before it times out. Websites and app-based content may be difficult to navigate and may de-emphasize less appealing information. User interfaces and menus on mobile channels may be confusing and not user-friendly, hampering effective disclosure as well as increasing the likelihood of consumers making mistakes when conducting transactions.

Regulatory approaches for poor disclosure formats

Rules mandating greater standardization of pricing and fees are a developing area. The ITU-T Focus Group on Digital Financial Services recommends that regulators should establish standard definitions for the cost and fees of digital microcredit, including all bundled services;

require disclosure in line with these standard definitions to ensure consistency across offerings; and require clear, conspicuous, and understandable disclosure of financial and other consequences of early, partial, late, or non-repayment of a digital loan.[132]

Plain language requirements, frequently applied to traditional products, are equally relevant to information disclosed regarding fintech products. There are various examples of requirements for "clear" and "understandable" terms with respect to e-money.[133] Disclosure for fintech products should avoid excess technical jargon. For example, the FCA undertook an initiative to consider the changes required for effective digital disclosure that allow for innovation while clarifying compliance with existing rules. The FCA emphasized the need for providers to develop consistent terminology and reduce the complexity of language and technical jargon.[134] Consideration may also be required regarding how graphic elements affect readability, particularly with respect to digital channels. In Portugal, best practices from Banco de Portugal (BdP) applicable to the sales of retail banking products and services via digital channels include that financial institutions "evaluate the use of graphic elements such as font size, color, icons and images in all information media, including on the screens of the marketing platform and in advertising, ensuring that those elements are not likely to affect the readability, understanding, and prominent of information."[135]

Provision of standardized information summaries/key facts statements (KFSs), typically via paper-based approaches, will require adaptation for digital channels. Approaches may need to vary depending on the level of standardization of the fintech product in question and the main channels via which the product is conveyed. For digital microcredit delivered via mobile phones, a summary of key T&C in a streamlined format may strike a sufficient balance between the limitations of devices and the need to ensure that key information is highlighted for consumers up front. Consumer testing on disclosure for digital microcredit in Kenya found that simpler versions of T&C led to better comprehension and more searching for products from other providers.[136] Adapting disclosure requirements for mobile channels could involve breaking down information into bite-sized chunks ordered in a more consistent manner across providers (for example, by fees, conditions and risks). For example, the FCA has asked providers to do more to incentivize consumers to engage with information delivered in a digital environment, including by layering information as a means to guide consumers through their journey in a way that enables them to digest each part easily, rather than including all information up front.[137]

Requirements regarding how key information should be positioned and given prominence, already established for paper documents, are increasingly being extended to digital channels. For example, disclosure requirements imposed by authorities in Brazil include an obligation that relevant information be displayed prominently on relevant electronic channels.[138] P2PL requirements in China include that mandated disclosures be set out in a dedicated, conspicuous section of websites and equivalent electronic channels.[139] BdP specifically notes that institutions that sell banking products or services through digital channels "should ensure that the information provided in these channels about those products or services is appropriate in terms of content, form of presentation and prominence, especially taking into account the marketing platform and the devices that bank customers may use to purchase these products or services."[140] Notably, this approach is specifically made to apply across all various digital marketing platforms and devices.

A range of approaches can be used to counterbalance some inherent limitations of digital disclosure. Prior to concluding transactions, providers could be required to give consumers access to additional channels, such as call centers, online chat, and agent/branch locations, in order to ask questions, clarify T&C, and obtain further assistance via live interaction with provider staff. For example, when conducting sales of retail banking products and services via digital channels, financial institutions in Portugal are required to assist customers to obtain further information by making available tools such as a hotline or live chat, chatbot, or other interactive tools.[141] In Ghana, e-money issuers are required to explain the "product material" and "general product elements" to prospective clients and "ensure that prospective client understands the nature and form of the product T&C, features and specifications."[142]

The order and flow in which information is required to be provided can also assist to enhance transparency and comprehension. As noted by the FCA, it can be beneficial to approach disclosure as a "digital journey" with an engaging digital format for consumers to progress through the steps of a transaction.[143] The Australian Securities and Investments Commission's (ASIC) guidance on good practices for digital disclosure notes that providers should consider whether disclosure flows logically in a way that aids understanding of the product.[144] There is international recognition of the need for appropriate prominence to be given to each aspect of a product, and that disclosure should not divert consumers away from less appealing information. In Kenya, the Competition Authority of Kenya (CAK) identified a particular issue with consumers not being aware of charges for transactions via mobile wallets because

providers were not disclosing the cost of such transactions until after the consumer accepted the transaction on their mobile device. The CAK therefore issued guidelines requiring all providers to disclose fully all applicable charges to customers for the mobile money service offered (including money transfers, microloans, and microinsurance) prior to completion of a transaction.[145] A survey of digital financial services users in Kenya found that the proportion of survey participants who could correctly estimate the cost of their last M-Shwari loan of K Sh 200 went up from 52 percent before the CAK order to 80 percent afterward.[146] Also in Kenya, consumer testing on disclosure of information for digital microcredit found that just moving the option to view T&C from the last option in the main menu for a digital loan product to its own screen increased consumer viewing of T&C from 9.5 percent to 23.8 percent.[147]

Regulatory requirements are also increasingly likely to be informed by behavioral insights, including into how consumers access financial products in a digital environment. In the aforementioned consumer study on digital microcredit in Kenya, requiring an opt-out approach to viewing T&C increased the rate of viewing from 10 percent to 24 percent, and the resulting delinquency rate was 7 percent lower for borrowers who read the T&C.[148]

Approaches to increase the effectiveness of digital disclosure could include requiring elements such as user-friendly sequencing and specific screens and pauses to assist consumers in absorbing important information. Research by the European Commission indicates that adding intermediate steps that customers must pass through, such a "review screen" in the purchasing process, has been shown to result in consumers making more optimal loan choices.[149] In Paraguay, lenders utilizing digital channels must provide consumers with a final option of rejecting or accepting the T&C prior to the conclusion of the loan contract and disbursement.[150] For sales of retail banking products and services through digital channels, financial institutions in Portugal are required both to ensure that the selling process proceeds to the next stage only after customers have confirmed that they have read to the end of mandatory information documents, and to use visual and textual techniques to encourage customers to do so.[151]

Requirements could be used to ensure that user interfaces are clear, user-friendly, and easy to navigate. ASIC guidance notes that digital disclosure should be easily navigable, providing a practical example of a menu feature in an app that allows consumers to go immediately to sections of the disclosure that are most important to them.[152] Rules should seek to ensure the same standards in quality of disclosure across different types of mobile phones and platforms.

The risk of unbalanced or misleading marketing and promotional information

Marketing and promotional information for fintech products may be unbalanced or, in more extreme cases, outright misleading. Unbalanced or misleading marketing is a longstanding core concern for regulators in any financial product context, but factors such as the novelty of fintech offerings for consumers, the impetus for providers to grow market share quickly, and their entry in new and less sophisticated markets, may increase the occurrence or exacerbate the impact of these practices. A European Commission study on the digitalization of marketing and distance selling of retail financial services highlighted several poor practices, including emphasizing benefits while giving lower prominence to costs; key information that is missing or difficult to find, such as risks or costs; and presenting unrealistic offers (such as loans that are almost or completely free of charge) while failing to mention the conditions attached to such offers.[153] P2PL platform operators in China were observed to focus on aspects such as average returns if they appear attractive, without highlighting associated risks sufficiently.[154] Adverse marketing practices observed in crowdfunding include promoting past performance without warning that it is not an indicator of likely future performance;[155] highlighting benefits without equally highlighting potential risks; selectively choosing information to create unrealistically an optimistic impression of the investment; and watering down important information by comforting statements based on past records. The FCA has also expressed concerns about misleading advertisements by e-money issuers and other payment services providers that allege that their services are "free"[156] even though fees are charged by intermediary service providers, and about non-bank providers that advertise themselves as offering "bank" accounts or imply that they are a bank.

Marketing practices adopting particularly aggressive approaches or exploiting behavioral biases can be particularly problematic in a digital context. Some digital microcredit providers have been identified as aggressively marketing credit to consumers, such as via push marketing and unsolicited, preapproved offers. Aggressive marketing techniques include push SMS (that is, unsolicited text messages) with credit offers often sent to customers of MNOs or e-money services. Such practices exploit behavioral biases, such as present bias and loss aversion, and lead consumers to make impulsive decisions to take out loans without a clear purpose or to take out larger loans than necessary. Certain digital microcredit providers utilize digital channels to target marketing at times when consumers are vulnerable to making poor decisions, such as weekend evenings.

Marketing techniques that exploit behavioral biases to entice consumers can be particularly impactful. Examples include marketing that encourages consumers to borrow the maximum amount possible, suggests that loans can be repaid easily, or trivializes the seriousness of a loan. Providers may market loans by focusing only on the maximum amount that can be borrowed. A study in Latvia found that digital lenders encouraged consumers to disclose a higher income in order to obtain a larger loan.[157] Aggressive advertising via "cute messaging" was noted by FinCoNet as undermining the seriousness of entering into a credit contract and distracting consumers from the high costs of loan.[158]

The remote nature of digital channels and the rapid speed of digital transactions increase the vulnerability of consumers to aggressive marketing practices. The lack of human interaction with provider staff, combined with the fact that consumers may be transacting from the comfort of their own homes, may result in consumers taking digital loans less seriously. In addition, digital microcredit can be advertised as "one-click" or nearly automatic. These factors may lead consumers to making hasty and poor decisions.

Regulatory approaches for unbalanced or misleading marketing and promotional information

Policy makers continue to use warnings as a key mitigant, and some are shifting to more targeted warnings delivered at crucial moments in providers' interactions with consumers. Nudges such as warnings to consumers regarding the risks of credit have been found to help improve decision-making.[159] Short-term credit providers in Armenia must add legislated warnings to their disclosure material, warning customers about the high cost of the credit and encouraging them to shop around and assess their ability to repay. In the United Kingdom, high-cost, short-term credit must include a prominent risk warning and redirect consumers to resources from the authority in charge of debt advice.[160] Similarly, obliging P2PL platform operators to provide certain warnings or disclaimers in key contexts is being used to assist in balancing out inappropriately optimistic perceptions by consumers. Platform operators in the United Kingdom are subject to rules that require providing a prominent warning that past performance is not a reliable indicator of future results,[161] while Brazilian authorities require that operators display on their website and in other electronic channels, as well as in promotional materials, a prominent warning that P2P loans constitute risky investments and are not subject to deposit insurance.[162]

In some jurisdictions, warnings are also coupled with acknowledgments from lenders/investors. The RBI requires P2PL platform operators to obtain explicit confirmation from a prospective lender/investor that they understand the risks associated with the proposed transaction, that there is no guarantee of return, and that there exists a likelihood of loss of the entire principal in case of default by a borrower.[163] As noted previously, it would be important to ensure that any such warnings or acknowledgments are not seen by regulators or fintech entities (or, importantly, misunderstood by consumers) as reducing the onus on entities to comply with their obligations and address relevant risks where appropriate.

In some instances, established rules requiring marketing information to be balanced are being augmented by fair advertising requirements specific to fintech-related risks. Regulators often request issuers and crowdfunding platform operators, as well as promoters, to ensure that advertisements are not misleading or deceptive by overstating or giving unbalanced emphasis to potential benefits, creating unrealistic expectations, or not clearly or prominently disclosing information about the risks facing the issuer's business or adverse information about the issuer. For example, P2PL operators in the United Kingdom are restricted from making inappropriate comparisons, such as making direct comparisons between investing money in P2PL and holding money on deposit.[164] The Financial Markets Authority of New Zealand issued guidance on the application of general fair dealing requirements to crowdfunding and P2PL products, focusing on balancing representations about risk and reward and providing performance information appropriately.[165]

Policy makers have sometimes decided that it is necessary to explicitly ban certain marketing practices. In Belgium, advertising that focuses on the ease of obtaining credit is prohibited.[166] In the United Kingdom, payday lenders are specifically required to refrain from advertising that trivializes the nature of payday loans, including by encouraging nonessential or frivolous spending or unacceptably distorting the serious nature of such loan products.[167] Rules in the European Union generally restrict the marketing of services that consumers have not solicited.[168] In Portugal, financial institutions should refrain from using pre-ticked boxes or graphic elements to lead customers to choose certain options when conducting sales of retail banking products via digital channels, and they should also refrain from using terms such as "preapproval" or "pre-acceptance" during the sales process, as such terms give the impression that credit is easy to obtain.[169]

Regulators have also been implementing rules to address potentially misleading or incomplete information shared between parties through platforms. Regulators have begun to take steps to regulate crowdfunding

platforms that support secondary markets or exchange of information about securities (bulletin boards), such as by requiring posters to disclose clearly if they are affiliated in any way with the issuer and by mandating that platform operators take reasonable steps to monitor and prevent posts on bulletin boards that are potentially misleading or fraudulent.[170]

Cooling-off periods within which investors can withdraw from investments without consequences are an additional consumer protection measure often applied by regulators. In the United States, crowdfunding regulations permit investors to withdraw up to 48 hours prior to the deadline specified in the issuer's offering materials.[171] In Italy, the applicable cooling-off period starts on the day when the investor subscribes to the offer and lasts seven days after that investment decision. In Australia, a cooling-off period also starts on the day when the investor makes an application (subscribes to the offer) and lasts up to five days after making the application. In Dubai, retail investors may withdraw during a 48-hour cooling-off period that starts at the end of the commitment period.[172]

f) Product is unsuitable for a consumer

The risk of unsuitability due to consumer lack of sophistication or inexperience

Fintech can result in consumers having increased access to novel and complex financial products, such as through P2PL and investment-based crowdfunding platforms, that they may lack the knowledge and experience to assess properly. Even if consumers are provided with all feasible and appropriate information about the risks and other key features of a particular fintech product, lower financial capability or sophistication can nevertheless expose them to losses or other harms. This situation can be exacerbated when a fintech offering entails more complex or riskier aspects than traditional financial products that consumers may be familiar with. It may also be the case that a platform operator does not have sufficient information or understanding about a consumer's lack of skills or sophistication. This may be due to a lack of effort or availability of data.

Investment-based crowdfunding and P2PL platforms have enabled more individuals to act as investors and lenders to small enterprises and to other consumers. While a positive outcome for the purposes of increasing access to finance, these products can expose retail investors to risks of loss with which they may not be familiar when contrasted with more traditional investments they have dealt in previously. The assessment of investment and lending opportunities in the context of crowdfunding and P2PL can require a level of analysis and understanding of potential investees and borrowers that retail investors may not be able to achieve.

Investor inexperience can also exacerbate other investing-related risks, such as excessive overall financial exposure (investing/lending too much of one individual's net worth) or impacts from lack of control over the ultimate investment. Regulators have expressed concern with the risk that P2PL may expose investors to excessive losses having regard to their financial and other personal circumstances. The UK regulator noted recently that, while losses and defaults in their P2PL sector had been low, it was important to recognize that the sector both was relatively new and had not been through a full economic cycle. When economic conditions tightened, losses on loans could increase.[173] Due to the highly dispersed nature of crowdfunding investments relative to the concentrated holdings of business owners and larger investors, the separation between the crowd and control over the management of investees is often high. This can create agency-related risks (and even moral hazard issues) to the detriment of the crowd, which may lack the skills and experience to protect their investor rights.

An oft-quoted benefit of digital microcredit, expanding access to credit to millions of low-income consumers, at the same time can heighten the risk of poor borrowing behavior and related negative consequences for consumers with limited prior experience with credit. Additional factors already discussed above, such as aggressive marketing, unsolicited offers for digital microcredit, and poor transparency regarding pricing, can further cause inexperienced consumers to take up credit without considering the consequences effectively. For example, in some countries, a growing number of consumers are developing negative credit histories due to digital microcredit.[174]

Regulatory approaches to risk of unsuitability due to consumer lack of sophistication or inexperience

Limits on consumers' exposures

In order to limit potential harm to retail investors from exposure to investments offered through P2PL and investment-based crowdfunding platforms, regulators are setting limits on individual investments. These lending/investing caps are being implemented on a variety of bases, ranging from overall caps to limitations on specific exposures. In Dubai, for example, an investment-based crowdfunding operator must ensure that a retail client does not invest more than $50,000 in total in any calendar year using its platform.[175] In contrast, Australia has set an investment cap of A$10,000 per annum per company without an aggregate investment cap. In India, the RBI has imposed both a cap on the total P2PL loans that a lender/investor may make of ₹1 million as well as a cap of ₹50,000 on a

lender/investor's exposure to any individual borrower.[176] The implementation of monetary caps on P2PL appears to be widespread in the European Union.[177] For example, in France, caps for individual lenders/investors of €2,000 per loan if interest-paying or €5,000 if interest-free apply, while Spain has prescribed limits on a per-loan and total-annual basis (of €3,000 and €10,000, respectively) for nonaccredited investors. Some limitations are being set by reference to an investor's specific circumstances. The UK rules on direct financial promotions[178] allow P2PL and investment-based crowdfunding platforms to communicate financial promotions directly only to retail investors that confirm that they will not invest more than 10 percent of their net investable assets unless receiving regulated financial advice.[179]

Some jurisdictions impose caps on the amount that an individual borrower may borrow through P2PL platforms or limit how much money a company can raise on a crowdfunding platform. In Australia, eligible companies are able to make offers of ordinary shares to raise up to A$5 million through crowdfunding in any 12-month period.[180] In Malaysia, an issuer may raise, collectively, a maximum amount of RM 10 million through equity crowdfunding in its lifetime.[181] P2PL rules in China impose a general obligation on platform operators to set limits on individual borrowers' total loan balances with individual platforms and across platforms. Limits of ¥ 1 million and ¥ 5 million have been set for total loan balances of a natural person or a legal person, respectively, across multiple platforms.[182] In India the RBI has imposed a cap on the aggregate P2P loans taken out by a borrower at any point in time of ₹1 million.[183]

Warnings and disclosures

Disclosure and transparency measures are obviously important in assisting to mitigate against additional risks faced by inexperienced or unsophisticated consumers, although such measures are unlikely to be a complete or even the main solution. For example, some regulators require platform operators to warn potential investors about risks affecting P2PL or investment-based crowdfunding offerings. These requirements are sometimes introduced specifically for fintech offerings and sometimes applied by extending existing requirements. Platforms in the United Kingdom have a general obligation to warn clients about the risks associated with investments in financial instruments that now apply to platforms.[184] In Dubai, information that must be displayed on platform websites includes warnings about the main risks of using crowdfunding platforms and consequences of risks, such as if there are defaults.[185]

Some regulators require platforms to obtain some level of confirmation regarding consumer understanding. In the United States, crowdfunding platform operators (funding portals)[186] must seek a demonstration from investors that they understand the risks of crowdfunded investing. In some jurisdictions, the focus is on assessing the appropriateness of a product for a client, where level of understanding may be one of the elements requiring consideration. This approach is discussed below in the context of suitability assessments.

The risk of unsuitability due to inadequate assessment or product design

Fintech credit products offered with limited or no assessments of a consumer's circumstances, or without adequate consideration of the target market for a product, may result in product offers that are unaffordable or not suitable for particular consumers. This risk already exists in the context of more traditional products but can be exacerbated by new factors in a fintech context. For example, digital microcredit providers may initially utilize blind "lend-to-learn" models that fail to consider repayment capacity sufficiently, or P2PL loans may be offered by platform operators whose business model causes them to be less concerned with assessing credit quality. As a result, borrowers may become over-indebted and consumers acting as lenders/investors may suffer losses. In the case of P2PL, lenders/investors may be heavily reliant on assessments by the platform to ensure that loans fit within parameters they are comfortable with,[187] lacking the ability to assess this for themselves. Investments may similarly be offered through crowdfunding or P2PL platforms that are inappropriate for certain retail investors. If an operator lacks the onus to assess a consumer's risk appetite, experience, and financial circumstances, investments offered through crowdfunding or P2PL platforms may be inappropriate for certain retail investors.

Regulatory approaches to risk of unsuitability due to inadequate assessment or product design

Affordability assessment

Many countries already have in place general obligations to obtain and verify information about a consumer's financial circumstances for consumer credit and, in some instances, specifically for short-term, high-cost credit. Different approaches have been taken to impose such obligations, from principle-based to more prescriptive.[188] In South Africa, providers are prohibited from "reckless lending" and from entering into a credit agreement without first taking reasonable steps to assess a consumer's financial circumstances. A credit agreement is considered reckless if the provider did not conduct such an assessment, if the consumer did not understand the risks and obligations of the credit agreement, or if entering into the credit agreement would make the consumer over-indebted.[189] Some countries employ more prescriptive measures

to gauge affordability. In Japan, moneylenders (including fintech lenders) are prohibited from lending where the total amount of borrowing exceeds one-third of a consumer's annual income.[190] Such regulatory approaches also help to address risks related to conflicts of interest raised below with respect to digital credit providers.

For P2PL, it is crucial that obligations apply to the entity in the best practical position to undertake such assessments, which is usually the P2PL platform operator, rather than the individual consumer. For example, in the United Kingdom, the FCA introduced rules that require a platform operator to undertake creditworthiness assessments equivalent to those that would need to be undertaken by a traditional licensed lender.[191] The rules set out detailed requirements for the information that should be obtained and verified about the borrower's income, expenditure, and other circumstances by the platform operator for the purposes of such an assessment, and how the assessment should be made.[192] India's RBI has similarly imposed obligations on platform operators to undertake credit assessment and risk profiling of borrowers and to disclose the results of these to prospective lenders/investors.[193]

Product suitability

Requirements to assess the appropriateness of products are being applied in a range of fintech contexts. In the case of investment-based crowdfunding, such requirements frequently include collecting information from prospective investors to establish their understanding of the risks involved with an intended transaction and whether the selected project is suitable for their profile. New EU regulation on crowdfunding requires that platform operators run an entry knowledge test on their prospective investors and that such prospective investors simulate their ability to bear loss.[194] In the United Kingdom, when a retail client is not receiving investment advice, a platform must undertake an appropriateness assessment before the client can invest. The operator is required to determine whether the client has the necessary experience and knowledge in order to understand the risks involved in relation to the opportunity being offered.[195] The FCA has included guidance with its new rules suggesting a range of multiple-choice questions that avoid binary (yes/no) answers that operators should consider asking prospective P2PL investors. Questions address matters such as the client's exposure to the credit risk of the borrower, the potential loss of capital, and that investing in P2PL is not comparable to depositing money in a savings.[196]

Product design and distribution

While product suitability requirements focus on interactions with individual consumers, emerging regulatory approaches on product design and distribution can help ensure appropriate design of fintech products and reduce risks to consumers before such products even enter the market. A recent World Bank publication discusses the increased emphasis by authorities on legal requirements that govern how retail financial products should be designed and distributed so they are appropriate for their target market, supported by product intervention powers granted to regulators.[197] Australia, the European Union, Hong Kong, South Africa, and the United Kingdom, for example, all have such frameworks or are developing them.

The main focus of such regimes is on requiring FSPs to put in place product oversight and governance arrangements designed to ensure that financial products meet the needs of consumers in target markets. Common elements of such regimes include the following:

- Governance standards: Requiring FSPs to establish and implement clear, documented product oversight and governance arrangements overseen by senior management.
- Target market assessments: Requiring FSPs to undertake an assessment of the target market for which the product is being developed. There may also be a need for product testing before the product is launched.
- Distribution arrangements: Requiring FSPs to ensure distribution channels are appropriate for consumers in the target market for a product.
- Post-sale product reviews: Periodically following product launch, requiring FSPs to review a product and related disclosure materials.

Such regimes may include or be complemented by product intervention powers. These allow regulators to impose restrictions on the marketing, distribution, or sale of specified products and can be used where there is evidence that a financial product has resulted or will likely result in significant detriment to retail clients that cannot be remedied in any other way.

Such regimes are starting to be applied to digital credit products. For example, the EBA specifically highlights that it would be good practice for providers to give further attention to "the risks that consumers might face due to the increasing use of digital channels by FIs [financial institutions] (e.g. exposing consumers to market practices that exacerbate behavioral biases) when improving their POG [product oversight and governance] processes."[198] Digital microcredit lenders in Ghana are required to present and demonstrate their product, the identified risks, and risk-mitigation strategies to a panel at the Bank of Ghana for assessment and approval before

launching the product.[199] Potential measures to address risks include requiring providers to place greater focus on customer segmentation[200] and to target and sell only those digital microcredit products that are suitable and appropriate for the interests, objectives, and characteristics of target segments.[201]

g) Conflicts of interest and conflicted business models

Risks to consumers

Certain characteristics of fintech arrangements can be conducive to conflicts between the interests of consumers and those of providers that may have significant adverse impacts on consumers. Such conflicts often arise in traditional financial product and service settings, but new or changed fintech business models may give rise to conflicts under new circumstances not foreseen by regulators (or expected by consumers), as well as producing new variations of typical conflicts.

Fee-revenue models underpinning some fintech businesses can give rise to perverse incentives for fintech entities to act in ways inconsistent with the interests of their consumers. Some P2PL platforms earn origination fees by facilitating new loans, while consumer investors bear the loss if those loans are made imprudently.[202] Some P2PL platform operators also receive additional revenue streams from charging debt collection fees to pursue delinquent loans on behalf of such investors. Such arrangements can give rise to a conflict between investors' interests in ensuring adequate credit assessments of all loans and an operator's potential interest in loosening such standards to enable more borrowers to qualify for loans that generate additional fees and market share.[203] The resulting conflict can also have an adverse impact on borrowers if they are approved for unaffordable loans. This can also be the case in digital microcredit business models where a digital lender's profitability is heavily dependent on generating up-front facilitation fees (which may be significant relative to the size of digital loans) or other fees that are not necessarily affected by loan quality, and less on interest income from repayments. A lender may accept high loss rates as a cost of doing business, focusing on growing loan volumes—facilitated by high-speed, low-contact digital loan distribution—rather than loan quality.

Such potentially harmful conflicts are frequently the result of a business model in which the fintech entity is empowered to make key decisions affecting risk of loss where resulting loss is borne by consumers. For example, the financial benefits that an investment-based crowdfunding platform operator derives from publicizing crowdfunding offers and ensuring their success may incentivize them to behave in ways contrary to the interests of prospective investors. The platform operator may not perform due diligence on prospective offers to a required standard, as this may result in having to decline hosting that offer, or the operator may be reluctant to assist investors in exercising cooling-off rights to cancel their investment, affecting the success of an offer. As another example, in some P2PL models where a consumer invests in a portfolio of loans rather than individual loans, the platform operator may have the right to change from time to time the loans that make up that portfolio. A lack of alignment between the operator's ability to make such changes and the investor's interests may mean that the operator does not exercise such rights in ways that always ensure that an investor's interests are protected. The operator may not properly take into account the up-to-date value of the loans being reassigned, to ensure that the investor is not exposed to greater risk or loss, in order to avoid operational cost or effort or to transfer changed risk to the investor, such as when facilitating the transfer of pre-funded loans initially arranged by the operator or related party or choosing to favor some investors over others in such transfers.[204]

Business models heavily dependent on generating certain fees, often volume-based, may also incentivize fintech entities to encourage consumers to engage in detrimental behavior. Digital lenders in a range of jurisdictions have been found to encourage consumers to continue rolling over the loans or to take up multiple loans. Even if a digital lender may be exposed to the risk of loan defaults, they may opt to focus on loan quantity rather than quality to maximize fee-related returns. While such practices have always been present in the financial sector, these practices are highly enabled by the digital nature of fintech, which allows providers to reach exponentially more customers at much lower costs. Providers may also be incentivized to offer refinancing to consumers struggling to repay a loan through a new loan that a borrower may perceive as staving off default but in fact causes them to incur additional fees and ultimately an even greater debt. Paying sales-based commissions to agents of e-money issuers may encourage them to recommend one provider over another regardless of whether the product is suitable for the consumer.

Remuneration structures for fintech entities' staff and agents may encourage them to engage in behavior inconsistent with the interests of the consumers they deal with. Such remuneration is variously referred to as "conflicted remuneration" or "perverse incentives." In the context of e-money arrangements, for example, sales-based commissions may encourage agents not to act in the best interests of consumers when recommending an e-money provider or product. An agent may recommend

one provider over another primarily because of the higher commissions involved, regardless of whether the product is suitable for the consumer's financial needs, objectives, or capacity.

Business models that allow fintech entities or affiliated parties to compete with consumers may give those entities unfair advantages, such as insider knowledge, and incentivize conduct that prejudices the interests of consumers. On an investment-based crowdfunding platform, for example, the operator or their affiliates may invest in offers hosted on the platform, or they may hold an interest in entities making offers through the platform or in investors taking up that offer. The way that the operator assesses such offers or represents them to prospective third-party investors may all be affected by such underlying interests.[205] A P2PL platform may similarly allow the platform operator or their affiliates, as well as the public, to invest in loans offered through the platform. The operator or affiliate may then enjoy advantages over ordinary investors. Such advantages may include, for example, better or prior access to loan selection or access to information, not available to other investors, about prospective borrowers and how they have been assessed. This may allow the operator or affiliate, for example, to relegate investors to choosing from lesser-quality loans.[206]

Regulatory approaches

General conflict mitigation obligations

A key mitigant against potential consumer harm from conflicts are obligations on fintech entities to manage and mitigate such conflicts that arise from their activities. This well-established mitigant places an onus on providers to identify and implement practical measures to address conflicts. Typical obligations of this kind would require fintech entities to implement adequate policies and procedures and effective organizational and administrative arrangements designed to prevent conflicts of interest from harming the interests of the consumers that they deal with. Such obligations encompass expectations that fintech entities take appropriate steps to identify and manage, or prevent, conflicts of interest within their business, such as conflicts between the interests of their management, staff, or agents and those of consumers, and even conflicts that their business model and platform arrangements may create between different clients. For example, crowdfunding platform operators in Dubai are required to take reasonable steps to ensure that conflicts, and potential conflicts, between themselves and clients as well as between clients are identified and prevented or managed in such a way that the interests of a client are not harmed, and all clients are treated fairly and not prejudiced by any such conflicts. If an operator is unable to prevent or manage a conflict, they must decline to provide relevant services to a client. In Italy, platform operators are similarly obliged to prevent any conflicts of interest that may arise in the management of platforms from having a negative effect on the interests of investors and ensuring equal treatment of recipients of offers who are in identical conditions. They must prepare, implement, and maintain an effective policy on conflicts of interest, defining the procedures to be followed and measures to be taken to prevent or manage such conflicts.[207]

Conflict-management obligations are often part of the general obligations that apply to entities licensed or otherwise authorized to provide financial products or services in a jurisdiction. For example, in Australia a P2PL platform operator—as the holder of an Australian credit licence—would be subject to a general obligation to have in place adequate arrangements to ensure that its borrower consumers are not disadvantaged by any conflict of interest that may arise wholly or partly in relation to credit activities engaged in by them or their staff or agents. They would also be subject to a similar obligation in relation to their consumer investors as the holder of a financial services license covering their investment activities.[208] In the United Kingdom, one of the "Principles for Business" applying to all authorized firms would require fintech entities to manage conflicts of interest fairly, both between themselves and the consumers they deal with, as well as between consumers.[209] However, it would also be important to ensure that such general conflict mitigation obligations cover fintech entities comprehensively, regardless of the basis on which any licensing or authorization framework applies.

Compulsory disclosure of conflicts more generally may go some way toward mitigating their impact on consumers. However, as demonstrated by regulators' development of a range of substantive conflict-management obligations on providers, there is increasing recognition that it is difficult for consumers to be able to avoid or mitigate the impact of conflicts even if they are aware of them. Consumers may also paradoxically place more trust in providers after they reveal conflicts, rather than less.

Conflicted remuneration restrictions and transparency

An important mitigant against conflicts driven by incentives are requirements on fintech entities to have in place policies to ensure that their internal remuneration arrangements do not encourage conflicted behavior. In the context of digital microcredit or P2PL, such obligations could include ensuring that incentives for staff undertaking or overseeing credit assessments (or designing those credit assessments, such as where these are automated) are not based solely on volume and take into account loan quality and overall performance.[210]

Disclosure of remuneration, such as sales-based commissions paid to e-money agents or financial interests

that a crowdfunding platform operator has in an issuer offering securities on their platform, may sometimes assist to mitigate risk of conflicted remuneration. This is particularly the case where consumers would rely on advice or recommendations from provider staff or agents without realizing these may be influenced by incentives. For example, in the United States, crowdfunding platform operators acting as intermediaries must clearly disclose the manner in which they are compensated in connection with offers and sales of securities undertaken through their platform.[211]

Duties to act in consumers' best interests

Duties on fintech entities to act in accordance with the best interests of their consumers can also act as a key mitigant against potential consumer harm from conflicts. If a conflict arises between the entity's interests and those of a consumer, such a duty would require them to adjust their conduct to place the consumer's interests first. In Australia, for example, a P2PL platform operator would be required to act in the best interests of investors when their platform arrangements constitute a managed investment scheme.[212] Sometimes such a duty is framed less onerously but still requires that appropriate regard be paid to consumers' interests. In the United Kingdom, one of the "Principles for Business" to which authorized firms must adhere is to pay due regard to the interests of their customers.[213] These kinds of duties seem to be imposed more commonly in relation to some types of financial products or services, such as investment-related services or financial advice. For example, under a new EU regulation on crowdfunding, platform operators are subject to a duty to act honestly, fairly, and professionally in accordance with the best interests of investors.[214]

Obligations targeting specific conflicted circumstances

Regulatory requirements targeting specific circumstances may sometimes be necessary, in addition to general conflict mitigation obligations, to address conflict root causes or harms effectively. Requirements on digital lenders and P2PL platform operators to undertake a proper creditworthiness assessment, as already discussed above, would assist in addressing lax lending practices that may arise as a result of business models that depend on loan volumes, rather than loan quality, to generate revenue. A need for targeted obligations was similarly identified by the UK regulator to mitigate against the risk of conflicts leading to inappropriate loan pricing by P2PL platform operators with interests that diverge from those of consumers. Such operators are obliged to have a mechanism in place to ensure that the pricing offered to investors accurately reflects the credit risk of the borrower. This was viewed as important both when setting the interest rate (for new loans) and when calculating the present value of a loan (interest and principal) for existing loans being transferred to an investor.[215]

Restrictions may need to be placed on particular aspects of fintech business models that increase significantly the likelihood of or the consumer harm from conflicts, such as arrangements that allow fintech entities or their affiliates to compete with their consumers unfairly. Many regulators have implemented restrictions on a crowdfunding platform operator, and their affiliated parties, investing in issuers whose offers are hosted on their platform, as a way to avoid conflicts of interest that may arise with other investors using the platform. Proposed crowdfunding rules in the European Union would prohibit platform operators from having any financial participation in crowdfunding offers that they host. Affiliates of an operator (such as shareholders holding 20 percent or more of share capital or voting rights, managers and employees, or any persons directly or indirectly controlling the operator) also would not be permitted to invest in such offers. In Dubai, any officer or employee of a crowdfunding platform operator (or their family members) is restricted from investing or issuing via the platform or to have financial interest in any issuer or investor. Some regulators have placed caps on such investments—in Malaysia, operators are permitted to have shareholdings in issuers hosted on their platform of up to 30 percent, accompanied by public disclosures. The United States, on the other hand, allows operators to invest in issuers selling securities through their platform, but only if the financial benefit they derive is compensation for their services and consists of the same class of securities, on the same terms, as those that the public receives. This concession was viewed as helpful in raising the profile of crowdfunding campaigns.[216] In some jurisdictions, restrictions have similarly been placed on P2PL platform operators or their associates investing in loans facilitated by their platforms. For example, regulations in China limit operators to intermediating loans made directly between lenders/individuals and borrowers and prohibit operators from making any loans themselves. Indonesian regulations similarly prohibit operators from acting as lenders or borrowers.[217]

Regulators may also find it necessary to prohibit certain specific financial benefits. For example, in order to ensure that prospective investors on crowdfunding platforms are offered investment opportunities on a neutral basis, new EU rules prohibit platform operators from paying or accepting any remuneration, discount, or non-monetary benefit for routing investors' orders to particular offers.[218]

h) Risks from algorithmic decision-making

Risks to consumers

The use of algorithms for consumer-related decisions is increasing in financial markets overall but is becoming particularly prevalent in highly automated fintech busi-

ness models. [219] In the case of the fintech product examples discussed in this paper, this is particularly relevant to credit scoring decisions for digital microcredit and P2PL. Consumers risks that may arise as a result of algorithmic scoring decisions that lead to unfair, discriminatory, or biased outcomes.

Regulatory approaches

This is a cutting-edge area with limited examples of regulatory approaches that have been implemented to date. However, general principles for algorithmic accountability are emerging around the key principles of fairness, explainability, auditability, responsibility, and accuracy. Emerging regulatory approaches relevant for fintech include applying fair treatment and anti-discrimination obligations to algorithmic processes; rules on safeguards for the development, testing, and deployment of algorithms and for auditability, and transparency for consumers.[220] For example, the EBA guidelines on loan origination and monitoring require that when using automated models for creditworthiness assessment and credit decision-making, financial institutions should have in place internal policies and procedures to detect and prevent bias and ensure the quality of input data.[221] Financial institutions in Portugal are explicitly required to inform bank customers of situations where their creditworthiness assessments rely exclusively on automated decision-making processes, particularly artificial intelligence models, in order to allow customers in such situations to exercise their rights under European Union data protection rules.[222]

i) Data privacy

Data privacy is obviously a crucial consideration in relation to fintech offerings, given their highly data-driven nature. Business models for fintech offerings often revolve around the innovative use of big data[223] and alternative data, whether to target consumers for product offerings, assess product applications, or design products. Alternative data may include, for example, data on airtime, usage of mobile data, usage of mobile money, calling patterns, social media activity and connections, internet usage and browsing history. Such data may be purchased from third parties or obtained from a consumer's phone. While such innovative data sourcing and analysis arrangements can, for example, expand access to finance for consumers in relation to whom limited formal data is available, they also raise new, complex data privacy concerns, such as regarding informed consent and legitimate uses.

This section briefly touches on data privacy issues from a fintech consumer's perspective as an introduction to their relevance to financial consumer risks and interaction with FCP regulation. However, as noted above, it is not intended to be an exhaustive canvassing of privacy risks.[224]

Consumers may lack awareness or understanding regarding how and what data about them is collected or used, not assisted by common approaches to notifications and consent. As already discussed, delivery of information through digital channels, such as through feature phones, and the speed with which fintech products are acquired can make it difficult for consumers to process information adequately, including data privacy-related notifications. Importantly, the complexity of data-sharing relationships underlying business arrangements, and the uses to which such data may be put (such as algorithmic decision-making), can make it inherently more difficult for consumers to understand privacy-related disclosures and their implications. Further, as highlighted in a previous World Bank publication on new forms of data processing, there are practical limitations with consent-based data privacy models that are exacerbated in the digital context and with greater complexity of data and uses.[225] The previous World Bank paper also discusses a range of risks that can arise as a result of new forms of data processing for the provision of financial services that are highly relevant in a fintech context, such as use of data to discriminate inappropriately between consumers and impacts on consumers from inaccurate data or data breaches.

Importantly, individuals may be affected by fintech-related data privacy issues regardless of whether they are ever customers or prospective customers of fintech entities. Personal information may be subject to data mining, purchasing, or analytics regardless of any existing or prospective consumer relationship, such as for product development or marketing research. There is an increasingly wide array of data brokers and data analytics companies (often not regulated under financial sector regulation).

Data privacy risks are not confined to the financial sector, given how data travels through and is exchanged and handled across different sectors. FCP regulation by itself can struggle to address such issues because of sectoral boundaries, hence the whole-of-economy/ jurisdiction approach to data privacy regulation reflected in regimes such the European Union's General Data Protection Regulation (GDPR).[226]

Without seeking to set out a full range of elements to mitigate data privacy risks comprehensively, the following are examples of data privacy regulatory measures emerging internationally and relevant to fintech:[227]

- **Coverage of alternative data:** It is important that definitions of personal data (or equivalents) are sufficiently broad and flexible to cover alternative data and, in particular, that they reflect the increasingly greater ability to identify individuals from data. Data associated with individuals can include, for example, information about internet or other electronic network activity (such as browsing and search histories, stored locally or with providers), geolocation data, and inferences drawn from such information to create a profile about an individual relating to matters such as (as referenced for example in California's recently implemented Consumer Privacy Act[228]) their preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.[229] California's Consumer Privacy Act defines "personal information" as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household", and then provides a non-exhaustive list of examples, including the kinds of data described above.[230]
- **While consent will likely continue to be a key element of data privacy frameworks, there is a clear shift away from bundled, overarching consent and toward models requiring more active, granular, and targeted consent.** For example, the European Union's GDPR notes that separate consent should be obtained for different personal data-processing operations where appropriate.[231]
- **There is also increasing recognition that consent-based approaches to data privacy are useful but likely insufficient.** An emerging approach puts greater focus on personal data being processed for legitimate purposes. The GDPR requires that personal information be collected for explicit, specific, and legitimate purposes and not processed in a way incompatible with such purposes.[232] Some commentators suggest that under some circumstances, policy makers could consider being more prescriptive regarding what qualifies as, and what are the boundaries of, legitimate use. For example, access to contacts and personal data to threaten customers (as opposed to using such data for lending decisions) could be banned.[233]
- **Data minimization and privacy-by-design requirements are becoming increasingly important.** The GDPR requires that personal data be adequate, relevant, and limited to what is necessary in relation to the purpose for which data is being processed and kept for no longer than necessary for the purposes for which the personal data are processed.[234] This is also reflected in other data privacy frameworks, such as in Australia and Canada.[235]
- **Similar to provider liability requirements for the behavior of agents, providers are being given greater responsibility regarding the data practices of third parties that they contract.** In some frameworks, this is more implicit, based on concepts of controls, but it seems likely to be increasingly more overt. For example, a draft data privacy bill proposed in the United States (the Consumer Online Privacy Rights Act) includes provisions that require providers to exercise reasonable due diligence in selecting a service provider and conduct reasonable oversight of its service providers to ensure compliance with data-protection rules on service providers and third parties.[236] The GDPR already focuses on this through, for example, responsibilities placed on data controllers for the actions of data processors.
- **In jurisdictions such as the European Union, individuals are being given a range of additional data-related rights allowing them to exercise greater access to and control over their data.** The GDPR, for example, provides for a right to data portability,[237] enabling individuals to obtain and transfer their personal data between providers for their chosen purposes, and a broad "right to be forgotten"—facilitating individuals' ability to have personal data about them erased and to prevent further processing.[238]

3.2 IMPLEMENTATION CONSIDERATIONS

For any regulator contemplating implementing the kinds of regulatory measures discussed in this paper, it will be important to tailor regulatory approaches to country context and to balance the need for consumer protection with the resulting impact on industry and market development and innovation. This section summarizes a range of key implementation matters for regulators to consider.[239]

a) Importance of country context and striking an appropriate balance

Although this paper identifies a range of potential regulatory measures to address relevant risks, it is not the authors' intent to suggest that all regulatory measures be implemented in all situations. Rather, the objective was to provide authorities with a range of regulatory measures from which to select approaches best suited to their particular circumstances. Some of the regulatory measures discussed in this paper can impose significant compliance costs on industry participants; implementing all regulatory measures could lead to excessive compliance burdens. A proportionate, risk-based approach will be needed. It

is important for any regulator contemplating implementing regulatory measures to strike an appropriate balance between the need for consumer protection and the resulting impact on industry and market development, including potentially harming access to finance. For example, as high-profile incidents of lender/investor losses and other consumer harms have affected P2PL in a number of countries, authorities deemed it necessary to increase obligations and restrictions on participants significantly to mitigate the risk of such harms occurring in the future. Reactions to this have been mixed. Media reporting in the United Kingdom suggests, for example, that platform operators themselves hope significant reforms by the UK regulator will help to restore the sector's damaged reputation by weeding out weaker, less compliant competitors.[240] By contrast, some industry participants in China have expressed concern that major reforms implemented by the Chinese authorities may stifle the sector and cause remaining players to change their business significantly to their detriment.[241]

b) Assessing the market, consumer experiences, and current regulatory framework

Policy makers should first seek to develop a good understanding of their fintech market and the financial sector more broadly in their country. Effective stakeholder consultation, at the consumer as well as industry level, will be essential. Within each fintech category available or entering a country's financial sector, a range of models may be being utilized, with different types of providers, operating models, product features, digital channels, and current and prospective customer bases and target markets. These differences will influence the risks being faced by consumers as well as how they can best be addressed.

A regulator's research to inform its regulatory policy making should include seeking to understand consumers' issues and experiences. This includes focusing on both consumer expectations and experiences in relation to fintech products and financial products more broadly in the context of their needs and circumstances, as well as in relation to potential measures, including but not limited to regulation, that may be able to address risks and concerns that consumers face.

Information for these purposes can be gathered from a variety of sources, including market research; consumer focus groups; meetings with providers, consumer and civil society representatives, experts, and other industry participants; complaints data; and supervisory activities. For example, BdP decided to first better understand the digital credit market in Portugal before issuing any new rules. BdP took a range of practical steps, such as requiring providers to provide information (via a structured questionnaire) on how consumer credit products are being offered through digital channels. BdP also held bilateral meetings with individual providers during which providers demonstrated the contracting flows via online or mobile channels. These were then discussed and suggestions provided by BdP when process revisions seemed necessary. Based on identified best practices as well as behavioral economics, BdP issued a set of recommendations in July 2020 on how institutions should comply with their duties when selling retail banking products and services through digital channels.[242] Countries such as Australia, Ireland, and the United Kingdom have conducted industry reviews of high-cost, short-term lenders as part of market monitoring activities, in some cases leading to the introduction of new rules. More broadly, the FCA, for example, undertakes a periodic "Financial Lives" survey to understand the financial products that consumers have, their experiences engaging with FSPs, and their attitudes about dealing with money and the financial sector.[243]

In their ongoing development of regulatory policy, regulators where feasible should also leverage information obtained from industry engagement through arrangements such as regulatory sandboxes. As discussed in a recent WBG note, for example, the benefits of such arrangements for regulators can include providing an evidence base from which to make policy and help to define, create, or amend regulation.[244]

In parallel, the existing regulatory framework should be assessed for gaps, including in relation to baseline FCP issues, and effectiveness. While this paper discusses new or changed manifestations of consumer risks, as already mentioned, equally important baseline consumer risks and corresponding regulatory measures apply across financial product types. Regulators should consider whether their existing frameworks address these baseline risks effectively, as well as new manifestations of consumer risk resulting from novel aspects of fintech products. This review should include any existing FCP rules, as well as other measures that may act as mitigants. In addition, given the breadth of consumer risks raised by fintech products of the kinds discussed in this paper, the assessment should include review of a broader range of rules, including those with respect to data privacy, credit reporting and scoring, general consumer protection, and digital channels, to determine overlaps and potential inconsistencies with proposed mitigants. Regulators should also seek to understand the effectiveness and impact of existing rules to inform decisions on whether and how to develop new regulation.

c) Determining the right regulatory approach

Based on a deeper understanding of the market and of consumers in their jurisdictions, as well as an assessment of existing regulation, policy makers should devise an appropriate policy strategy and prioritize actions. Different approaches being taken by authorities in this regard are discussed in this paper. It may be the case that it is more appropriate to add targeted rules to existing FCP laws, or it may be necessary to develop stand-alone rules. Policy makers may also determine it to be preferable to address topics selectively or in a staged manner. Experience from other countries to date reveals that policy makers are frequently addressing at least some fintech-related consumer risks using a piecemeal approach, most likely out of necessity. Factors affecting prioritization may include, for example, the need to address risks that are having the most significant immediate impact on individual consumers or consumer populations in a particular market. They may also depend on the stage of development of particular fintech offerings in the market and their accessibility to consumers. Ultimately, the optimal solution will depend highly on country context. A combination of approaches will likely be necessary in order to address the key risks posed to consumers comprehensively, regardless of the approach taken.

A staged approach can be employed, as it is likely that ongoing adjustments will need to be made, given the rapidly evolving nature of fintech innovation as well as the cutting-edge nature of some approaches discussed herein. This is demonstrated by some jurisdictions' policy-development journeys mentioned in the product-specific chapters of this paper.

Regulators should also consider carefully what coordination and cooperation arrangements are needed with national and international authorities to assist regulatory development and implementation and ultimately achieve policy aims. Close coordination between fellow domestic financial sector authorities is likely to be essential, even more so if multiple authorities are responsible for FCP regulation of the financial sector and fintech entities. This is likely to be needed for a range of reasons, including to ensure consistency in approaches, mutual assistance with supervision and enforcement, and effectiveness of complementary initiatives (such as initiatives to foster financial sector innovation and improve financial inclusion and capability). It could also assist with increasing knowledge and capacity within each institution as well as with broader government communication and engagement with industry and consumers. Coordination with authorities having related responsibilities (such as telecommunications regulators) is also likely to be important for similar reasons. Some areas of regulation, such as rules governing the use of algorithms, may also require coordination beyond the financial sector.

Cross-border cooperation between authorities may be necessary given the increasing ease with which foreign fintech entities may engage with consumers in other countries. Such coordination may be needed, for example, to promote consistent policy approaches across borders and to develop cooperative arrangements to ultimately assist with supervision and enforcement. It would also assist more broadly with knowledge sharing, including relating to regional and international market developments. Given the increasingly cross-border nature of FSPs internationally (which is an issue that, of course, goes beyond fintech entities), greater harmonization and, to the extent possible, regional coordination of regulatory efforts could be beneficial. For example, efforts have been undertaken in the East African community to develop a common framework for SIM card registration for the explicit purpose of limiting mobile money fraud.[245] Another possible approach—where relevant—would be to regulate the domestic agents or intermediaries of foreign fintech companies, an approach utilized in the case of remittances.[246]

Regulators should be cautious about imposing unnecessarily prescriptive regulation. A regulator may determine legitimately that certain topics and issues are better addressed through more detailed rules, having regard to relevant consumer impacts and industry practices. However, it can be useful to start from the premise of developing regulation that will be based on principles and more general provisions, including supported by guidance, and to adopt more prescriptive regulation only when necessary. Setting principles for industry allows providers with more flexibility and ideally places less restriction on innovation, but practices will of course need to be appropriately monitored via supervisory activities. Monitoring and testing the effectiveness of approaches (including both positive impacts for consumers and compliance costs for providers) and maintaining communication with industry will be beneficial over the long run in order to determine the right balance.

Regulators should also consider when complementary, non-regulatory measures may be more appropriate as an alternative to, or until, development of regulatory measures. For example, encouraging development of industry standards and codes of conduct may assist in establishing industry familiarity with acceptable practices. It may also assist in addressing consumer risks more quickly, particularly where FCP regulatory capacity is lim-

ited. Of course, this would also depend on the oversight and enforcement mechanisms that support such initiatives.

There is currently debate regarding the appropriateness of establishing differentiated regulation based on the type, size, and complexity of entities' operations. However, it has also been noted that, on a behavioral level, specific products and services may carry similar risks for the consumer, regardless of the type of institution providing them, and thus should be regulated accordingly.[247] Regulators should pay careful attention to the nature and level of risks in their market when determining the correspondingly appropriate level of legal obligations they may decide to impose to address them. It is also the case that regulators are increasingly building proportionality into FCP requirements themselves, rather than seeking to predetermine such proportionality in advance. For example, regimes imposing obligations on FSPs to implement financial product oversight and governance arrangements increasingly provide that these arrangements should be proportionate to the nature, scale, and complexity of the FSP's business and relevant consumer risk and product complexity.[248]

A potential pitfall that countries should seek to avoid when adopting separate frameworks for traditional and fintech activities of a similar nature is different substantive treatment under different sets of FCP rules. This can distort competition and encourage regulatory arbitrage.

d) Effective supervision critical for impact

Effective supervision of any regulatory measures that are implemented, and monitoring of fintech developments and consumer risks more broadly, will be essential for policy aims underlying such measures to be achieved. While a discussion of FCP/market conduct supervisory practices and approaches is outside the scope of this paper, but it is also important to acknowledge that changes in markets, products, and participants fostered by fintech developments equally also present a range of challenges and new issues for supervisors.[249]

Supervisors will need new strategies and new technological tools in order to monitor financial sectors being expanded and changed by fintech entrants and offerings, including as-yet-unregulated providers and changed businesses of some already-regulated entities. New publications by the World Bank and FinCoNet explore developments in relation to market conduct supervisory technology (suptech) tools that could assist supervisors in such contexts.[250] Supervisors will need to analyze information from an expanding range of sources, including consumer-side research, monitoring of social as well as traditional media, activity on digital platforms, and various types of industry-side data.[251]

Supervisors will need adequate resourcing and capacity. For example, some commentators claim that effective implementation of new P2PL regulations in China has been hampered by lack of resourcing for supervising authorities, leading to practical obstacles such as delay of registration approvals and lack of guidance.[252] While this should not be used to avoid the need for adequate resourcing, a realistic assessment of available resources would be one of the factors to be considered when planning eventual implementation of new regulatory measures. Issues can also arise due to lack of clarity regarding regulator responsibility and authority for new types of innovative providers. Such issues may need to be addressed, and heightened coordination may need to be pursued among both financial and non-financial sector authorities as well as on a cross-border basis. It will also be important for supervisors to build internal capacity and expertise, ensuring that they have the increasingly multidisciplinary capabilities needed to understand and deal with fintech-related risks.

e) Complementary non-regulatory measures

A range of complementary measures will be needed to accompany regulatory measures. As indicated at the outset, this paper focuses in particular on regulatory measures to address risks posed by fintech. Regulatory measures are often necessary but are by no means the only measures that will be required. For example, complementary measures will be needed to increase consumers' digital and financial literacy and to increase awareness and understanding among market participants regarding responsible practices.

Awareness building and efforts to improve financial capability for both consumers and industry will also be essential to support the positive impact of regulatory measures, as well as addressing consumer risks more broadly. For example, it will be imperative to ensure as much as possible—through measures such as awareness campaigns and financial capability initiatives and tools—that consumers understand adequately product benefits and risks and their rights and responsibilities. It will similarly be essential to promote fintech entities' awareness and understanding—through measures such as regulator guidance and capacity building and training efforts—of consumer expectations, risks, and issues, as well as of their responsibilities to consumers, again not limited to legal responsibilities that may be specified in regulation but also having regard to fair practices more generally.

NOTES

30 For example, as further discussed in Chapter 5, earlier in the development of the United States' P2PL market, the securities regulator felt compelled to issue a cease-and-desist order against a major P2PL platform in order to signal strongly the applicability of existing securities legislation.
31 Payment Systems (E-Money) Regulations 2019 (Malawi), s. 5.
32 BSP E-Money Circular 2009 (Philippines), s. 3.
33 Financial Technology Institutions Law 2018 (Mexico), art. 11.
34 Payment Systems and Services Act 2019 (Ghana).
35 Financial Services Act 2013 (Malaysia).
36 The People's Bank of China and nine other government bodies jointly introduced a new framework in 2015 by initially issuing "Guiding Opinions on Promoting the Healthy Development of Internet Finance" and supported a range of additional rules such as the Interim Measures for the Administration of the Business Activities of Online Lending Intermediary Institutions 2016 (China).
37 See the SEC's Proposed Rules on Crowdfunding (USA).
38 Financial Technology Institutions Law 2018 (Mexico).
39 Law on Transparency for Financial Services 2007 (Mexico).
40 Mazer, "Does Transparency Matter."
41 See National Consumer Credit Protection Act 2009 (Cth) (Australia), ss. 6 and 29 (requirement to be licensed if undertaking credit activities). The Act also applies a broad range of conduct and disclosure obligations when engaging in credit activities involving consumers.
42 1933 Securities Act 15 USC § 77a.
43 Lo, "If It Ain't Broke," 88–89.
44 Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (SI 2001/544) (UK), art. 36H, and FCA, *FCA's Regulatory Approach*, para 2.8.
45 Regulation of the Financial Services Authority Number 77/POJK.01/2016 Concerning Information Technology-Based Loan Services (Indonesia), Chapter II, Part 4.
46 See, for example, Australia, Corporations Amendment (Crowd-sourced Funding for Proprietary Companies) Act 2018, https://www.legislation.gov.au/Details/C2018A00106.
47 Buku and Mazer, "Fraud in Mobile Financial Services." See also ITU-T Focus Group on Digital Financial Services, *Commonly Identified Consumer Protection Themes*, s. 3.3.
48 See Huang, "Online P2P Lending," 77.
49 Hornby and Zhang, "China's Middle Class."
50 Owens, "Responsible Digital Credit," 8–9.
51 The Australian regime includes certain very specific and technical exemptions not relevant for the purposes of this discussion.
52 EBA, "Opinion of the European Banking Authority," para 70 and 71.
53 Peer-to-Peer Lending Information Intermediaries of Guangdong Province—Detailed Implementation Rules for Recordation and Registration (Exposure Draft issued on February 14, 2017). See also Huang, "Online P2P Lending," 73–74.
54 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 12.
55 Regulation Crowdfunding (USA), Rule 227.400.
56 Corporations Act 2001 (Cth) (Australia), s. 738C.
57 Regulatory Law 2004 (Dubai), art. 42(1), and DFSA Rulebook (Dubai), GEN 2.2.8.
58 SEC's Proposed Rules on Crowdfunding (Nigeria), art. 4 (e).
59 EBA, "Opinion of the European Banking Authority," para 70 and 71.
60 Regulatory Law No. 1 of 2004 (Dubai), art. 42, and DFSA Rulebook (Dubai), GEN 5.3.19, GEN/VER48/04-20.
61 As noted earlier, this paper is not intended to cover prudential concerns and requirements. Of course, it is the case that these overlap with consumer risks and FCP rules. For example, for a discussion of the relevance of capital requirements to operational risks, see World Bank Group, *Prudential Regulatory and Supervisory Practices*, 17–19.
62 FCA Principles for Businesses—October 2020 (UK), 2.1.1R (Principle 3).
63 FCA Senior Management Arrangements, Systems and Controls Sourcebook—October 2020 (UK), 4.1.1R and 7.1.3R.
64 Financial Technology Institutions Law 2018 (Mexico), art. 37.
65 EU Directive 2015/2366 on Payments Services 2015 (EU) (PSD2), art. 96.
66 Licensing and Authorization of Payment Instrument Issuers Directive No. ONPS/01/2020 (Ethiopia), art. 13.(2)1.
67 National Payment System Regulations 2014 (Kenya), s. 29(2)(b) and (c).
68 PSD2, art. 96(1).
69 Payment Systems and Services Act 2019 (Ghana), s. 86(1).
70 Payment Systems and Services Act 2019 (Ghana), s. 20(2)
71 PSD2, art. 73 and 74.
72 PSD2 2015, art. 71(1). Here the relevant period is 13 months, but this should not be considered the norm.
73 PSD2, art. 51, 69, and 70.
74 PSD2, art. 72(1).
75 Regulation Crowdfunding (USA), Rule 227.301.
76 FCA Consultation Paper 18/20 (UK), 4.21 and 4.22.

77 Corporations Act 2001 Pt 6D.3.A—Crowd Sourced Funding, s. 738Q(5).
78 DFSA Rulebook (Dubai), COB 11.3.6.
79 Guidelines on Recognized Markets SC-GL/6-2015(R3-2019), Rule 13.05.
80 Committee on Global Financial System and Financial Stability Board Working Group, *FinTech Credit*, 26.
81 See, for example, Kyamutetera, "Hackers Break Into Mobile Money System." See also Stanbic Bank Uganda, MTN Uganda, and Airtel Uganda, "System Incident Impacting Bank."
82 Regulation of the Financial Services Authority Number 77/POJK.01/2016 Concerning Information Technology-Based Loan Services (Indonesia), art. 25; Financial Services Authority Circular Number 18/SEOJK.02/2017 Regarding Information Technology Risk Management and Management in Information Technology-Based Lending (Indonesia).
83 PSD2, art. 95.
84 BNM Guideline on E-Money 2016 (Malaysia), ss. 8.2–8.5.
85 Payment Systems and Services Act 2019 (Ghana), s. 45(1).
86 See, for example, ASIC, *Survey of Marketplace Lending Providers: 2016–2017*, para 21.
87 RBI NBFC—Peer to Peer Lending Platform Directions 2017 (India), para 17 and annex VI.
88 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 9(3).
89 PSD2, arts. 83–87.
90 Payment Systems and Services Act 2019 (Ghana) s. 45(2).
91 FCA, *FCA's Regulatory Approach to Crowdfunding (and Similar Activities)*, para 3.19.
92 EBA, "Opinion of the European Banking Authority," para D3 and 43.
93 EBA, "Opinion of the European Banking Authority," para 79–80.
94 RBI NBFC—Peer to Peer Lending Platform Directions 2017 (India), para 9(1).
95 Regulation of the Financial Services Authority Number 77/POJK.01/2016 Concerning Information Technology-Based Loan Services (Indonesia), art. 24.
96 FCA, *FCA's Regulatory Approach to Crowdfunding (and Similar Activities)*, para 3.34–3.36. Also, see FCA Client Assets Sourcebook—October 2020 (UK), 7, and FCA Senior Management Arrangements, Systems and Controls Sourcebook—October 2020 (UK) 4.1.8ER.
97 For a discussion of fund-segregation requirements, see also World Bank Group, *Prudential Regulatory and Supervisory Practices*, 19.
98 Payment Systems (E-Money) Regulations 2019 (Malawi), Part IV.
99 National Payment System Regulations 2014 (Kenya), s. 25(3) and Fourth Schedule.
100 Payment Systems and Services Act 2019 (Ghana), s. 46.
101 See https://www.federalregister.gov/documents/2016/11/22/2016-24503/prepaid-accounts-under-the-electronic-fund-transfer-act-regulation-e-and-the-truth-in-lending-act#footnote-150%E2%80%89151-p83947.
102 Havrylchyk, *Regulatory Framework*, 26.
103 EBA, "Opinion of the European Banking Authority," para 69.
104 PSD2, art. 5 (1)(h).
105 BNM Guideline on Electronic Money (Malaysia), ss. 7.2 and 8.4.
106 Thirty-one percent of respondents selected limited disclosure of costs as the main market conduct and consumer protection issue, followed by high costs of digital microcredit (14 percent), limited suitability and misleading advertising (14 percent), and data security and privacy (12 percent). See AFI, "Digitally Delivered Credit: Policy Guidance Paper."
107 Kaffenberger and Totolo, *Digital Credit Revolution*.
108 FCA's General Standards and Communication Rules for the Payment Services and E-money Sectors in Policy Statement PS 19/3 2019 (UK), para 3.18 to 3.24.
109 For example, see Lenz, "Peer-to-Peer Lending," 695.
110 Truth in Lending Act 1968 15 USC § 1601 (USA).
111 Truth in Lending (Regulation Z) 12 CFR Part 1026 (USA).
112 National Payment System Regulations 2014 (Kenya), s. 35(1).
113 Busara Center for Behavioral Economics, *Pricing Transparency*.
114 Examples of such requirements can be found in Kenya, Malawi, and Malaysia. See National Payment System Regulations 2014 (Kenya), s. 35(1)(a); Payment Systems (E-Money) Regulations 2019 (Malawi), s. 21(3)(e); and BNM Guideline on Electronic Money 2016 (Malaysia), s. 9.3 (i).
115 For example, the EU Payment Services Directive 2015 (PSD2) requires that all charges be disclosed to the consumer before the contract is entered into and before a transaction is initiated.
116 National Monetary Council Resolution Number 4,656 of April 26, 2018 (Brazil).
117 National Payment System Regulations 2014 (Kenya), ss. 41(1)(a) and (2).
118 BSP E-Money Circular 2009 (Philippines), s. 4(G).
119 BdP Circular Letter No. CC/2020/00000044 on best practices applicable to the selling of retail banking products and services through digital channels.
120 ASIC's guidance on good practices for digital disclosure discusses the importance of clients being able to keep a copy of disclosed information so that they can access the information in the future. This can include the ability to save either a digital copy or a hyperlink to disclosed information on a website that continues to be accessible for a reasonable period of time. See ASIC, *Facilitating Digital Financial Services Disclosures*.
121 For example, Kenya's National Payment System Regulations 2014 require publication of terms and fees (rates) and display at "all points of service," s. 35, and BNM Guideline on Electronic Money 2016 requires that terms and conditions must be available through various channels, including on the issuer's website, in brochures, and on registration forms, s. 9.3.

122 Banking Regulatory Commission Guide to the Disclosure of Information on Business Activities of Peer-to-Peer Lending Information Intermediaries 2016 (China).
123 National Monetary Council Resolution Number 4,656 of April 26, 2018 (Brazil).
124 FCA Conduct of Business Sourcebook—October 2020 (UK), 4.6; FCA, *FCA's Regulatory Approach to Crowdfunding (and Similar Activities)*, para 3.72.
125 National Monetary Council Resolution Number 4,656 of April 26, 2018 (Brazil), art. 17.
126 RBI NBFC—Peer to Peer Lending Platform Directions 2017 (India), para 12(2).
127 For example, on a monthly or quarterly basis (depending on loan term), P2PL operators in China must provide to lenders/investors prescribed ongoing information in relation to their individual loans, including changes to the borrower's financial circumstances and repayment ability, any overdue repayments, and additional charges imposed on the borrower and other matters may affect their position. See Banking Regulatory Commission Guide to the Disclosure of Information on Business Activities of Peer-to-Peer Lending Information Intermediaries 2016 (China), art. 9 and Attachment—Explanation on the Content of the Disclosure of Information. In the United Kingdom, operators must ensure that, at any point in time, a lender/investor is able to access a range of details of each of their loans, such as pricing, the borrower's interest rate, a fair description of the likely actual return, taking into account fees, default rates, and taxation, and so on. See FCA Conduct of Business Sourcebook—October 2020 (UK), 18.12.31R.
128 Banking Regulatory Commission Guide to the Disclosure of Information on Business Activities of Peer-to-Peer Lending Information Intermediaries 2016 (China), art. 10.
129 For example, Kenya has requirements for the payment service provider "without undue delay" to provide the payer with a unique transaction reference and detail of the amount, payee and their account, and the debit. See National Payment System Regulations 2014 (Kenya), s. 35(3).
130 For example, in Ethiopia, at least the last 10 transactions must be available for viewing online. See Licensing and Authorization of Payment Instrument Issuers Directive No. ONPS/01/2020 (Ethiopia), art. 12(2).
131 For example, the Payment Systems and Services Act 2019 (Ghana) requires seven days' notice of changes to fees and charges, which must be made through SMS or any other method approved by the Bank of Ghana, s. 45(9).
132 ITU-T Focus Group on Digital Financial Services, *Main Recommendations*.
133 See National Payment System Regulations 2014 (Kenya), s. 35(1); Payment Systems and Services Act 2019 (Ghana), s. 44(a).
134 https://www.fca.org.uk/publications/discussion-papers/smarter-consumer-communications-further-step-journey.
135 BdP Circular Letter No. CC/2020/00000044 on best practices applicable to the selling of retail banking products and services through digital channels.
136 Busara Center for Behavioral Economics, *Pricing Transparency*.
137 FCA, *Feedback Statement FS16/10*.
138 National Monetary Council Resolution Number 4,656 of April 26, 2018 (Brazil), art. 17.
139 Banking Regulatory Commission Guide to the Disclosure of Information on Business Activities of Peer-to-Peer Lending Information Intermediaries 2016 (China), art. 3.
140 BdP Circular Letter No. CC/2020/00000044 on best practices applicable to the selling of retail banking products and services through digital channels.
141 BdP Circular Letter No. CC/2020/00000044 on best practices applicable to the selling of retail banking products and services through digital channels.
142 Payment Systems and Services Act 2019 (Ghana), s. 45(5).
143 FCA, *Feedback Statement FS16/10*.
144 ASIC, *Facilitating Digital Financial Services Disclosures*.
145 Based on World Bank conversation with Competition Authority of Kenya. The guidelines apply to financial services conducted through SIM cards, USSD, and apps.
146 Mazer, "Does Transparency Matter."
147 Mazer, Vancel, and Keyman, "Finding 'Win-Win.'"
148 Mazer, Vancel, and Keyman, "Finding 'Win-Win.'" Subsequent to this study, the digital microcredit provider in the study integrated research insights into its new USSD menus, including (1) separating finance charges from principal, (2) adding a line showing loan fees as a percentage, (3) adding a separate screen with late payment penalties, and (4) creating active choice to view terms and conditions.
149 EC, *Behavioral Study on Digitalisation*.
150 Circular SB. SG. No. 00065/2015.
151 BdP Circular Letter No. CC/2020/00000044 on best practices applicable to the selling of retail banking products and services through digital channels.
152 ASIC, *Facilitating Digital Financial Services Disclosures*.
153 EC, *Behavioral Study on Digitalisation*.
154 Duoguang, "Growing with Pain," 49.
155 FCA, *FCA's Regulatory Approach to Crowdfunding over Internet*, para 3.75.
156 FCA's General Standards and Communication Rules for the Payment Services and E-money Sectors in Policy Statement PS 19/3 2019 (UK), para 3.18–3.24.
157 The study found that 20 percent of consumers who had taken out credit were actively prompted by the digital application system to indicate a higher income. See FinCoNet, *Report on Digitalisation*.
158 FinCoNet, *Report on Digitalisation*.
159 EC, *Behavioral Study on Digitalisation*.

160 All examples from OECD, *Short-Term Consumer Credit*.
161 FCA Conduct of Business Sourcebook—October 2020 (UK), 4.6; FCA, *FCA's Regulatory Approach to Crowdfunding (and Similar Activities)*, para 3.72.
162 National Monetary Council Resolution Number 4,656 of April 26, 2018 (Brazil), art. 17.
163 RBI NBFC—Peer to Peer Lending Platform Directions 2017 (India), para 12(2).
164 FCA Conduct of Business Sourcebook—October 2020 (UK), 4.5.6R; FCA, *FCA's Regulatory Approach to Crowdfunding (and Similar Activities)*, para 3.74–3.75.
165 Financial Markets Authority of New Zealand, *Fair Dealing in Advertising*.
166 Consumer Credit Act 1991 (Belgium), art. 6.
167 Committee of Advertising Practice, "Trivialisation in Short-Term High-Cost Credit Advertisements."
168 Directive 2002/65/EC on distance marketing of consumer financial services.
169 BdP Circular Letter No. CC/2020/00000044 on best practices applicable to the selling of retail banking products and services through digital channels.
170 For example, see SEC Regulation Crowdfunding (USA) and DFSA Rulebook (Dubai).
171 SEC Regulation Crowdfunding (USA), General Rules and Regulations 17 CFR Part 227 (USA), Rule 402(a).
172 DFSA Rulebook (Dubai), COB 11.5.2.
173 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20), para 5.45–5.47.
174 For example, an estimated 500,000 digital borrowers in Kenya have been blacklisted by credit-reference bureaus, https://www.theeastafrican.co.ke/business/Should-digital-lenders-worry-as-clients-struggle/2560-5179802-fs8a8qz/index.html.
175 DFSA Rulebook (Dubai), COB 11.5.3.
176 RBI NBFC—Peer to Peer Lending Platform Directions 2017 (India), para 7.
177 See Lenz, "Peer-to-Peer Lending," 699.
178 FCA Conduct of Business Sourcebook—July 2019 (UK), 4.7.
179 Platforms in the United Kingdom are required to classify investors to determine whether direct financial promotions for unlisted securities can be communicated to them (for example, links to an investment website or to an investment subscription form). Only retail investors that are certified as sophisticated investors, who certify as high-net-worth investors, who confirm that they will receive regulated advice, or those who confirm that they will not invest more than 10 percent of their net investable portfolio in unlisted securities may be the targets of a direct offer.
180 Corporations Act 2001 (Cth) (Australia), ss. 738G(1)(d) and 738G(2).
181 Guidelines on Recognized Markets SC-GL/6-2015(R4-2020) (Malaysia), 13.9.
182 Interim Measures for the Administration of the Business Activities of Online Lending Intermediary Institutions 2016 (China), art. 17.
183 RBI NBFC—Peer to Peer Lending Platform Directions 2017 (India), para 7.
184 FCA Conduct of Business Sourcebook—July 2019 (UK), 4.5, 4.5A.
185 DFSA Rulebook (Dubai), COB 11.3.1 to COB 11.3.2.
186 SEC Regulation Crowdfunding introduced a new category of registered intermediary, a funding portal, that may facilitate transactions under the exemption, subject to certain restrictions. The statute and rules provide a safe harbor from broker-dealer registration under which funding portals can engage in certain activities conditioned on complying with the restrictions imposed by SEC's Regulation Crowdfunding. For example, a funding portal may not offer investment advice or make recommendations; solicit purchases, sales, or offers to buy securities offered or displayed on its platform; compensate promoters and others for solicitations or based on the sale of securities; or hold, possess, or handle investor funds or securities. See https://www.sec.gov/regulation-crowdfunding-2019_0.pdf.
187 See, for example, ASIC, *Survey of Marketplace Lending Providers* (Report 526), para 81–82; see also Committee on Global Financial System and Financial Stability Board Working Group, *FinTech Credit*, 26.
188 See, for example, FinCoNet, *FinCoNet Report on Responsible Lending*.
189 National Credit Act 2005 (South Africa), Part D.
190 Money Lending Business Act 1983 (Japan), art. 13-2.
191 FCA Consumer Credit Sourcebook—October 2020 (UK), 5.5A.
192 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP19/14), para 4.1–4.6.
193 RBI NBFC—Peer to Peer Lending Platform Directions 2017 (India), para 6(1).
194 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 21.
195 FCA Conduct of Business Sourcebook—October 2020 (UK), 10.
196 FCA Conduct of Business Sourcebook—October 2020 (UK), 10.2.9G.
197 Boeddu and Grady, *Product Design and Distribution*; FinCoNet and the G20 Task Force are also undertaking detailed research on policy and supervisory approaches to financial product governance with a report expected to be published in 2021; see FinCoNet, "FinCoNet Annual General Meeting."
198 EBA, *Second EBA Report*.
199 AFI, "Digitally Delivered Credit: Consumer Protection Issues."
200 McKee et al., "Doing Digital Finance Right."
201 FinCoNet, *Guidance to Supervisors on Digitalization*.
202 See, for example, Owens, "Responsible Digital Credit," 18, and *The Economist*, "Created to Democratise Credit."
203 Oxera, *Crowdfunding from Investor Perspective*, 25; FCA, *FCA's Regulatory Approach to Crowdfunding (and Similar Activities)*, 43 and 45.

204 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20), para 4.42–4.46.
205 See, for example, Dentons, "SEC Adopts Final Rules," 12.
206 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20), para 5.39–5.40.
207 Resolution no. 18592 of 26 June 2013 (Italy), art. 13.
208 National Consumer Credit Protection Act 2009 (Cth) (Australia), s. 47(1)(b), and Corporations Act 2001 (Cth) (Australia), s. 912A(1)(aa).
209 FCA Principles for Businesses—October 2020 (UK), 2.1.1R (Principle 8).
210 For example, see FinCoNet, *Guidance to Supervisors on Setting of Standards,* and World Bank Group, *Good Practices*, C8: Compensation of Staff and Agents.
211 SEC Regulation Crowdfunding (USA), Rule 227.302 (d).
212 Corporations Act 2001 (Cth) (Australia), s. 601FC(1)(c).
213 FCA Principles for Businesses—October 2020 (UK), 2.1.1R (Principle 6).
214 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 3(2).
215 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20), para 4.38–4.41.
216 SEC Regulation Crowdfunding (USA), Supplementary Information, 163.
217 Interim Measures for the Administration of the Business Activities of Online Lending Intermediary Institutions 2016 (China), art. 10.
218 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 3(3).
219 This topic is interlinked with the data privacy risks discussed below, as algorithmic scoring in fintech relies on alternative data and big data analytics.
220 See, for example, Hong Kong Market Authority, *Consumer Protection*; EBA, *Final Report on Guidelines*, s. 4; GDPR, art. 22.
221 EBA, *Final Report on Guidelines*.
222 BdP Circular Letter No. CC/2020/00000044 on best practices applicable to the selling of retail banking products and services through digital channels.
223 *Big data* refers to situations where high volumes of different types of data produced with high velocity from a high number of various types of sources are processed, often in real time, by IT tools such as powerful processors, software, and algorithms.
224 For further discussion of these issues see, for example, OECD, *Financial Consumer Protection Policy Approaches,* and Grady et al., *Financial Consumer Protection*.
225 Grady et al., *Financial Consumer Protection*.
226 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
227 See also, for example, the discussion of data privacy in a DFS context in OECD, *Financial Consumer Protection Policy Approaches.*
228 Consumer Privacy Act of 2018 (California, USA).
229 Consumer Privacy Act of 2018 (California, USA), s. 1798.140(o)(1)(K).
230 Consumer Privacy Act of 2018 (California, USA), s. 1798.140(o).
231 GDPR, Recital 43.
232 GDPR, art. 5(1).
233 MicroSave, "Making Digital Credit Truly Responsible."
234 GDPR, art. 5(1).
235 Also see OECD, *Financial Consumer Protection Policy Approaches.*
236 Bill on Consumer Online Privacy Rights Act, s. 2968, 116th Congress (December 2019) (USA).
237 GDPR, art. 20.
238 GDPR, art. 17.
239 For a detailed discussion and country examples, see also G20/OECD Task Force on Financial Consumer Protection, *Financial Consumer Protection Policy Approaches.*
240 Megaw, "Peer-to-Peer Groups"; Makortoff, "Peer-to-Peer Lender."
241 Deng and Yu, "Business Is Withering."
242 Based on discussion with BdP. See BdP Circular Letter No. CC/2020/00000044 on best practices applicable to the selling of retail banking products and services through digital channels. Also see BdP Circular Letter No. CC/2018/00000004 for form of questionnaire. For further details, see G20/OECD Task Force on Financial Consumer Protection, *Financial Consumer Protection Approaches.*
243 FCA, *Financial Lives Survey*.
244 World Bank Group, *Global Experiences from Regulatory Sandboxes.*
245 Buku and Mazer, "Fraud in Mobile Financial Services."
246 A similar approach is utilized in the case of remittances, where domestic regulation applies to agents that originate or disburse remittances.
247 ASBA and IDB, *Consumer Protection,* 21.
248 See Boeddu and Grady, *Product Design and Distribution*, 10 and 23.
249 See, for example, ASBA and IDB, *Consumer Protection,* 41–52; FinCoNet, *Guidance to Supervisors on Digitalisation.*
250 World Bank Group, *Next Wave;* FinCoNet, *SupTech Tools.*
251 For example, see FinCoNet, *Guidance to Supervisors on Digitalisation.*
252 Reuters, "Regulatory Problems."

DIGITAL MICROCREDIT

4

DIGITAL MICROCREDIT

4.1 INTRODUCTION

a) Scope of chapter

This chapter focuses on innovative microcredit products that are seeing significant consumer take-up, particularly in emerging market and developing economies. These products are typically accessed via mobile devices and often involve automated credit scoring and fast approval. For purposes of this paper, such products are referred to herein as "digital microcredit." Digital microcredit products introduce new manifestations of risks to consumers due to the unique characteristics of such products. Note that in order to provide focused discussion of a defined set of products, this chapter does not specifically cover lending via mobile banking (that is, traditional loan products accessed through a bank's mobile banking platform) or online or digital lending more broadly, including the increasing range of credit services being made available to consumers via non-financial institutions such as e-commerce platforms. However, many of the risks discussed below (as well as regulatory approaches) may also apply to broader online and digital lending.

b) Key characteristics of digital microcredit

Digital microcredit products, particularly in developing countries, are often short term and low value and may have high fees. Loan terms can range from one week to a few months. Loan sizes range from a few to a few hundred US dollars. For example, a 2017 study in Tanzania found the mean loan size for digital microcredit to be TSh 33,757 (approximately $15).[253] Digital microcredit products tend to be more expensive than traditional credit products, and a variety of pricing models may be used. Digital microcredit providers may charge fixed interest rates per day, week, or month. Interest rates vary widely. When translated into APR, studies have shown rates for digital microcredit ranging from 24 to 174 percent[254] and from 12 to 621 percent in Kenya specifically.[255] Alternatively, flat fees or fees based on a percentage of loan principal may be charged instead of (or in addition to) interest rates. Digital microcredit offers may be bundled with additional products, such as bill-payment services, money-transfer services, and insurance.

Digital microcredit products are accessed via remote digital channels with little to no human interaction. The majority of digital microcredit models initially relied on feature phones, using SMS, SIM card toolkits, or Unstructured Supplementary Service Data (USSD). Increasingly, digital microcredit products are also available via smartphones and app-based lenders. For example, in Sub-Saharan Africa, digital microcredit offered via feature phones remains predominant in Kenya and Tanzania, whereas in Nigeria the number of feature phone-based products equals that of app-based digital microcredit products.[256] Funds are disbursed directly into mobile money accounts or bank accounts.

Digital microcredit products are rapidly approved and typically employ automated credit scoring that leverages alternative data. The application and approval process for digital microcredit is often instantaneous or near instantaneous or takes only a matter of hours. Digital microcredit models frequently rely on innovative, alternative data sources such as mobile phone activity, mobile

money transactions, or social media data. Such data is analyzed via algorithmic processing to generate rapid, automated credit decisions. Digital microcredit providers may outsource certain activities to third parties, including algorithm development, data analytics, and credit scoring, as well as marketing and loan recovery.

Business models for digital microcredit often involve non-bank lenders and outsourcing to third parties. Digital microcredit providers include banks, MNOs, and other non-bank lenders. Though digital microcredit business models are constantly evolving, many can be categorized under one of the following four models:[257]

1. *Bank + MNO partnership*: Licensed bank partners with MNO with mobile money service. Bank conducts credit scoring and lending; MNO provides access to customers, transactional data, and channel for disbursements and repayments (for example, M-Shwari in Kenya and M-Pawa in Tanzania).
2. *Non-bank lender + MNO partnership*: Regulated or semi-regulated non-bank financial institution partners with MNO (for example, Timiza and Nivushe in Tanzania).
3. *E-money issuer + regulated financial institution*: Licensed e-money issuer partners with bank or semi-regulated non-bank financial institution (for example, Billetera Personal by Personal S.A. in Paraguay).
4. *Non-bank mobile internet application*: Non-bank lender, often unregulated, may be based outside the country; accessed via smartphones and utilize smartphone data (for example, Branch in Kenya and Tanzania and Tala in Kenya, Philippines, Mexico, and India).

Digital microcredit customers often use digital microcredit for day-to-day needs and household expenses.[258] Some digital microcredit providers target specific customer segments, such as low-income borrowers, urban borrowers, small-business owners, or students. Many consumers have an ongoing need for such loans, as evidenced by the high number of consumers who have active digital loans, borrow on a recurring basis, and have multiple digital loans.[259] In addition, 56 percent of borrowers in Tanzania and 47 percent in Kenya indicate they have been late on repayments for digital microcredit. [260] Data from digital microcredit borrowers in Kenya between 2016 and 2018 showed that more than a quarter of active digital loans were non-performing loans, and half of non-performing digital loans had outstanding balances of less than $10.[261]

c) Benefits and risks of digital microcredit

Digital microcredit has expanded access to credit to millions of low-income consumers, many with no formal credit histories. Digital microcredit can also be quick and convenient to obtain, with little formal documentation required and no need to visit physical outlets.

However, digital microcredit also poses new manifestations of risk to consumers arising from the digital delivery channel and the nature of the product and underlying business models. Consumer risks can arise due to digital delivery channels, such as with respect to poor disclosure via feature phones. Consumer vulnerability to aggressive sales and marketing practices can be heightened by digital microcredit providers who exploit behavioral biases. The increasing prevalence of short-term, high-cost consumer credit has already raised alarm in many countries. The risks related to such loans can be compounded where digital loans are marketed to consumers with little regard for the capacity to repay. Consumers may face aggressive debt collection practices and inappropriate use of personal data. Digital microcredit also poses new risks that arise from the use of alternative data and algorithmic scoring models.

Such risks have already translated into real harms to consumers. As noted above, the levels of non-performing loans and defaults are quite high in certain digital microcredit markets. Consumers are developing negative credit histories and may become increasingly indebted and caught in debt traps. Instances have been observed of digital microcredit borrowers reducing food purchases in order to repay a digital microloan.[262] On the flip side, use of algorithms may lead to discrimination and unfairly exclude potential borrowers.

d) Emerging examples of regulatory approaches to address risks

The following sections explore new manifestations of risks to consumers that arise from digital microcredit and emerging policy approaches to address such risks. Discussion of risks to consumers and accompanying regulatory approaches to address such risks are organized by the following categories:

- Disclosure and transparency (for example, incomplete or non-transparent information on pricing, inadequate access to incomplete T&C, poor format of disclosure and user interface, poor timing and flow of disclosed information).

- Marketing practices via remote channels (for example, "push" marketing and unsolicited offers, exploitation of behavioral biases, misleading ads targeting vulnerable consumers, remote nature and speed of digital channels).
- Unfair lending (for example, high prices, business models based on high loss rates, mass marketing to consumers without assessing ability to repay, rolling over loans and multiple borrowing, abusive debt collection practices)
- Algorithmic scoring (for example, bias and discrimination based on proxies reflecting sensitive attributes).
- Gaps in the regulatory perimeter (for example, digital microcredit providers not being subject to requirements equivalent to those for traditional lenders or not falling under any regulatory authority).

Due to the cutting-edge nature of many risks, real-life examples of regulatory approaches specific to digital microcredit are still limited. Therefore, this chapter draws from multiple sources depending on the nature of the consumer risk. For example, to address risks related to the challenges of effective disclosure via digital channels, examples are drawn from a range of emerging approaches related to digital disclosure more broadly. Similarly, addressing risks related to aggressive marketing and unfair lending practices draws from approaches used to address such issues for short-term, high-cost consumer credit (whether digital or not) that have been employed in developed countries. In all cases, concrete examples of regulatory approaches employed by policy makers are provided where available. However, where real-world examples of regulatory approaches are lacking, suggested approaches are instead drawn from relevant research and international guidance, or from innovative approaches introduced by industry that could be further encouraged by policy makers. For example, emerging proposals on how to address risks arising from the use of algorithms draw from a range of research on algorithms, artificial intelligence (AI), and machine learning, often in settings beyond credit scoring or beyond the financial sector.

e) Summary of risks and regulatory approaches discussed in this chapter

Table 3 summarizes the new manifestations of consumer risks and corresponding regulatory approaches discussed in this chapter.

4.2 CONSUMERS NOT PROVIDED WITH ADEQUATE INFORMATION

Poor disclosure practices are a common cause for concern with respect to digital microcredit, due to poor practices by providers and exacerbated by digital disclosure factors and constraints. Risks to consumers can arise from a lack of key information being disclosed, information being disclosed in an unclear manner, and information being disclosed too late to be of use to consumers. For example, in a study on digital microcredit in Kenya and Tanzania, 19 percent of borrowers in Kenya and 27 percent of borrowers in Tanzania reported experiencing poor transparency, such as unexpected fees or not understanding the terms of a loan. Experiencing poor transparency correlated with higher levels of late repayment and default (37 percent and 39 percent, respectively) compared to digital borrowers that did not report experiencing poor transparency.[263] Conveying information clearly and comprehensively via the small screens of mobile phones also poses an inherent challenge.

Fundamental good practices for disclosure and transparency remain relevant to digital microcredit, but with necessary adaptations to address the unique aspects of digital microcredit and digital channels. As a starting point, existing disclosure and transparency rules could be made to apply to digital microcredit, such as use of plain language. The principle of having clear and consistent pricing information, such as APR and TCC, will require adaptation for digital microcredit. Requirements geared toward paper-based approaches, such as KFSs, will also require adaptation for digital channels. Practical means for highlighting the most important T&C of a digital microcredit product will be even more critical than when highlighting T&C of standard credit products, given the limited space to convey information.

Digital channels do not only have to pose a challenge to transparency, though; digital models can also be actively and strategically leveraged to enhance transparency. For example, mobile channels provide an opportunity to have interaction with a consumer that is more dynamic than that provided by a static document. Digital channels also allow for more personalization. Digital models provide an opportunity to incorporate behavioral insights into the design and the process of disclosing information, which could be leveraged to address common shortfalls in disclosure.

Countries that have begun to tackle these issues increasingly seek to integrate behavioral insights and rely on practical guidance. Leveraging the wide range of existing research on how to make disclosure more effec-

TABLE 3: Consumer Risks and Regulatory Approaches: Digital Microcredit

RISKS TO CONSUMERS	REGULATORY APPROACHES	SEE PAGE
Disclosure and transparency **Content of disclosure** • Information on pricing is incomplete and non-transparent (for example, range of different methods used to convey pricing, finance charges not disclosed separately from principal or) • Inadequate access to complete information on T&C—for example, links to full T&C provided at separate location)	• Require prominent disclosure of both total cost metrics and clear breakdown of costs • Require disclosure of key T&C in channel being used for transaction • Indicate specific T&C that must be disclosed in transaction channel • Require access to full T&C, including after transaction completed	54
Format of disclosure • Lack of standardized format for costs • Information conveyed via mobile phones in a format or manner that does not facilitate comprehension • Consumers may not be able to retain information	• Encourage greater standardization in presentation of fees/pricing • Require plain language without technical jargon or graphical elements affecting readability • Require standardized presentation of information adapted for digital channels (for example, bite-sized chunks of info provided in consistent manner) • Provide secondary layers of information for further details • Provide offline channels to obtain further info and assistance as well as the ability to access info for future reference	55
Timing and flow of information • Key information such as pricing provided after completion of a transaction • Less appealing information may be de-emphasized	• Require order and flow of info to enhance transparency and comprehension, providing an intuitive "digital journey" through a transaction process • Require disclosure of pricing and key T&C earlier in transaction process • Leverage behavioral insights to encourage consumers to engage with info (for example, require confirmation to move to next stage of transaction)	57
User interfaces • User interface may not be user-friendly, with complex menus that are difficult to navigate	• Require user interface be user-friendly and easy to navigate, including on low-end mobile devices • Encourage consumer testing of user interfaces • Require providers to provide guidance to consumers on user interfaces	58
Marketing practices via remote channels • Push marketing and unsolicited offers encourage impulse borrowing • Exploitation of behavioral biases (for example, encouraging borrowing of maximum amount possible, trivializing loans) • Misleading ads targeting vulnerable consumers (for example, emphasizing benefits, hiding risks, unrealistic offers with hidden conditions, marketing on weekend evenings) • Remote nature of digital channels and rapid speed of transactions increase consumer vulnerability	• Require explicit warnings on risks of short-term, high-cost credit and information on alternatives to such loans and helpful resources • Ban sales practices that focus on ease of obtaining credit, trivialize credit, or target vulnerable consumers • Slow down process of transacting digitally to allow consumers more time for reflection and deliberation (for example, intermediate steps/screens, adding a review screen) or appropriate cooling-off period • Require loan options be presented in manner that is beneficial (or at least neutral) to consumers and not exploitative (for example, banning default selection of maximum loan size, pre-ticked boxes that lead customers to suboptimal options)	59
Unfair lending • High prices for digital microcredit • Mass marketing to consumers with little assessment of individual consumer circumstances or ability to repay ("lend-to-learn" models) • Certain business models based on high loss rates (for example, large late fees relative to size of loan) • Poor practices such as rolling over loans or encouraging multiple borrowing • Abusive debt collection practices utilizing mobile phone and social media data to contact relatives, friends, and colleagues	• Require providers to assess the ability of prospective customers to repay loans and grant loans only where they are affordable to potential borrower • Impose requirements that limit rollovers and multiple borrowing to decrease risk of over-indebtedness • Require enhanced monitoring of loan portfolio, particularly where automated credit scoring is utilized • Apply product design and governance rules to digital microcredit—that is, design process and customer acquisition plans should ensure that potential harms and risks to consumers are considered and mitigated • Adapt debt collection rules to prevent abusive debt collection practices utilized by digital lenders	61

TABLE 3, *continued*

RISKS TO CONSUMERS	REGULATORY APPROACHES	SEE PAGE
Algorithmic scoring • Biased outcomes due to poor algorithm design, incomplete or unrepresentative input data, biased input data • Discrimination based on proxies reflecting sensitive attributes • Consumers unaware or powerless regarding use of algorithm • Regulators lack technical expertise to evaluate algorithmic systems; proprietary nature of algorithms	• Apply fair treatment and anti-discrimination rules to algorithms • Require appropriate procedures, controls, and safeguards during development, testing, and deployment of algorithms to assess and manage risks related to bias and discrimination • Require regular auditing of algorithmic systems by external experts • Ensure transparency to consumers regarding use of algorithms • Provide consumers with the right not to be subject solely to automatic processing and the right to request human intervention	64
Regulatory perimeter (cross-cutting issue) • Unlevel playing field for different types of providers, with often weaker rules for non-bank lenders • Regulatory gaps for app-based lenders, who may not be covered by any regulatory authority and/or may be based in another country	• Establish activity-based framework covering all providers of digital microcredit (banks, MNOs, non-bank lenders) so that activities with the same risks are covered by the same rules • Where activity-based approach not feasible, be opportunistic and build off of existing rules and powers to cover non-bank microcredit providers • Coordinate with domestic and international regulatory authorities • Consider regulating domestic agents and intermediaries of foreign fintech companies • Pursue complementary, non-regulatory measures, including industry codes of conduct and working with mobile platforms to establish and enforce rules in key areas for app-based lenders	67

tive, particularly by incorporating insights on consumer behavior, will be important. As technology and business models continue to evolve rapidly, policy makers will need to balance between providing flexibility for innovation with the need for clear, prescriptive rules for certain elements of disclosure. Obtaining a better understanding of industry practices and providing ongoing and evolving guidance to industry is a useful approach, rather than moving too quickly to issue rigid rules.

a) Lack of adequate information

Consumers often face a lack of key information when obtaining digital microcredit products. Full information on cost and relevant T&C is particularly incomplete for digital microcredit products. A 2015 survey of regulators in 15 developing countries found that limited disclosure of costs was the highest market conduct concern for regulators with respect to digital microcredit.[264]

Risk: Lack of complete information on pricing

Pricing for digital microcredit products is very often incomplete and non-transparent. Issues that commonly arise include pricing for digital microcredit being portrayed in the form of an interest rate, finance charge, or a combination of the two. Finance charges are often not conveyed separately from repayment of principal. Total cost metrics such as APR and TCC are often not provided. Repayments may be presented on a daily, weekly, or monthly basis depending on the provider or product. Fees for third-party charges, such as cash-out fees by an MNO or fees for bundled products, are not clearly communicated to consumers. As a result, it is difficult for consumers to understand the full costs of a digital microcredit product or to compare across providers easily, difficulties that can be made greater by the remote and speedy method of acquiring such credit via a digital channel.

Regulatory approaches to address lack of complete information on pricing

Similar to paper-based disclosure, digital microcredit providers could be required to provide total cost indicators. Research on digital microcredit has shown that presenting TCC (as opposed to showing fees individually, with no sum indicating total cost) results in consumers being 64 percent more likely to choose the lower-cost loan product.[265] Total cost indicators such as APR or TCC can be used to capture all known up-front and recurring costs over the life of a digital microloan, including costs for required third-party services. Particularly given the short-term nature of digital microcredit, policy makers should consider which metric (APR or TCC) is more appropriate and useful to consumers. Though APR is typically preferred, TCC (a monetary figure) may be more useful in the case of short-term credit.[266]

In either case, total cost indicators would need to be calculated in a consistent manner and displayed prom-

inently in a digital context. APR and TCC are often required to be emphasized in paper-based disclosures. Such emphasis can be replicated in mobile disclosure—for example, by highlighting APR or TCC visually and requiring that it be included on the same screen with headline prices.

In addition to total cost indicators, a clear breakdown of fees is likely to be important. Consumer focus groups have shown that a price breakdown or summary of charges is very beneficial to consumers' understanding of personal loans.[267] In particular, finance charges should be displayed separately from repayment of loan principal. Research has shown that separating financing fees from loan principal repayments improves consumer borrowing decisions as evidenced by a decrease in default rates.[268] Charges for bundled services should also be disclosed separately.

Risk: Inadequate access to key information on terms and conditions

T&C are often not easily accessible. Given the limited space available to convey information via mobile channels, some providers cherry-pick appealing information to disclose, providing incomplete information on risks or other obligations. Where full T&C are made available, a common practice among digital microcredit providers is to provide a link to full T&C to be found online. This poses a significant barrier to feature phone users to access such information, as well as an inconvenience to smartphone users in the middle of a transaction. In addition, T&C found online are often long and full of complex legal language and technical terms, making the information difficult for consumers to understand. T&C may also be difficult to store and access at a later date.

Regulatory approaches to address inadequate access to key information on terms and conditions

Requiring a summary of key T&C to be disclosed within the channel being used to access the digital microcredit product would help lack of awareness about T&C. Merely linking to full T&C elsewhere could be insufficient, although access to full T&C should be provided prior to conclusion of the transaction. For example, when conducting sales of retail banking products and services via digital channels, financial institutions in Portugal are required to "prominently present information on the basic features of the banking product or service and on other elements deemed relevant, such as fees and expenses that may be applicable, on the main screen or webpage of the marketing platform, using larger characters, information boxes, pop-ups, simulations, overviews or other similar means."[269] In addition, BdP requires credit institutions to report to BdP information on the marketing of consumer credit products initiated and concluded via digital channels (including both internet platforms and mobile apps), with the intent to ensure respect for the rights of bank customers, in particular in the access to precontractual and contractual information.[270]

It may be worthwhile for regulators to be more prescriptive regarding which specific T&C are considered key and must be disclosed in this summary. Guidance on digital credit from FinCoNet states that providers should be required to provide a summary of key information to consumers including specific features such as TCC, APR, and repayment amounts, risks, such as consequences of rollovers and late repayment, and their right to obtain further information or recourse.[271] When disclosing risks, risks should be given equal prominence as benefits. For example, the Bank of Lithuania requires that advertisements not show benefits unless they are equally visible as potential risks.[272] Information on bundled products should also be provided. In Pakistan, one of the largest digital credit providers conducted focus groups with consumers in order to identify the main T&C to focus on disclosing, such as risks of being reported to the credit bureau or not being able to graduate to a higher credit limit. The provider itself noted that it would be beneficial to have prescriptive rules on what specific key T&C must be actively disclosed to the consumer, tailored to the particular risks and vulnerabilities of local consumers of digital credit products.[273]

Digital channels also provide the opportunity to craft messaging regarding key T&C that is more tailored than with static paper-based disclosure. For example, providers can highlight risks specific to the particular user or product being purchased, such as the risk of variable interest rates.

Full T&C should also be made accessible after the digital loan transaction is completed. In Australia, ASIC guidance on good practices for digital disclosure notes that clients should be able to keep a copy of disclosed information so that they can access the information in the future. This can include either the ability to save a digital copy, or provision of a hyperlink to disclosed information on a website that continues to be accessible for a reasonable period of time.[274]

b) Poor format of disclosed information

Disclosing information in an engaging format is especially critical in digital microcredit's digital context. Key information may be difficult to find or hard to understand. Particularly with respect to feature phones, practical limitations on the space to convey information as well as the ability use different design formats pose a challenge to

transparency. Consumers' attention span may also be more limited, combined with a desire for rapid transactions.

Risk: Lack of standardized format for costs

A particular issue with respect to digital microcredit seems to be inconsistent practice toward disclosing costs. As stated above, costs associated with digital microcredit are disclosed as rates or monetary figures and using a variety of repayment periods. The proliferation of different and sometimes complex pricing methods can be confusing for consumers and, in some cases, is used by providers to hide fees.

Regulatory approaches to address lack of standardized format for costs

Policy makers could establish greater standardization regarding the presentation of fees for digital microcredit. While there are many different business models for digital microcredit, as well as differing pricing methods tied to these various models, providers should not take advantage of complex and impenetrable pricing. Similar to issues that arose in the microfinance industry a decade ago, when different pricing models were sometimes employed to confuse and mislead consumers, greater standardization is needed throughout the digital microcredit industry to improve transparency. Consumer research on digital microcredit in Kenya found that displaying cost information in a consistent way made consumers more likely to choose the cheapest option.[275]

Rules will need to strike a balance between more standardized presentation and terminology for digital microcredit pricing while still allowing for innovation and differentiation. For example, in addition to requiring disclosure of total cost indicators along with a breakdown of fees, presentation by repayment period could be standardized (based on different categories of digital credit products). Terminology used for fees could also be made more consistent across providers, in particular any fee charged that is the equivalent of a finance charge. Rules could be considered on the general order in which different types of fees and charges are displayed. The ITU-T Focus Group on Digital Financial Services suggests that regulators establish standard definitions for the cost and fees of digital credit, including all bundled services; require disclosure in line with these standard definitions to ensure consistency across offerings; and require clear, conspicuous, and understandable disclosure of financial and other consequences of early, partial, late, or non-repayment of a digital loan.[276]

Risk: Poor format of terms and conditions

At a broader level, information on the key T&C of digital microcredit products is often not conveyed in a format or manner that facilitates comprehension. Several challenges arise due to the nature of the digital channel. Space is limited to convey all information fully. The basic technology of feature phones limits the design elements that can be used to convey information. Mobile channels do not allow for further explanations about key T&C that consumers may find confusing. These challenges are compounded by the behavioral tendencies of consumers, who already tend to pay less attention to T&C for short-term loans.[277]

In addition, consumers may not be given the ability to retain information. Retention of disclosed information is important as a reference for consumer understanding of their rights and obligations and as evidence in the case of a complaint or dispute. This risk is compounded when information is provided via USSD on feature phones with small screens or is available only on a website that may not retain the version of the information originally given to the consumer.

Regulatory approaches to address poor format of terms and conditions

As a general principle reflecting international good practice on disclosure, communications from FSPs to consumers should be in plain and easily understandable terms and not misleading, regardless of the channel being used to communicate. Disclosure of T&C for digital microcredit products should therefore be in plain language without confusing technical jargon, particularly given that users of digital microcredit products typically have lower financial and digital literacy. For example, recognizing that paper-based disclosures do not match the current reality of consumers engaging via digital channels, the FCA undertook an initiative (called "Smarter Consumer Communications")[278] to consider the changes required for effective digital disclosure that allowed for innovation while clarifying compliance with existing rules. This initiative was driven partly by the need to provide clarity to firms regarding acceptable disclosure practices among innovative new communications approaches. As part of this initiative, the FCA emphasized that providers should work together to develop consistent terminology and reduce the complexity of language and technical jargon.

Consideration may also be required regarding how graphic elements affect readability, particularly with respect to digital channels. In Portugal, best practices from BdP applicable to the sales of retail banking product and services via digital channels include that financial institutions "evaluate the use of graphic elements such as font size, color, icons and images in all information media, including on the screens of the marketing platform and in advertising, ensuring that those elements are not likely

to affect the readability, understanding, and prominent of information."[279]

Existing requirements on disclosure via paper-based formats—that is, page length, font size, use of KFSs—will need to be appropriately adapted for mobile channels. As noted above, a summary of key T&C for digital microcredit can be provided directly to potential borrowers. It will be important for such summaries to be designed well and user-friendly, and for information to be conveyed in a manner that increases the likelihood of consumers paying attention to such information. A European Commission behavioral study on digital sales of retail financial services found that well-laid-out, ordered information had a substantial positive effect on consumers' choosing more optimal products in a test environment, and the positive impact actually proved greater on mobile phones than desktop channels.[280] Consumer testing on disclosure for digital microcredit in Kenya found that summarized, simpler versions of T&C led to better comprehension and more searching for products from other providers, a positive outcome since one of the objectives of disclosure is to increase comparison shopping.[281]

Adapting (paper-based) KFS requirements for mobile channels could involve standardizing presentation in order to highlight key information in a structured and consistent manner. Information could be broken up into bite-sized chunks that are easier for consumers to digest and that are grouped and ordered in a consistent manner across providers (for example, by fees, conditions, risks, and so on), in order to achieve similar benefits from paper-based KFSs. The FCA has asked providers to do more to incentivize consumers to engage with information delivered in a digital environment, including by layering information as a means to guide consumers through their journey in a way that enables them to digest each part easily, rather than including all information up front.[282] For example, summary information can be included up front, with more detailed information included in secondary layers in a menu.

To counterbalance the limitations of digital disclosure, consumers could be given easy access to off-line channels to obtain further information as well as the means to access disclosed information for future reference. The Center for Financial Inclusion suggests that providers offer consumers channels to contact a provider representative (for example, via a call center, online chat, or an agent/branch location) to ask questions and clarify T&C prior to agreeing to T&C.[283] For example, when conducting sales of retail banking products and services via digital channels, financial institutions in Portugal are required to assist customers to obtain further information by making available tools such as a hotline or live chat, chatbot, or other interactive tools.[284]

c) Timing and flow of disclosed information

Risks to consumers

The timing and flow of information disclosed via digital channels can impede transparency. Key information such as pricing may be provided only after a consumer completes a digital microcredit transaction. Consumers may not be given sufficient time to review a mobile screen before it times out. Less appealing information may be de-emphasized. More broadly, user interfaces on mobile phones may be challenging to navigate, hampering effective disclosure. However, digital channels also provide certain benefits that can be leveraged to enhance transparency by making disclosure more "active" for users.

Regulatory approaches

The order and flow in which information is provided can enhance transparency and comprehension. As noted by the FCA, it can be beneficial to approach disclosure as a "digital journey" and use an engaging digital format to help consumers progress through the steps of a transaction. [285] ASIC guidance on good practices for digital disclosure notes that "provider(s) should consider whether the disclosure flows logically in a way that aids understanding of the product."[286] Appropriate prominence should be given to each aspect of a product and disclosed information should not divert consumers away from less appealing information.

One approach would be to make mandatory the timely disclosure of pricing earlier in the transaction process. ITU-T Focus Group on Digital Financial Services suggests that regulators require disclosure of fees prior to the completion of a transaction, with the option to cancel the transaction after the disclosure.[287] In Kenya, the CAK identified a particular issue with consumers not being aware of charges for their digital loans (and other transactions conducted via mobile wallets) due to the fact that providers were not disclosing the cost of such transactions until after the consumer accepted the transaction on their mobile device. The CAK therefore issued guidelines requiring all providers of digital financial services to disclose all applicable charges to customers for a mobile money transaction (including microloans, money transfers, and microinsurance) prior to completion of the transaction. The CAK chose not to be overly prescriptive; rather, they gave general guidelines that providers should disclose what charges would be incurred, give consumers an opportunity to cancel, and provide a receipt afterward. The CAK also reviewed samples of disclosure messages to be used

by providers.[288] As a result, a survey of users of digital financial services in Kenya found that the percentage of survey participants who could correctly estimate the cost of their last M-Shwari loan of KSh 200 went up from 52 percent before the CAK order to 80 percent afterward.[289]

Similarly, key T&C could be provided earlier in the transaction process and given prominence. Key T&C should obviously be provided before a consumer accepts a digital loan offer. In Kenya, consumer testing on disclosure of information for digital microcredit found that just moving the option to view T&C from the last option in the main menu for a digital loan product to its own screen increased consumer viewing of T&C from 9.5 percent to 23.8 percent.[290]

Integrating behavioral insights into regulatory approaches can help to encourage consumers to engage with information provided. Regulators who have taken action to adapt consumer protection approaches for digital credit specifically cite the need to incorporate behavioral insights into their approaches. While less information can be conveyed via mobile channels, such channels pose an opportunity to allow consumers to review information at their own pace and in a certain order. These characteristics of digital channels can be taken advantage of. For example, for sales of retail banking products and services through digital channels, financial institutions in Portugal are required to ensure that the selling process proceeds to the next stage only after customers confirm that they have read to the end of mandatory information documents, and financial institutions should use visual and textual techniques to encourage customers to do so.[291]

The dynamic nature of mobile phones could similarly be leveraged to require consumers to confirm or acknowledge key information before moving forward in the transaction process. In the aforementioned consumer study in Kenya, requiring an opt-out approach to viewing T&C increased the rate of viewing from 10 percent to 24 percent, and the resulting delinquency rate was 7 percent lower for borrowers who read the T&C.[292] Similarly, consumers could be required to confirm or acknowledge APR, TCC, or repayment amounts or confirm that they understand conditions or risks associated with a digital product before moving forward in the transaction process.

Measures could be used to ensure that consumers are given adequate time to review information via digital channels. The Center for Financial Inclusion highlights the need for providers to build in time for consumers to review T&C by having appropriate time limitations to review multiple screens in a mobile app or USSD menu.[293] However, consideration should be given to any negative impacts from increased airtime costs, particularly for low-income consumers.

Beyond disclosure at the point of sale, digital channels can be leveraged during the duration of the loan term to nudge consumers toward healthier behaviors. For example, text alerts and notices on mobile apps can be used to send direct, timely reminders to borrowers regarding upcoming due dates for repayments. Though related to banking alerts and not digital microcredit specifically, research by the FCA found that text alerts or notices via mobile banking apps that were triggered automatically were effective in changing consumer behavior and reducing overdraft charges.[294] Policy makers could consider similar requirements with respect to digital microcredit, in order to help consumers avoid late payment penalties or default. Providers could be required to send texts or digital alerts seven days before loan repayments are due or for missed payments, accompanied by concise warnings on the risks of continued late repayment. This practice has already been observed among more responsible digital credit providers.[295]

d) User interfaces

Risks to consumers

User interfaces for digital microcredit are often not user-friendly and can be ineffective in assisting consumers to review and understand information. Information may not well adapted to suit different types of mobile screens—for example, using apps on low-end smartphones, making information literally difficult to read. Menus may be complex and confusing to navigate, leading to consumers accepted terms without reviewing them or making mistakes in their transactions. Menus may also be in English or a formal version of the local language, making them more difficult for low-literacy consumers to understand.

Regulatory approaches

Requirements could be used to ensure that user interfaces are clear, user-friendly, and easy to navigate. The Center for Financial Inclusion suggests that user interfaces provide step-by-step instructions in a major local language.[296] ASIC guidance notes that digital disclosure should be easily navigable, providing a practical example of a menu feature in an app that allows consumers to go immediately to sections of the disclosure that are most important to them.[297] The same standards in quality of disclosure should apply across different types of mobile phones and platforms. Additional methods to improve the user interface include designing interfaces and processes to reduce keystroke error; applying human-cen-

tered design; providing key instructions as needed within the transaction flow (more relevant for smartphones); and providing full transaction details on one screen to finalize the transaction at the end stage.[298]

Similar to consumer testing of KFSs, testing of user interfaces for the provision of digital microcredit via mobile channels would also be highly beneficial. The G20 Task Force suggests that policy makers encourage FSPs to test digital disclosure approaches to ensure their effectiveness, taking into account factors such as different screen sizes and communication formats.[299] The FCA has also emphasized that firms should use behavioral insights to create more effective product information for consumers and test communications with real consumers. To complement the measures suggested above, providers could also be required to provide guidance and training to consumers on user interfaces, including via agents.

4.3 MARKETING PRACTICES VIA REMOTE CHANNELS

a) Risks to consumers

Marketing practices employed by some digital microcredit providers pose several risks to consumers. Common issues include digital microcredit being aggressively marketed to consumers, such as via unsolicited, preapproved offers, or using misleading or incomplete information in marketing materials. Marketing practices may also exploit behavioral biases by leading consumers into making impulsive decisions to take up loans that they do not need or larger loans than necessary. The negative repercussions of aggressive or misleading marketing can be heightened by the remote nature and ease and speed of digital transactions, resulting in poor decision-making by consumers.

Push marketing and unsolicited offers used by some digital microcredit providers may encourage consumers to borrow on impulse, without prior intention or a clear purpose for the loan. In general, there is evidence that providers drive demand for high-cost, short-term credit more than consumers, more so than in a traditional financial services context.[300] With respect to digital microcredit specifically, aggressive marketing techniques include push marketing. The business model for mobile-based lending is often based on recurring invitations for prequalified credit sent to existing or prospective consumers via unsolicited text messages or phone calls. Such practices exploit behavioral biases, such as present bias and loss aversion, and may lead consumers to take out loans without considering whether they really need them or are able to repay them, as they are afraid of "missing out." In fact, research in Kenya has shown that many first-time users of M-Shwari (the most popular digital credit product) tried it out for "no reason at all."[301]

Providers may use marketing techniques that exploit behavioral biases to entice consumers to borrow more than necessary. Examples include marketing that encourages consumers to borrow the maximum amount possible, suggests that loans can be repaid easily, or trivializes the seriousness of a loan. Providers may market loans by framing them based on the maximum sum that can be borrowed. "Interviews with consumers and lenders confirmed that many customers borrow at the suggested loan limit rather than propose a lower sum that would be sufficient to meet their immediate needs."[302] A study in Latvia found that digital lenders encouraged consumers to disclose a higher income in order to obtain a larger loan.[303] Aggressive advertising via "cute messaging" was noted by FinCoNet as undermining the seriousness of entering into a credit contract and distracting consumers from the high costs of a loan.[304]

Advertising for digital microcredit may be misleading or targeted at vulnerable consumers, and both risks may be enhanced by the use of technology. A European Commission behavioral study on the digitalization of marketing and distance selling of retail financial services highlights several poor practices that also apply to digital microcredit.[305] These include emphasizing benefits while giving lower prominence to costs; omitting or making key information such as risks or costs difficult to find; and presenting unrealistic offers (such as loans that are almost or completely free of charge) while failing to mention the conditions attached to such offers. In addition, with big data and digital channels, it is now easy for providers to tailor the content, timing, and framing of offers to consumers' specific habits, needs, and concerns. While such capability can be beneficial for consumers, irresponsible providers can use such capability to target vulnerable consumer segments—for example, by targeting low-income households or targeting marketing at times when consumers are vulnerable to making poor decisions, such as weekend evenings.

Finally, the remote nature of digital channels combined with the rapid speed of digital transactions increase the vulnerability of consumers to aggressive marketing practices. The lack of human interaction with provider staff, combined with the fact that consumers may be transacting from the comfort of their own homes, may result in consumers taking digital loans less seriously. In addition, digital microcredit can be advertised as "one-click" or nearly automatic. These factors may lead consumers to make hasty and poor decisions.

b) Regulatory approaches

Policy makers have increasingly recognized that policy action is needed to curtail the more exploitative practices of digital lenders. For example, the Organisation for Economic Co-operation and Development suggests that "measures should be taken to identify consumer characteristics (e.g. behavioral biases or vulnerabilities) that have the most effect on borrowing decisions that consumers make and which measures can be taken to mitigate these effects."[306] This approach should be applied to digital microcredit in particular. A range of policy approaches can be employed, from less interventionist (that is, requiring warnings) to more interventionist (that is, banning push marketing).

Policy makers in several countries have taken proactive action by requiring providers to warn consumers about the risks of short-term, high-cost credit. Nudges such as warnings to consumers have been found to help improve decision-making.[307] FinCoNet suggests the inclusion of specific warnings regarding the costly nature of short-term, high-cost credit, the risks associated with short maturity, and the risks and consequences of over-indebtedness.[308] For example, short-term credit providers in Armenia must add legislated warnings to their disclosure material warning customers about the high cost of the credit and encouraging them to shop around and assess their ability to repay. In Australia, payday lenders must display a warning that borrowing small amounts of money can be expensive, suggest alternatives to taking out such loans, and provide the contact details for resources on debt help and counseling and financial education. Similarly, in the United Kingdom, high-cost, short-term credit must include a prominent risk warning and redirect consumers to resources from the authority in charge of debt advice.[309] Such approaches could be applied to digital microcredit as well as a form of short-term, high-cost credit.

Rules could be used to ban explicitly sales practices that focus on the ease of obtaining credit, trivialize credit, or target vulnerable consumers. FinCoNet suggests preventing or limiting the use of statements that induce consumers to take out short-term, high-cost credit to solve financial problems or purchase nonessential goods or that divert consumers attention from the seriousness of taking out such loans.[310] The Center for Financial Inclusion's Standards of Protection for Digital Credit note that marketing should not employ predatory sales techniques such as language implying "use it or lose it" opportunities or push messaging sent after working hours or more than once a week.[311] In Latvia, amendments to the Consumer Rights Protection Law specifically prohibit online consumer credit providers from selling their services between 23:00 and 07:00.[312] In Belgium, advertising that focuses on the ease of obtaining credit is prohibited.[313] In the United Kingdom, payday lenders are specifically required to refrain from advertising that trivializes the nature of payday loans, including by encouraging nonessential or frivolous spending or unacceptably distorting the serious nature of such loan products.[314] In Portugal, BdP requires that financial institutions refrain from using terms such as "preapproval" or "pre-acceptance" during the sales process, as such terms give the impression that credit is easy to obtain.[315]

Steps could also be taken to slow down the process of transacting digitally to allow consumers more time for reflection and deliberation. In consumer testing aimed at slowing down the transaction process via digital channels, adding intermediate steps or screens that customers must pass through, such as adding a "review screen" in the purchasing process, successfully resulted in consumers making more optimal loan choices.[316] FinCoNet suggests that supervisors establish technological requirements that allow a thorough analysis of the information by consumers and limit the risks of impulsive credit decisions, including through "restrictions that prevent consumers from moving forward in the borrowing process without checking the relevant information on the STHCCC [short-term, high-cost consumer credit]" and "measures that aim to ensure that consumers go over all relevant information on the STHCCC (e.g. minimum reading time, compulsory scroll down, questionnaire on the main features of the STHCCC)."[317] For example, in Paraguay, lenders utilizing digital channels must provide consumers with a final option of rejecting or accepting the T&C prior to the conclusion of the loan contract and disbursement.[318] Cooling-off periods could also be considered that are proportionate to the short tenure of digital loans (for example, one day for a one-month loan).[319]

The presentation of loan options should be beneficial to consumers and not exploitative. FinCoNet guidance suggests that supervisors consider taking action to restrict the use of default options for digital credit and to prevent or limit the use of illustrative examples that induce consumers to borrow higher amounts—for example, by using the maximum amount that a consumer can take out as a benchmark.[320] For example, in Portugal, financial institutions are required to refrain from using pre-ticked boxes or graphic elements to lead customers to choose certain options when conducting sales of retail banking products via digital channels.[321] Rather than marketing that defaults to preselecting the largest loan size, providers could be required to provide a range of options for consumers to choose from. A further step would be to require "smart defaults" where consumers are automatically defaulted to the best option for them.

Finally, policy makers could consider outright bans or limitations on preapproved, unsolicited offers for digital microcredit. Such rules already exist more broadly, such as rules in the European Union restricting the marketing of services that consumers have not solicited.[322] In the case of digital microcredit, MNOs or other entities may operate on the basis of obtaining broad consent for marketing further products to customers. [323] Rules could be put in place to restrict the breadth of such consent—for example, by requiring that consumers actively opt in specifically to the marketing of digital microcredit. At a minimum, consumers should also be given an easy option to opt out of push marketing of digital microcredit.

More generally, good practices in advertising and sales should be applied to digital microcredit, with adaptations for digital channels. For example, qualifying information should be placed near claims in advertising. Disclosures should be clear and conspicuous regardless of the device or platform a consumer is using to view an advertisement. Including total cost metrics such as APR or TCC could be required for advertisements for digital microcredit. Sales incentives for provider staff and representatives should be designed not to incentivize behavior that may harm consumers.[324] At a practical level, regulatory gaps may need to be addressed where existing advertising rules do not apply to advertising and marketing via new digital channels such as social media campaigns.

4.4 UNFAIR LENDING

a) Risks to consumers

The design of and business model for certain digital microcredit products pose increased unfair lending risks to consumers that require direct policy responses beyond disclosure rules. Broadly speaking, "the design of many financial and new fintech products is inherently complex… [c]ompanies can use strategies, such as price discrimination, price obfuscation, product bundling and complexity and promotion of brands leading to complicated markets and products that are difficult or impossible to compare."[325] As discussed below, such issues are highly relevant for digital microcredit products.[326]

Digital microcredit products are often characterized by very high fees. For example, high flat fees based on the full amount of the microloan may be charged regardless of how soon a borrower repays, resulting in the equivalent of a very high interest rate given the short-term nature and small loan size of digital microcredit. An Alliance for Financial Inclusion survey found that the costs of digital microcredit products were typically quite high, often in excess of 100 percent APR.[327] While pricing for digital loans tends to vary significantly across providers, the upper range of pricing can be quite high. A review of digital microcredit products in Kenya found that APR ranged from 12 percent to 621 percent.[328] Pricing for one-week loans tends to be the highest when translated into APR, with non-bank and app-based lenders charging higher rates. Some app-based lenders may also ask for a deposit or registration/membership fee before a consumer is eligible for a loan.

Digital loans may be mass marketed to consumers with little assessment of a consumer's circumstances or ability to repay. Certain digital lenders employ a "lend-to-learn" approach, where initial rounds of credit offers are intended to gather more information about consumers to strengthen internal credit scoring models. With such business models, there is little attempt to assess whether a digital loan product is appropriate or suitable for the needs or circumstances of a consumer. As a result, inappropriate products are marketed to and taken up by consumers, and loan defaults can be expected to be high, at least during initial stages as algorithms are refined.[329] Anecdotal information from digital lenders indicates that some have default rates as high as 40 percent to 50 percent for their first round of loan offers, which are sent blindly to a large number of prospective borrowers.[330] In addition, the business model of certain digital lenders (sometimes referred to as payday lenders) is openly predatory, based on high loss rates and generation of revenue via late payment fees. In addition to increasing consumer risk of over-indebtedness, the negative impact on consumers' credit histories affects their ability to access credit or employment in the future.

Poor practices may be used to roll over loans or encourage multiple borrowing. Digital lenders often encourage customers to roll over loans or to take out more loans or larger loans. For example, a review of 68 digital credit products in India, Kenya, Nigeria, Tanzania, and Ghana found that nearly half of such products (32 products) advertised reward programs that incentivized certain behaviors from consumers, such as continued use of the loan product.[331] In addition, the same study found that some digital credit providers extend loan terms automatically when payments are missed, with accompanying penalties. Particularly given that many digital loans have flat facilitation fees, providers are incentivized to focus on the quantity of loans disbursed to maximize returns. As a result, consumers may end up with multiple digital loans, sometimes taking out one digital loan to pay off another one, resulting in an endless cycle of borrowing.

Some providers use aggressive or abusive debt collection practices unique to digital microcredit. Providers may reserve the right to post about loan defaults on a

borrower's social media page, contact a borrower's contacts on their mobile phone regarding late payments or defaults in order to shame the borrower into repaying, or harass a borrower via numerous and excessive reminders sent to borrower's mobile phone. For example, the National Privacy Commission in the Philippines has reported receiving about 1,000 complaints from borrowers who used online lending apps, particularly regarding use of customers' personal data to contact relatives, friends, and colleagues to harass and shame delinquent borrowers.[332] While in some instances consumer consent may have been acquired for these practices, such consent is often not informed. Regardless, there should be appropriate limits on what types of debt collection practices digital microcredit providers may utilize that respect the privacy and dignity of consumers.

b) Regulatory approaches

A range of regulatory approaches could be considered to address the above risks, particularly around product suitability and affordability. Many examples exist of policy actions taken in other countries to address the risks of short-term, high-cost credit more broadly. Such approaches are highly relevant to digital microcredit.

Digital microcredit providers could be required to assess the ability of prospective customers to repay digital loans and to grant digital loans only where they are affordable to the consumer. The Organisation for Economic Co-operation and Development recommends that measures be put in place to "ensure that a consumer's ability to meet relevant payment obligations is assessed before a transaction is concluded, or before any significant increase in the amount of credit. The assessment should be based on relevant and proportionate information regarding the consumer, such as income and expenses, and the likely costs and risks of the credit."[333] In addition, "[c]redit should not be granted if the credit is clearly not affordable by the consumer or is likely to have a significant adverse effect on their overall financial situation."[334] Many countries already have in place general obligations to obtain and verify information about a consumer's financial circumstances. Different approaches can be used to frame this obligation, from principles-based to more prescriptive. The main considerations revolve around what a provider is required to assess and against what criteria such an assessment should be undertaken.

Principles-based approaches focus on assessing consumer affordability. For example, in the Netherlands, credit providers are required to carry out a creditworthiness assessment of a consumer before entering into a consumer credit agreement.[335] Providers should obtain information about a consumer's financial position and consider whether entering into the credit agreement is a "sound decision" for the consumer. Similarly, in South Africa, providers are prohibited from "reckless lending" and from entering into a credit agreement without first taking reasonable steps to assess a consumer's financial circumstances. A credit agreement is considered reckless if the provider did not conduct such an assessment, if the consumer did not understand the risks and obligations of the credit agreement, or if entering into the credit agreement would make the consumer over-indebted.[336]

Some countries employ more prescriptive measures to gauge affordability. For example, in Japan, moneylenders are prohibited from lending where the total amount of borrowing exceeds one-third of a consumer's annual income.[337] In Australia, the percentage of certain consumers' gross income that can be used to repay all small short-term loans is capped at 20 percent.[338]

Some regulators are making limited exceptions for "lend-to-learn" models, but such exceptions should be considered with caution, given the potential downside for consumers if they are inappropriately calibrated. In Portugal, for example, providers are required to assess a consumer's creditworthiness taking into consideration elements such as age, profession, regular income and expenses. However, an exception was made allowing providers to estimate indirectly a consumer's regular income and expenditures based on other information for loans that are equal to or less than the equivalent of 10 times the monthly minimum wage.[339] Such an exception was created to allow for more innovative, convenient, and faster digital microcredit business models.

Increasing reliance on automated credit assessments is also leading regulators to adjust traditional creditworthiness requirements by introducing stronger requirements on monitoring of portfolio performance. New guidelines on loan origination and monitoring from the EBA, which go into effect in June 2021 for financial institutions in the European Union, set out specific requirements regarding the use of automated models in credit decision-making and creditworthiness assessments.[340] The guidelines require that institutions specify the use of any automated models in creditworthiness assessment and credit decision-making processes in their credit risk policies and that institutions, when using technology-enabled innovation for credit-granting purposes, should "ensure the performance of the model, including the validity and quality of its outputs, is continuously monitored and appropriate remediation measures are taken in a timely manner in the case of detected issues (e.g. worsening or deviating from expected behavior)."[341] FinCoNet also suggests that

providers of digital credit should have automated systems that allow for prompt detection of signs of deterioration of consumers' financial capacity.[342] Such approaches are particularly relevant for "lend-to-learn" models.

Regulators are increasingly applying product design and governance rules and using product intervention powers with respect to credit products.[343] The EBA highlights that it would be good practice for providers to give further attention to "the risks that consumers might face due to the increasing use of digital channels by FIs [financial institutions] (e.g. exposing consumers to market practices that exacerbate behavioral biases) when improving their POG [product oversight and governance] processes."[344] Such requirements could be particularly relevant for digital microcredit. Product-governance rules could require that both the design process and customer acquisition plans for digital microcredit ensure that potential harms and risks to consumers are considered and mitigated. For example, digital microcredit providers could be required to strengthen customer segmentation[345] and to target and sell only those digital microcredit products that are suitable and appropriate for the interests, objectives, and characteristics of target segments.[346] Prelaunch reviews of digital credit products also provide an opportunity to examine potential consumer risks and internal measures to prevent or mitigate such risks. Digital lenders in Ghana are required to present and demonstrate their product, the identified risks, and risk-mitigation strategies to a panel at the Bank of Ghana for assessment and approval.[347] In extreme cases, regulators could also leverage product intervention powers. In Australia, ASIC has employed its product intervention powers to ban a specific model of short-term lending found to cause significant consumer detriment.[348]

Regulation on pricing has been employed in some countries, but policy makers should be cautious and judicious in utilizing such approaches, given the potential to hamper market growth and access to finance. Regulation on pricing can take various forms. A principles-based approach could focus on requiring that pricing practices for digital microcredit be responsible and reasonable.[349] Some countries have been more prescriptive—for example, by capping the amount that providers can charge for late fees or capping interest rates altogether for short-term, high-cost consumer credit. In the United Kingdom, research was conducted to determine appropriate price caps that would make it unprofitable for providers to lend to those consumers who would be worst harmed by high-cost, short-term credit. The resulting price cap formulation consists of three elements: (1) interest rate and fees cannot exceed 0.8 percent per day on the outstanding principal; (2) default fees are capped at £15; and (3) a total cost cap was put in place taking into account all fees, charges and interest, which cannot exceed 100 percent of the amount borrowed.[350]

Specific measures could be taken to limit rollovers and multiple borrowing in order to decrease the risk of over-indebtedness. Policy measures that have been utilized for short-term, high-cost credit and could be applied to digital microcredit include imposing a limit of two rollovers for short-term, high-cost credit (United Kingdom);[351] staggering interest rate caps on short-term loans with a cap of 5 percent per month on the first loan in a calendar year and 3 percent for all subsequent loans, specifically to address roll-over abuse (South Africa);[352] or prohibiting charging an establishment fee if credit is used to refinance another small credit contract (Australia).[353] Where loan terms are extended automatically due to missed payments, such an extension should be clearly communicated in advance to consumers, with clear disclosure on related costs. In addition, in Australia, there is a (rebuttable) presumption of unsuitability if a consumer either is in default under another small credit contract or has had two or more other such loans in the previous 90 days. Digital microcredit providers could also be required to monitor actively levels of over-indebtedness and report such information to regulators. The Center for Financial Inclusion suggests that providers have a working definition of client over-indebtedness and that staff monitor portfolio quality at least monthly to identify areas with high risks of over-indebtedness. Such monitoring could apply particularly for those loans internally designated as "lend-to-learn" digital loans.

More broadly, policy makers should ensure that rules on fair T&C apply to digital microcredit. The ITU-T Focus Group on Digital Financial Services suggests that regulators review digital financial service providers' contracts with customers on a regular basis for unconscionable and unfair terms and practices that should be banned, and that regulators publish examples of such terms and practices to raise public awareness.[354] For example, auto-deduction of loan repayments from mobile wallets could be considered unfair unless consumers are given a clear choice to actively opt in.

On a broader level, policy makers could take steps to monitor levels of over-indebtedness with respect to consumer credit, including digital microcredit, on an ongoing basis. This will require obtaining data from all credit providers in order to have a comprehensive overview of the market. Such data can be obtained from both supply-side sources as well as demand-side sources, including via household surveys. Metrics and indicators will also need to be developed in order to define and track over-indebtedness levels.[355]

Existing rules on debt collection and/or data privacy should be applied to digital lenders, with adaptations to address abusive practices specific to digital microcredit. Greater clarity and specificity may be needed regarding what are considered abusive and inappropriate debt collection practices to ensure respectful treatment of borrowers of digital microcredit and appropriate protection of borrowers' rights to privacy and dignity. For example, in the Philippines, the National Privacy Commission issued a circular in 2020 that prohibits lenders operating online apps on smartphones from harvesting personal information, such as phone and social media contact lists, for debt collection purposes.[356]

4.5 ALGORITHMIC SCORING

a) Risks to consumers

New and complex algorithms that rely on big data, AI, and machine learning[357] are being utilized to provide digital credit.[358] Big data analytics are one of the core innovations driving digital credit (along with many other fintech innovations). Even low-income consumers now have digital footprints associated with them, potentially drawing from an array of alternative data from sources such as social media, mobile phone usage, internet transactions and geolocation data.[359] Digital credit providers are developing and utilizing algorithmic processing to analyze huge data sets covering a wide range of characteristics for predictive purposes, such as the likelihood of default and future repayment behavior. Such tools allow providers to assess vast numbers of potential borrowers rapidly, with little to no human interaction, expanding access to credit for large numbers of consumers, in particular those lacking formal credit histories.

Use of algorithms can give the semblance of objective, data-driven analysis, but still pose risks to consumers. Such analytics have introduced new manifestations of fair lending and data privacy risks, as algorithms can potentially be embedded with or result in biased results. "Automated decision systems are not built and used in a vacuum: humans classify what data should be collected to be used in automated decision systems, collect the data, determine the goals and uses of the systems, decide how to train and evaluate the performance of the systems, and ultimately act on the decisions and assessments made by the systems."[360]

Biased outcomes that negatively discriminate may potentially arise due to multiple factors. The original design of an algorithm itself can incorporate bias. However, even where the design of an algorithm itself is not problematic, results may still be biased due to the input data used to develop automated scoring systems. Input data may be incomplete and unrepresentative (resulting in erroneous scoring) or reflect historical bias (influencing the algorithm toward biased results). Input data may also be poorly weighted, overemphasizing certain inputs. When such data is used to train algorithms, the predictions emanating from such models may be systematically worse for certain groups and perpetuate existing social inequalities. Such effects continue in a feedback loop as a biased algorithm learns and reinforces its own bias. As highlighted in the 2019 WBG/International Committee on Credit Reporting (ICCR) guidelines on credit scoring approaches: "A well-intentioned algorithm may inadvertently make biased decisions that may discriminate against protected groups of consumers. For example, if there are limitations in the data used for model development, selection bias may occur. If there are limitations in the methodology used to develop the models, then statistical bias may occur. If historical data are used where social bias was prominent, the algorithm may enforce and amplify the social bias (for example, penalizing along racial lines)."[361]

The results of algorithmic processing can be discriminatory based on sensitive attributes. Even assuming that input data is not flawed, algorithms may be applied in a manner where information serves as a proxy for sensitive attributes. For example, information such as zip codes or social media contacts may be highly correlated with sensitive and protected attributes, such as race, ethnicity, or gender. As a result, potential customers may be unfairly discriminated against based (indirectly) on protected attributes as opposed to being evaluated based on their own merits.

There is a lack of transparency regarding the application of algorithms for regulators. Algorithms are often called "black boxes" and are considered proprietary by providers. Regulators lack both transparency into the operation of algorithms and the technical expertise to evaluate such systems. Providers themselves may be unaware of how algorithms work when they are purchased from third parties. As noted in the WBG/ICCR guidelines on credit scoring approaches: "[T]he opaqueness of innovative algorithms may raise concerns. When innovative algorithms are used to assign credit scores to make credit decisions, providing consumers, auditors, and supervisors with an explanation of a credit score and resulting credit decision if challenged is generally more difficult."[362] Challenges in the ability to interpret model inputs, modelling logic, and post-modeling results in turn make it more difficult to mitigate the potential risk of bias and discrimination.

Consumers may not be aware of the role of algorithmic processing when credit is denied. They may be unaware of what factors led to their denial of credit. And even when consumers are aware of the use of algorithmic scoring, there may be little action that they can take to address their concerns. While laws such as the US Fair Credit Reporting Act give consumers who are denied credit the right to know what factors were used to make this decision, it is unclear how such rights translate in the case of algorithmic processing. Consumers are therefore left in the dark, unable to correct any potential errors or understand how to improve their credit scores based on algorithms.

b) Regulatory approaches

There is a limited but growing body of research with suggested approaches to address risks to consumers that arise from the use of algorithms. The following section summarizes emerging regulatory approaches that could be considered by policy makers. It draws from both measures related to general use of algorithmic processing as well as measures specific to big data analytics and algorithmic credit scoring in the financial sector.[363] Complementary measures will also be needed on the demand side (such as algorithmic literacy) and the supply side (such as industry standards for algorithms and self-regulation).

As an initial step, the application of fair treatment and nondiscrimination rules to algorithms and algorithmic processing may need to be clarified and strengthened. As noted by the Global Partnership for Financial Inclusion: "Policymakers and industry participants should adopt measures to ensure that… scoring models developed using alternative data do not unfairly discriminate against protected groups. The use of alternative data that carries forward historical discrimination is either prohibited or restricted."[364] One of the high-level policy recommendations from the WBG/ICCR guidelines on credit scoring approaches is that the decisions made on the basis of credit scoring should be explainable, transparent, and fair, in particular including that "the data used, and the decisions made on the basis of credit scoring, should operate within equal opportunity or anti-discrimination laws."[365] Where rules are in place on fair treatment and nondiscrimination for sensitive categories, policy makers may need to clarify and strengthen the application of these rules to algorithmic scoring. For example, the Hong Kong Monetary Authority issued a set of guiding principles on consumer protection with respect to use of big data analytics and AI specifically by banking institutions, focusing on four main areas: (1) governance and accountability, (2) fairness, (3) transparency and disclosure, and (4) data privacy and protection. The guiding principles specifically notes that institutions should ensure that big data analytics and AI models produce fair outcomes that comply with applicable laws, including those related to discrimination.[366]

Algorithmic accountability refers to the assignment of responsibility for how an algorithm is created and its impact on society.[367] As noted above, algorithms are both complex and proprietary, and directly regulating the actual design of algorithms may be neither practical nor feasible. Therefore, a commonly suggested approach is to place greater emphasis and responsibility on the deployers of algorithms (in this case, digital microcredit providers) regarding the processes by which algorithms are designed and utilized, and to require that potential harms arising from algorithmic systems are identified, assessed, documented, and minimized.

Algorithmic accountability centers on principles such as fairness, explainability, auditability, responsibility, and accuracy.[368] Policy makers could reflect such principles of algorithmic accountability in regulatory frameworks and provide guidelines for achieving these principles. As noted by the G20 Task Force, policy makers should ensure that providers have "robust and transparent governance, accountability, risk management and control systems relating to use of digital capabilities (such as AI, algorithms and machine learning technology). This includes ensuring that the methodology of algorithms underpinning digital financial services (e.g., digital financial advice) is clear, transparent, explainable and free from unlawful and exclusionary biases, and with options for recourse where necessary."[369] For example, the guidance on big data analytics and AI from the Hong Kong Monetary Authority requires banking institutions to ensure that there is an "appropriate governance, oversight and accountability framework which is established and documented," "appropriate level of explainability of the [big data analytics and AI] models," and proper validation and ongoing reviews to ensure the reliability, fairness, accuracy, and relevance of the models, data used, and results.[370] The EBA recently introduced guidelines on loan origination and monitoring that require financial institutions employing technology-enabled innovations for credit-granting purposes to ensure the traceability, auditability, and robustness and resilience of such models.[371]

The WBG/ICCR guidelines on credit scoring approaches recommend that credit scoring models using traditional and innovative techniques be subject to a model governance framework. An effective model governance framework should consider the following items (among others):[372]

- Management of model risk, including the conceptual soundness of the model.

- Assessment of unintended consequences, such as cascading risks and the disregard of protected characteristics (for example, race, gender, and religion).
- Model ownership within a business context.
- Regular reviews and back-testing of models, including validation of model performance, such as receiver-operator-characteristics curves and/or precision-recall curves.

Operationalizing the principles of algorithmic accountability requires that appropriate procedures, controls, and safeguards be put in place during the development, testing, and deployment of algorithms to ensure fairness and accuracy. For example, deployers (and, by extension, any entities to which development of algorithmic scoring is outsourced) could be required to establish clear strategies to avoid creating or reinforcing unfair bias in AI systems. Processes could be required to test and monitor for potential bias during the development, testing, and deployment stages. Methods that can be employed include impact assessments, error testing, and bias testing.[373] More broadly, incorporating inclusive design principles and diverse, cross-functional work teams can also be beneficial. Practical examples of actions that have been suggested in the international literature include the following: [374]

- Assess possible limitations stemming from the composition of training data.
- Consider the diversity, representativeness, and reliability of training data.
- Identify for which groups there is the greatest concern regarding training-data errors, disparate treatment, and impact, and test for specific groups or problematic use cases.
- Assess whether possible decision variability can occur under the same conditions and, if so, what the possible causes of this are.
- Ensure that an adequate working definition of fairness is applied in designing AI systems, and that metrics are used to measure and test the applied definition of fairness.
- Determine how potential bias will be detected.
- Determine how and when the algorithm will be tested and who the targets will be.
- Determine the threshold for measuring and correcting for bias in the algorithm.
- Identify potential bad outcomes and what steps will be taken if bad outcomes are predicted to arise from the deployment of the algorithms.

For example, the EBA guidelines on loan origination and monitoring require that when using automated models for creditworthiness assessment and credit decision-making, financial institutions should have in place internal policies and procedures to detect and prevent bias and ensure the quality of input data. Financial institutions should also have internal policies and procedures to ensure that the quality of model outputs is regularly assessed, including back-testing the performance of the model, and control mechanisms, model overrides, and escalation procedures within the credit decision-making framework, including qualitative risk-assessment tools and quantitative limits.[375]

In order to ensure auditability and explainability, the controls and safeguards noted above will need to be documented well. In the case of automated credit scoring, providers could be required to document the rationale for algorithms, the variables used in such algorithms, and the justification for using such variables. The process of assessing matters such as training data, decision variability and testing for bias, identifying areas for improvement, and implementing corrective action could all be required to be documented as well. For example, the EBA guidelines on loan origination and monitoring require institutions to have adequate documentation of automated credit scoring models that covers methodology, assumptions, and data inputs; an approach to detecting and preventing bias and ensuring the quality of input data; and the use of model outputs in the decision-making process and the monitoring of these automated decisions on the overall quality of the portfolio or products in which these models are used.[376]

Where digital credit providers outsource algorithm development to third parties, providers could be required to ensure that appropriate controls were used by developers during the development process. Outsourcing of algorithmic scoring processes to third parties should not absolve digital credit providers of all responsibility. For example, the European Central Bank notes that, where a provider uses credit scores provided by a third-party vendor using alternative data sources and credit scoring methodologies, authorities should assess the capacity of the provider to understand the credit scoring process and data sources and to audit the outsourced credit scoring activities.[377] Providers could also be made directly responsible for regular testing and monitoring for bias during the ongoing deployment of the algorithm.[378]

Algorithmic systems could be required to undergo regular auditing and assessments by external experts.[379] Assessments would evaluate input data, training data, design and testing processes, decision factors, and output

decisions for potential negative impacts.[380] Assessments could involve running algorithmic systems through testing of hypothetical scenarios. Assessments could identify, assess, and document potential negative impacts and suggest appropriate risk-mitigation measures to address any flaws found. For example, a draft data privacy bill in the United States (the Consumer Online Privacy Rights Act) requires that entities engaging in algorithmic decision-making to facilitate credit opportunities annually conduct an impact assessment (by either an external, independent auditor or researcher) that:

- Describes and evaluates the development of the entity's algorithmic decision-making processes, including the design and training data used to develop the algorithmic decision-making process and how the algorithmic decision-making process was tested for accuracy, fairness, bias, and discrimination; and
- Assesses whether the algorithmic decision-making system produces discriminatory results on the basis of an individual's or class of individuals' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income, or disability.[381]

Similarly, a draft bill before the US Congress (the Algorithmic Accountability Act)[382] requires entities to conduct impact assessments on high-risk automated decision systems in order to evaluate the impact of the system's design process and training data on accuracy, fairness, bias, discrimination, privacy, and security. Supervisors can also play a role in evaluating the use of algorithms by digital credit providers. FinCoNet suggests that supervisors evaluate whether automated creditworthiness assessment based on big data and AI are leading to responsible lending decisions.[383]

At a minimum, consumers could be given a clear right to know when they are subject to automated decision-making that uses algorithms. The WBG/ICCR guidelines on credit scoring approaches recommend that consumers receive information on the data used and the decisions made on the basis of a credit scoring method. "The focus should, however, not be on the direct or indirect disclosure of the algorithm, but rather on the rationale behind the credit risks decision."[384] In order to ensure fair and transparent processing, the European Union's GDPR requires that data controllers provide consumers with information on "the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject."[385] In particular, consumers could be informed about any adverse action taken against them based on automated decision-making and the key characteristics that led to such decision.[386] For example, financial institutions in Portugal are explicitly required to inform bank customers of situations where their creditworthiness assessments rely exclusively on automated decision-making processes, particularly AI models, in order to allow customers in such situations to exercise their rights under the GDPR.[387]

In addition, consumers could be empowered with further rights, in particular the right to challenge the outcome of automatic decision-making and the right to request human intervention. Consumers could have the right to request why automated decisions were made and to know the logic involved in the automatic processing of data concerning them. Providers could be required to provide consumers with meaningful information "to enable those adversely affected by an AI system to challenge its outcome based on plain and easy-to-understand information on the factors, and the logic that served as the basis for the prediction, recommendation or decision."[388] The WBG/ICCR guidelines on credit scoring approaches suggest that "organizations should consider providing the data subjects with an avenue to request a review of decisions that were fully automated and a correction of underlying inaccurate data (if this resulted in their credit score being impacted)."[389]

Consumers could also be given the right not to be subject to a decision based solely on automated decision-making. For example, the GDPR provides consumers with the right "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[390] The G20 Task Force similarly states that providers using automated credit scoring models should provide for human intervention, where appropriate, to mitigate against inappropriate outcomes such as automatic refusals.[391]

4.6 GAPS IN THE REGULATORY PERIMETER

a) Risks to consumers

Most countries face gaps in regulatory authority or coverage for certain digital credit products or providers. As noted in chapter 3, fintech products in general raise a range of issues related to regulatory gaps due to the novelty of the product as well as new types of providers. With respect to digital microcredit, a mix of regulated, semi-regulated, and unregulated providers often

offer similar products to similar consumer segments but operate under different legal requirements. A particular challenge posed by digital microcredit is the small but increasing numbers of app-based lenders that do not fall under the authority of any regulatory body (and may even be based outside the country). For example, research in Kenya shows that the usage of non-regulated digital credit has grown from 0.6 percent in 2016 to 8.3 percent in 2019.[392] Where consumer protection rules for credit do exist, they are often more developed for regulated, deposit-taking institutions. Weaker rules (and quite often, weaker supervision) exist for non-bank lenders where regulated, while unregulated lenders have no rules applied to them. At the same time, research suggests that some of the more irresponsible practices highlighted in this chapter are more common among app-based lenders, as evidenced by the significantly higher levels of non-performing loans for app-based lenders compared to other digital microcredit providers.[393] In addition, some FCP frameworks explicitly do not apply to small value loans. The result is an unlevel playing field and increased risks to consumers, as well as increased potential for fraud.

b) Regulatory approaches

As noted in chapter 3, an activity-based framework should ideally be put in place for digital credit, ensuring comprehensive protection for consumers and a level playing field for the market. Regulating by activity rather than by institutional form would cover all models of digital credit, regardless of whether digital credit is provided via banks, MNOs, non-bank lenders, or some combination of these actors in partnership. Concerns regarding regulatory arbitrage would also be diminished. For example, all providers of consumer credit are regulated in Australia and Portugal. However, such an approach would require the licensing of all credit providers, which may represent a significant undertaking for financial sector authorities.[394]

Where app-based lenders are based overseas, cross-border coordination between authorities will be necessary, such as via sharing information, redirecting consumer complaints to competent authorities, and promoting consistent policy approaches.[395] From a legal perspective, to support more effective regulation and supervision of cross-border activity, it may also be necessary to apply a country's FCP requirements (and regulators' mandates) to any fintech entities dealing with consumers in that country, regardless of where the providers are based.

Where an activity-based approach is not feasible, policy makers could be pragmatic and opportunistic, building off of what rules and regulatory powers do exist in order to ensure coverage of non-bank digital microcredit providers. For example, the broader powers of general consumer protection or competition authorities could be employed to introduce consumer protection rules on specified elements of digital credit. An example is the case of Kenya, where the CAK has issued rules on disclosure for digital credit that apply for all providers, including those not regulated by financial sector authorities.[396] Another is the Philippines, where the data privacy authority issued rules restricting use of mobile phone and social media data for debt collection purposes.[397] Another approach could be to introduce consumer protections via telecommunications authorities when MNOs and mobile channels are utilized or via mobile money regulation where digital credit models are linked to mobile wallets. While none of these approaches is necessarily ideal (and may raise difficulties in ongoing monitoring and enforcement), they can at least be leveraged to make incremental progress in putting in place protections for consumers. Where such approaches are employed, close coordination will be necessary between sectoral authorities.[398]

Complementary measures could be pursued that go beyond regulation, including where regulation may not be feasible for a variety of reasons, such as encouraging industry standards or codes of conduct. In Kenya, the Digital Lenders Association of Kenya has developed a code of conduct for digital lenders focused on consumer protection in an effort to address irresponsible behaviors seen in the market.[399] Similarly, the three fintech associations in Indonesia have developed a joint code of conduct. However, it is estimated that only one-third of digital lenders in Kenya are members of the Digital Lenders Association of Kenya, and there may be issues with self-selection of membership by lenders who are already more committed to responsible behavior. While codes of conduct are not a substitute for regulation, they can still be beneficial in establishing industry consensus regarding acceptable practices. In order to strengthen codes of conduct, policy makers can make membership in associations mandatory and encourage strong self-enforcement mechanisms.[400] In some countries, codes of conduct also allow consumers to bring disputes to financial sector ombudsmen or to court.

To address the specific issue of app-based lenders, platform operators themselves may have a role to play in ensuring appropriate behavior (and/or banning egregious practices). Given the important role that platforms now play in serving as an interface between consumers and hundreds of thousands of apps, the Federal Trade Commission in the United States has suggested that platforms should play a role in promoting best practices among app developers with respect to data pri-

vacy by requiring that platform operators make privacy disclosures, reasonably enforce these requirements, and educate app developers.[401] The same principles could be extended to other topics specific to financial services and digital credit. In August 2019, Google Play published new policies on its Developer Policy Center aimed at preventing predatory lending apps on its platform.[402] Google's stated policies already banned apps from exposing users to "deceptive or harmful" financial services but now include further details specifying that apps for personal loans must disclose metrics such as APR and TCC, banning apps that promote short-term loans of less than 60 days, and banning apps in the United States that have an APR higher than 36 percent (in accordance with US rules).

In order to be effective, stronger enforcement of platform policies will be needed. While Google Play's new policies on personal loan apps are potentially a useful step forward, it is currently unclear to what extent such policies are being monitored and enforced. Many lending apps on Google Play still appear not to abide by these new policies.[403] This may indicate that reliance on commercial arrangements policed by platform operators alone is insufficient and that further regulatory action is needed. Regulators may still need to work with platform operators in supervising and enforcing platform requirements.

Regulators will still need to work directly with platforms to address fraudulent lending apps. Issues with fraud extend beyond the traditional discussion about FCP, as they do not relate to poor practices by providers but involve outright fraud, such as soliciting application fees or personal data without providing a loan. Such situations should be addressed directly. In markets such as Kenya and Indonesia (and presumably others), there appears to be a high prevalence of fraudulent lending apps. When removed from platforms, the same developers often come back with new apps. National authorities should monitor such activities and work closely with platforms to address them, preferably with longer-term solutions to ban fraudulent developers. For example, in Indonesia OJK is working directly with Google to request removal of unlicensed online lending apps from Google Play.[404]

New research suggests that ex-ante vetting of finance-related apps, ex-post monitoring, and demand-side interventions can be beneficial.[405] There appear to be common red flags that can be observed regarding fraudulent app-based lenders, including a lack of valid e-mail addresses or a provider website for app developers and similarities in the metadata for fraudulent apps (for example, icons, titles, descriptions). New requirements could be put in place to screen for such red flags before apps are approved for inclusion in app stores. In addition, closer monitoring and reporting of data on mobile apps could be utilized to identify and take swifter action against fraudulent apps. Demand-side efforts such as financial literacy and "buyer beware" labeling could also be beneficial.

NOTES

253 Izaguirre, Mazer, and Graham, "Digital Credit Market Monitoring."
254 Reynolds et al., "Review of Digital Credit Products."
255 Kaffenberger and Chege, "Digital Credit in Kenya."
256 Reynolds et al., "Review of Digital Credit Products."
257 Blechman, "Mobile Credit," and AFI. 2017. AFI, "Digitally Delivered Credit: Consumer Protection Issues."
258 FSD Kenya, "Tech-Enabled Lending in Africa."
259 Kaffenberger and Totolo, *Digital Credit Revolution*.
260 Kaffenberger and Totolo, *Digital Credit Revolution*.
261 MicroSave, "Making Digital Credit Truly Responsible."
262 Izaguirre, Kaffenberger, and Mazer, "It's Time."
263 Kaffenberger and Totolo, *Digital Credit Revolution*.
264 Thirty one percent of respondents selected limited disclosure of costs as the main market conduct and consumer protection issue, followed by high costs of digital credit (14 percent), limited suitability and misleading advertising (14 percent), and data security and privacy (12 percent). See AFI, "Digitally Delivered Credit: Policy Guidance Note."
265 Busara Center for Behavioral Economics, *Pricing Transparency*.
266 As APR can be somewhat misleading for very short-term credit, an alternative approach is to allow for the presentation of monthly APR. This approach was taken in the Philippines, where banks were allowed to express effective interest rate (EIR) as a monthly rate for loans with contractual interest rates stated on a monthly basis. See Circular No. 730 of July 2011.
267 EC, *Behavioral Study on Digitalisation*.
268 Mazer, Vancel, and Keyman, "Finding 'Win-Win.'"
269 BdP Circular Letter No. CC/2020/00000044 on best practices applicable to the selling of retail banking products and services through digital channels.
270 BdP Circular Letter No. CC/2018/00000004 on best practices applicable to the selling of retail banking products and services through digital channels.

271 FinCoNet, *Guidance to Supervisors on Digitalisation.*
272 Guidelines on Advertising Financial Services, Bank of Lithuania, 2012.
273 Based on World Bank phone conversation with digital credit provider.
274 ASIC, *Facilitating Digital Financial Services Disclosures.*
275 Busara Center for Behavioral Economics, *Pricing Transparency.*
276 ITU-T Focus Group on Digital Financial Services, *Main Recommendations.*
277 OECD, *Short-Term Consumer Credit.*
278 https://www.fca.org.uk/publications/discussion-papers/smarter-consumer-communications-further-step-journey.
279 BdP Circular Letter No. CC/2020/00000044 on best practices applicable to the selling of retail banking products and services through digital channels.
280 EC, *Behavioral Study on Digitalisation.*
281 Busara Center for Behavioral Economics, *Pricing Transparency.*
282 FCA, *Feedback Statement FS16/10.*
283 The Smart Campaign, "Standards of Protection."
284 BdP Circular Letter No. CC/2020/00000044 on best practices applicable to the selling of retail banking products and services through digital channels.
285 FCA, *Feedback Statement FS16/10.*
286 ASIC, *Facilitating Digital Financial Services Disclosures.*
287 ITU-T Focus Group on Digital Financial Services, *Main Recommendations.*
288 Based on World Bank conversation with Competition Authority of Kenya. The guidelines apply to financial services conducted through SIM cards, USSD, and apps.
289 Mazer, "Does Transparency Matter."
290 Mazer, Vancel, and Keyman, "Finding 'Win-Win.'"
291 BdP Circular Letter No. CC/2020/00000044 on best practices applicable to the selling of retail banking products and services through digital channels.
292 Mazer, Vancel, and Keyman, "Finding 'Win-Win.'" Subsequent to this study, the digital credit provider in the study has since integrated research insights into its new USSD menus, including (1) separating finance charges from principal, (2) adding a line showing loan fees as a percentage, (3) adding a separate screen with late payment penalties, and (4) creating active choice to view terms and conditions.
293 The Smart Campaign, "Standards of Protection."
294 FCA, *Message Received?*
295 "Of the 21 products with clear information, 16 products had a warning system in place to remind borrowers about repaying their loans or about imminent default. Most of the time these reminders were sent via SMS, email, or app notification, either on the payment due date or up to seven days prior… Forty-seven products had no clear indication that any warnings were sent to the borrower, and five products did not send out notifications at all." See Reynolds et al., "Review of Digital Credit Products."
296 The Smart Campaign, "Standards of Protection."
297 ASIC, *Facilitating Digital Financial Services Disclosures.*
298 For further information, see McKee et al., "Doing Digital Finance Right," and Chen, Fiorillo, and Hanouch, "Smartphones & Mobile Money."
299 G20/OECD Task Force on Financial Consumer Protection, *Financial Consumer Protection Policy Approaches.*
300 For example, see FCA's review of practices for high-cost credit at https://www.fca.org.uk/firms/high-cost-credit-consumer-credit/high-cost-credit-review.
301 Central Bank of Kenya, *2016 FinAccess Household Survey.*
302 Mazer and McKee, "Consumer Protection in Digital Credit."
303 The study found that 20 percent of consumers who had taken out credit were actively prompted by the digital application system to indicate a higher income. See FinCoNet, *Report on Digitalisation.*
304 FinCoNet, *Report on Digitalisation.*
305 EC, *Behavioral Study on Digitalisation.*
306 OECD, *Recommendation of the Council on Consumer Protection.*
307 EC, *Behavioral Study on Digitalisation.*
308 FinCoNet, *Guidance to Supervisors on Digitalisation.*
309 All examples from OECD, *Short-Term Consumer Credit.*
310 FinCoNet, *Guidance to Supervisors on Digitalisation.*
311 The Smart Campaign, "Standards of Protection."
312 Consumer Rights Protection Law (Latvia), art. 2.1.
313 Consumer Credit Act 1991 (Belgium), art. 6.
314 Committee of Advertising Practice, "Trivialisation in Short-Term High-Cost Credit Advertisements."
315 BdP Circular Letter No. CC/2020/00000044 on best practices applicable to the selling of retail banking products and services through digital channels.
316 EC, *Behavioral Study on Digitalisation.*
317 FinCoNet, *Guidance to Supervisors on Digitalisation.*
318 Circular SB. SG. No. 00065/2015.
319 For example, the EU Consumer Rights Directive (Directive 2011/83/EU) provides a 14-day cooling-off period for purchases made online or through other types of distance selling.

320 FinCoNet, *Guidance to Supervisors on Digitalisation.*
321 BdP Circular Letter No. CC/2020/00000044 on best practices applicable to the selling of retail banking products and services through digital channels.
322 Directive 2002/65/EC on distance marketing of consumer financial services.
323 See section 3.1 for further discussion on the limitations of the consent-based approach with respect to data privacy, which has similar relevance here.
324 For further information, see FinCoNet, *Guidance to Supervisors on Setting of Standards.*
325 EC, *Behavioral Study on Digitalisation.*
326 Unfair lending can encompass a range of potential issues. This section focuses on issues related to predatory pricing, irresponsible lending, and abusive collections. Discrimination due to the use of algorithmic scoring is discussed separately in section 4.5, given the more cutting-edge nature of the topic and its broader applicability (within and beyond the financial sector).
327 AFI, "Digitally Delivered Credit: Consumer Protection Issues."
328 Kaffenberger and Chege, "Digital Credit in Kenya."
329 The fair lending risks that arise from algorithmic scoring are discussed separately in section 4.5.
330 AFI, "Digitally Delivered Credit: Consumer Protection Issues." Similarly, research in Tanzania showed that first-time borrowers of digital microloans had the highest default rate, nearly 40 percent. See Izaguirre and Mazer, "How Regulators Can Foster."
331 Reynolds et al., "Review of Digital Credit Products."
332 Guzman, "SEC to Shut Down Eight More Online Lending Apps."
333 OECD, *Recommendation of the Council on Consumer Protection.*
334 OECD, *Recommendation of the Council on Consumer Protection.*
335 Consumer Credit Act. More broadly, the EU Consumer Credit Directive (Directive 2008/48/EC) requires that creditors assess a consumer's creditworthiness before the conclusion of a credit agreement. Details on how member states have implemented this requirement can be found at https://ec.europa.eu/info/sites/info/files/mapping_national_approaches_creditworthiness_assessment.pdf.
336 National Credit Act 2005 (South Africa), Part D.
337 Money Lending Business Act 1983 (Japan), art. 13-2.
338 National Consumer Credit Protection Act 2009 (Cth) (Australia), s. 28S. This cap applies to consumers who receive at least 50 percent of their gross income as payments under the Social Security Act 1991 (Cth) (Australia).
339 Notice of Banco de Portugal No. 4/2017 (Portugal).
340 EBA, *Final Report on Guidelines.*
341 EBA, *Final Report on Guidelines*, s. 4.3.3 (53).
342 FinCoNet, *Guidance to Supervisors on Digitalisation.*
343 For example, Australian product design and distribution governance rules originally were not envisaged to apply to credit products on the basis that existing requirements under credit legislation, such as responsible lending obligations, were sufficient to address relevant consumer issues. However, this position was subsequently reversed. See Boeddu and Grady, *Product Design and Distribution* and Corporations Amendment (Design and Distribution Obligations) Regulations 2019 (Australia).
344 EBA, *Second EBA Report.*
345 McKee et al., "Doing Digital Finance Right."
346 FinCoNet, *Guidance to Supervisors on Digitalisation.*
347 AFI, "Digitally Delivered Credit: Consumer Protection Issues."
348 In this business model, a short-term credit provider and its associate charged separate fees under separate contracts, thereby avoiding existing caps on fees. The combined fees added up to almost 1,000 percent of the loan amount. See ASIC Corporations (Product Intervention Order—Short Term Credit) Instrument 2019/917.
349 For example, the Smart Campaign's Standards of Protection for Digital Credit recommends that provider's fees are reasonable (for example, penalty, prepayment, other fees); that there is a reasonable limit when loan interest and/or fees (including arrears interest) stops accruing that is proportionate to loan tenure; that arrears interest/fees and penalties do not compound debt and are calculated based on principal amount only; and that due diligence is conducted on pricing of third-party partners whose charges or fees impact clients (for example, for payment and/or cash-in or cash-out services).
350 Detailed rules for the price cap on high-cost, short-term credit, including feedback on CP14/10 and final rules. Policy Statement PS14/16. Financial Conduct Authority, November 2014 https://www.fca.org.uk/publication/policy/ps14-16.pdf.
351 FCA Consumer Credit Sourcebook—November 2020 (UK), 6.7.23R.
352 Regulations on Review of Limitations on Fees and Interest Rates. Department of Trade and Industry, November 2015.
353 S. 31A(1A), National Consumer Credit Protection Act 2009.
354 ITU-T Focus Group on Digital Financial Services, *Main Recommendations.*
355 For example, see EFIN Working Group on Over-Indebtedness, *Indicators to Monitor Over-Indebtedness.*
356 NPC Circular No. 20-01 on Guidelines on the Processing of Personal Data for Loan-Related Transactions.
357 While precise definitions vary, on a conceptual basis, algorithms are a set of step-by-step instructions that computers follow to perform a task. Machine learning is a set of techniques and algorithms where multiple data sets, or training data, are used to train a program to recognize patterns in a set of data automatically. Artificial intelligence and automated decision systems are powered by algorithms and machine learning. See Lee et al., "Algorithmic Bias Detection." See also AI Now Institute, "Algorithmic Accountability Policy Toolkit."
358 Complex algorithmic processing is increasingly being used in multiple fintech applications (including P2P, insurtech, robo-advice, and so on), as well as in many circumstances far beyond the financial sector. This section focuses on risks arising from the use of algorithmic scoring for digital credit. Regulatory approaches to mitigate such risks are drawn from credit-related examples where possible, as well as more general examples.

359 For discussion on the data privacy risks for consumers related to use of alternative data and potential measures to address such risks, see section 3.1.
360 AI Now Institute, "Algorithmic Accountability Policy Toolkit."
361 World Bank Group and International Committee on Credit Reporting, *Credit Scoring Approaches Guidelines*.
362 World Bank Group and International Committee on Credit Reporting, *Credit Scoring Approaches Guidelines*.
363 Hong Kong Monetary Authority, *Consumer Protection*.
364 GPFI, *Data Protection and Privacy*.
365 World Bank Group and International Committee on Credit Reporting, *Credit Scoring Approaches Guidelines*.
366 Hong Kong Monetary Authority, *Consumer Protection*.
367 Caplan et al., *Algorithmic Accountability*.
368 https://www.fatml.org/resources/principles-for-accountable-algorithms.
369 OECD, *Financial Consumer Protection Policy Approaches*.
370 Hong Kong Monetary Authority, *Consumer Protection*.
371 EBA, *Final Report on Guidelines*.
372 World Bank Group and International Committee on Credit Reporting, *Credit Scoring Approaches Guidelines*.
373 Error analysis involves manual review, variance analysis (analyzing discrepancies between actual and planned behavior), and bias analysis. Bias analysis provides quantitative estimates of when, where, and why systematic errors occur, as well as scope of errors. See New and Castro, "How Policymakers Can Foster."
374 For further examples, see "Trustworthy AI Assessment List" in High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*. See also "Template of Bias Impact Statement" in Lee et al., "Algorithmic Bias Detection."
375 EBA, *Final Report on Guidelines*.
376 EBA, *Final Report on Guidelines*.
377 European Central Bank, *Guide to Assessments*.
378 The Smart Campaign, "Standards of Protection."
379 The intensity of policy approaches to algorithmic accountability should vary depending on the potential severity of consumer harm arising from particular uses of algorithms. For deployments of algorithms deemed lower risk, alternatives to more intensive impact assessments include third-party certification of algorithmic systems or a no-fault/strict liability regime to algorithmic decisions. See further discussion in European Parliamentary Research Service, *A Governance Framework*.
380 See G20/OECD Task Force on Financial Consumer Protection, *Effective Approaches*. *See* also Lee et al., "Algorithmic Bias Detection."
381 Bill on Consumer Online Privacy Rights Act, 116th Congress (December 2019), s. 2968.
382 Bill on Algorithmic Accountability Act, H.R. 2231, 116th Congress (April 2019), s. 1108.
383 FinCoNet, *Guidance to Supervisors on Digitalisation*.
384 World Bank Group and International Committee on Credit Reporting, *Credit Scoring Approaches Guidelines*.
385 GDPR, art. 13.
386 GPFI, *Data Protection and Privacy*.
387 BdP Circular Letter No. CC/2020/00000044 on best practices applicable to the selling of retail banking products and services through digital channels.
388 OECD, *Recommendation of the Council on Artificial Intelligence*.
389 World Bank Group and International Committee on Credit Reporting, *Credit Scoring Approaches Guidelines*.
390 GDPR, art. 22.
391 OECD, *Financial Consumer Protection Policy Approaches*.
392 FSD Kenya, *Digital Credit Audit Report*.
393 In Kenya, the rate of non-performing loans for digital loans from MNO-led banks and banks was 6 percent and 21 percent, respectively, while the rate for digital loans from app-based lenders was 29 percent. See MicroSave, "Where Credit Is Due."
394 An alternative approach would be to register at least all credit providers, as opposed to a full licensing regime.
395 G20/OECD Task Force on Financial Consumer Protection, *Effective Approaches*.
396 Based on World Bank conversation with Competition Authority of Kenya. The guidelines apply to financial services conducted through SIM cards, USSD, and apps.
397 NPC Circular No. 20-01 on Guidelines on the Processing of Personal Data for Loan-Related Transactions.
398 For example, in Tanzania, digital credit models may fall under the regulatory scope of the Ministry of Industries and Trade or the Bank of Tanzania. The Fair Competition Commission has been collaborating with both authorities via a memorandum of understanding in order to address financial consumer protection issues in the market.
399 https://www.dlak.co.ke/dlak-code-of-conduct.html.
400 For examples of good practices to strengthen the enforcement of codes of conduct, see Australian Competition and Consumer Commission, *Guidelines for Developing Effective Voluntary Industry Codes of Conduct*.
401 FTC, *Mobile Privacy Disclosures*.
402 https://play.google.com/about/restricted-content/financial-services/.
403 CGTN Africa, "Google Fails to Stamp Out Short-Term Payday Lending Apps."
404 Based on World Bank communication with OJK.
405 https://www.centerforfinancialinclusion.org/combating-the-rise-in-fraudulent-fintech-apps.

PEER-TO-PEER LENDING

5

PEER-TO-PEER LENDING

5.1 INTRODUCTION

Peer-to-peer lending is often described as one of the most significant developments in fintech, although its basic elements are not new. From a lending product perspective, consumer P2P loans are typically unsecured, amortizing loans, very similar to personal installment loans provided by traditional lenders such as banks and finance companies.[406] From an investment perspective, the concept of investing in loans made by another lender also is not new, given the range of arrangements—such as loan securitization—that have allowed third-party investment long before P2PL developed.

The key innovation represented by P2PL and facilitated by technology—specifically by online platforms—has been to give prospective borrowers, particularly consumer borrowers, access to potential lenders that they did not have before. As a result, it can offer alternative sources of funding for consumers to more traditional channels. Similarly, from a lender/investor perspective, and particularly from a consumer investor perspective, it has given consumers access to investment opportunities in loans that they formerly did not have.[407]

a) What is meant by peer-to-peer lending?

As with the concept of fintech, there is no single, widely accepted definition of the concept of P2PL. Even the term peer-to-peer lending is not consistently preferred internationally. Terms such as marketplace lending,[408] loan-based crowdfunding,[409] crowdlending,[410] and social lending[411] and, occasionally, combinations of these[412] are also used frequently.

The overarching idea of P2PL platforms has been described as providing an online market that allows lenders to trade directly with borrowers.[413] However, many models have developed in the market that go significantly beyond a pure matching model where prospective lenders can select prospective loans directly based on information provided to them.[414] In this chapter, P2PL is used to refer to the provision of credit facilitated by online platforms that match borrowers with lenders, encompassing a spectrum

- from platforms that facilitate consumers acting as direct lenders for individual loans to other consumers;
- through to platforms that allow consumers to invest in individual consumer loans or in pools or portfolios of loans indirectly, in a variety of ways that expose them to credit risk without being the lender of record.

As discussed later in the chapter, in some jurisdictions legislation now restricts P2PL activities to, or has caused them to converge around, only some models. It has also been the case that in some jurisdictions P2PL platforms have increasingly been backed by institutional lenders (to at least some extent thus moving away from the "peer-to-peer" element).

P2PL platforms offer various services for the purposes of matching lenders/investors with loan requests and concluding loan contracts. These can include, depending on the model, activities such as collecting and presenting applicant information, assessing loan applications, providing the contractual framework and mechanisms for entering into loan contracts, and setting loan pricing and selection. They also typically undertake loan-servicing

activities, such as collecting lenders/investors' funds for disbursement to borrowers, collecting repayments from borrowers to be repaid to lenders/investors, and dealing with loan defaults. Where a platform comprises more complex aspects, such as allowing investment in loan pools or portfolios, platform operators are typically also responsible for more complex loan selection, allocation, and pricing activities.

Characteristics of P2PL platforms vary significantly internationally and even within individual markets. In the United Kingdom the FCA, for example, recently sought to group platforms into three general categories: "conduit platforms" (where the lender/investor selects the loans they wish to invest in); "pricing platforms" (where the platform sets the price, but the lender/investor selects the loans); and "discretionary platforms" (where the platform sets the price and chooses the lender/investor's portfolio to generate a target rate). However, the FCA also noted that these platform types were neither exclusive nor exhaustive and that even single platforms could operate in multiple ways.[415]

In some P2PL models, individual "lenders" invest in specific loans through a platform operator or associated entity that in turn is the actual lender to the individual borrower. While such individual "lenders" are exposed to the credit risk of relevant loans, their role is strictly as investors in an interposed instrument or arrangement, such as a security or collective investment scheme. At a less technical level, it is often the case that even in platform models where individuals are lending directly, such lending is perceived as a form of "investment." Therefore, in this chapter the combined term *lender/investor* is generally used to refer to consumers (typically individuals) under either circumstance.

Given the variety in platform offerings and business models, there can be overlap between the concepts of P2PL and investment-based crowdfunding discussed in the next chapter. Platforms may potentially fall within both categories. P2PL as discussed in this chapter is generally concerned with the provision of ordinary loans (secured or otherwise) to finance recipients, rather than facilitation of investments in debt securities issued by finance recipients.

Entities responsible for operating P2PL platforms, or key aspects of such platforms, are referred to in the chapter as P2PL operators. Although a single entity frequently has operational and legal control over a platform, some P2PL arrangements comprise different entities operating key aspects of the arrangement or providing key services to consumers.

b) Importance of effective financial consumer protection for P2PL

P2PL grew rapidly internationally, and in recent years lending volumes, while still representing a fraction of global consumer lending, have been significant. In 2018, consumer P2PL represented the largest online alternative finance model by market segmentation, facilitating $195.29 billion in lending transactions volume, or 64 percent of the total global volume for the alternative finance industry.[416] China, for example, saw a rapid expansion of its P2PL market from 2013, which at its peak reportedly comprised around 6,000 platforms.[417] P2PL in China attracted significant numbers of ordinary investors reportedly due to such factors as tightening of bank lending, a growing perception of P2PL as a good investment opportunity, and, notably, a then lack of regulatory requirements and oversight.[418] Chinese investors were perceived to have been attracted by P2PL as they had very limited investment options.[419] Although pre-COVID-19 fintech credit volumes (comprising P2PL consumer lending, among other platform-based lending) were found to have declined in China and to have plateaued in the United States and United Kingdom, they were continuing to grow in a range of other jurisdictions, and fintech lenders were becoming economically significant lenders for specific segments, such as small and medium-sized enterprises.[420]

The growth of P2PL has also seen major platform collapses and other concerning incidents in a variety of jurisdictions, highlighting the importance of identifying and addressing new and increased risks for consumers, whether as lenders/investors or borrowers. Some of these developments—and their adverse impacts on consumers—have been widely reported in the media. They have also triggered significant regulatory responses in many jurisdictions. It is thus unsurprising that in a recent survey of regulators, fraud was ranked as the top risk in connection with P2PL.[421] The peak of P2PL in China was followed by a number of significant platform collapses and incidents of fraud and misconduct involving platform operators. One of the highest-profile incidents of fraud involved a platform ultimately found to be a Ponzi scheme (most of its loan listings were fraudulent), causing almost 900,000 individual lenders/investors to lose the equivalent of $7.6 billion.[422] This was by no means an isolated incident.[423] Extensive platform failures resulted in major financial losses for many consumers. Many lost their savings as a result; severe financial and personal impacts were reported in the media.[424] Following significant reforms by regulators (which, as discussed later in the chapter, some commentators now argue may have gone too far), the number of P2PL platforms in China reportedly recently dropped to as few as 29 from a peak of about 6,000.[425]

The United Kingdom's P2PL market has also seen a significant toughening of regulations, following a run of high-profile problems and continuing concerns. The market experienced various platform collapses and other problems affecting platform performance, with corresponding losses, said to be due to factors such as a lack of credit expertise of some participants.[426] As a result, the British regulator's attitude has toughened toward P2PL. In 2013, when developing its initial framework for P2PL regulation, the FCA expressed the view that P2PL was a less risky proposition for consumers than investment-based crowdfunding.[427] However, its views have since hardened, and it recently highlighted how the complexities of P2PL drove a need for measures such as sophisticated risk management and controls.[428]

From a borrower's perspective, there have been media reports in Indonesia of deeply concerning incidents affecting individuals who have borrowed from unlicensed P2P lenders, and the COVID-19 crisis may have worsened these impacts. The incidents include instances of harsh debt collection practices, even driving borrowers to take their own life, although such problems are not confined to P2PL but extend to unregulated online lending more broadly.[429] Recent reports in the context of the COVID-19 crisis indicate that P2P lenders/investors are being adversely affected by potentially risky loans, as are borrowers that obtained such loans but are now struggling to have lenders/investors agree to restructure them.[430]

c) Risks for consumers as lenders/investors or as borrowers

Some of the consumer risks identified in this chapter affect both lenders/investors and borrowers, while others are unique to one of these cohorts. The chapter therefore first discusses risks common to consumers that are lenders/investors or borrowers and corresponding regulatory approaches. Risks specific to investors/lenders or to borrowers are then discussed next.

Many of the risks discussed in this chapter are not new in nature—what is new, or different from a traditional lending and investment context, are the ways they transpire or are heightened in a P2PL context. As is the case with the basic elements of P2PL discussed above, the basic elements of many of the risks discussed in the chapter can also arise in connection with more long-standing lending and investment offerings. However, the impact and extent of these risks is affected by factors such as the nature and extent of reliance on technology, the unfamiliarity and complexity of P2PL business models for consumers, and the expanded access to unfamiliar investment opportunities facilitated by P2PL platforms.

d) Summary of consumer risks and regulatory approaches discussed in this chapter

Table 4 summarizes the new manifestations of consumer risks and corresponding regulatory approaches discussed in this chapter.

TABLE 4: Consumer Risks and Regulatory Approaches: Peer-to-Peer Lending

RISKS TO CONSUMERS	REGULATORY APPROACHES	SEE PAGE
Risks for both lenders/investors and borrowers		
Gaps in regulatory perimeter: P2PL is not adequately covered by a country's FCP regime, and borrowers and lenders/investors receive even less protection than applies to traditional lending	• Apply FCP requirements on an activities basis (lending and investment-related services), rather than by institution type • Extend existing FCP requirements to P2PL, and, where necessary, introduce additional FCP rules for P2PL • Issue regulatory guidance to address uncertainty regarding the application of existing FCP requirements to P2PL *(Also, see approaches for addressing cross-border risks summarized above in the context of digital microcredit)*	78
Fraud or other misconduct: Fraud or other misconduct by P2PL platform operators, related parties, or third parties	• Impose licensing/registration and vetting and competence requirements on operators and related parties • Require operators to have in place adequate risk management and governance arrangements • Require operators to segregate consumers' funds and deal with them only in prescribed ways • Consider compensation funds *(Also, see below for approaches to address platform/technology vulnerability risks that may facilitate fraud)*	81

TABLE 4, *continued*

RISKS TO CONSUMERS	REGULATORY APPROACHES	SEE PAGE
Platform/technology unreliability or vulnerability: Platform/technology unreliability or vulnerability that causes or facilitates loss, inconvenience, or other harms	• Require operators to have in place adequate risk management and governance arrangements • Require operators to comply with targeted risk management and operational reliability requirements, including for technology-related risks and outsourcing • Impose specific competence requirements on operators in relation to matters such as information technology-related risk	82
Business failure or insolvency: Business failure or insolvency of operator causing loss, such as of lenders/investors' capital or future income on loans or borrowers' committed loan funds or repayments	• Require operators to segregate consumers' funds, hold them with an appropriately regulated entity, and deal with them only in prescribed ways • Require operators to have in place business continuity and hand-over/resolution arrangements • Require operators to comply with recordkeeping requirements to support business continuity arrangements • Impose vetting and competence requirements on operators and related parties	83
Inadequate credit assessments: Inadequate credit assessments, increasing the risk of losses from borrower defaults for lenders/investors and over-indebtedness for borrowers	• Impose creditworthiness assessment requirements on operators regardless of whether they are the lender of record	85
Conflicts of interest: Conflicts of interest between platform operators (or their related parties) and lenders/investors or borrowers, leading operators and related parties to engage in conduct not in the interests of their consumers: • Conflicts of interest leading to imprudent lending assessments by operators • Conflicts of interest leading to unfair or inappropriate loan pricing • Conflicts of interest from intra-platform arrangements, causing operators to engage in conduct favoring related parties over consumers	• Impose general conflict-mitigation obligations on operators • Require operators to comply with duties to act in consumers' best interests • Require operators to meet obligations regarding fair loan pricing and fees and charges-setting policies consistent with consumers' interests • Place restrictions or prohibitions on operators or their associates investing in loans facilitated by their platforms • Impose creditworthiness assessment requirements on operators regardless of whether they are the lender of record	86
Additional risks for lenders/investors		
Inadequate investment-related information: Lenders/investors are not provided with adequate investment-related information, including: • Inadequate up-front information when considering or making investments/loans • Information being provided in an inadequate format	• Require platform operators to provide/make available to consumers ahead of any transaction information highlighting key matters relating to P2PL, such as expected risks, factors affecting returns, and restrictions on early exit • Require platform operators to provide key precontractual information about individual loans to prospective lenders/investors in business models allowing individual loan selection • Mandate warnings or disclaimers in key contexts to highlight risks for consumers and assist in balancing out inappropriately optimistic perceptions • Require platform operators to give key information appropriate prominence on electronic channels • Require key information to be provided in a standardized format to assist clarity and comparability *(Also, see approaches for risks from digital disclosure summarized above in the context of digital microcredit)*	88

TABLE 4, *continued*

RISKS TO CONSUMERS	REGULATORY APPROACHES	SEE PAGE
Additional risks for lenders/investors		
• Unbalanced or misleading marketing regarding P2PL investment/lending opportunities • Inadequate ongoing information about the performance and status of lenders/investors' investments/loans	• Require platform operators to comply with general prohibitions against providing misleading information (and, when necessary, clarify via more specific regulatory guidance the application of such prohibitions to marketing of P2PL opportunities) • Impose targeted restrictions on specific P2PL circumstances presenting higher risk of misleading investors • Require platform operators to provide ongoing information to lenders/investors at prescribed times or frequencies regarding matters affecting their investments/loans specifically, such as defaults, changes to borrowers' circumstances, and so on, or more generally, such as performance of the operator and adverse events	
Harm due to lenders'/investors' lack of sophistication or inexperience: Such as taking on risk of loss they cannot afford or do not understand	• Impose lending/investment caps on less sophisticated or more vulnerable lenders/investors (jurisdictions have done so on a variety of bases) • Impose caps on the amount that individual borrowers may borrow through P2PL platforms as another way to reduce risk of loss to lenders/investors • Consider compensation funds	94
Borrower fraud: Loss for lenders/investors due to borrower fraud	• Require platform operators to comply with risk management requirements referred to above, as well as targeted requirements, such as to obtain appropriate identification information and implement measures against fraudulent access to their platform (know your customer requirements under AML/CFT laws would also be relevant) • Impose creditworthiness assessment requirements on platform operators regardless of whether they are the lender of record	97
Additional risks for borrowers		
Inadequate loan-related information	• Extend application of existing traditional credit-disclosure requirements to platform operators even when they are not the lender of record • Address gaps in existing borrower-disclosure regimes by developing requirements specific to P2PL *(Also, see approaches for risks relating to credit disclosure summarized above in the context of digital microcredit)*	97
Risks from digital distribution of P2PL credit: Risks arising from digital distribution of credit summarized above in the context of digital microcredit can also affect digital distribution of P2P loans to borrowers	*See approaches summarized above in the context of digital microcredit*	98

5.2 CONSUMER RISKS FOR BOTH LENDERS/INVESTORS AND BORROWERS

a) Gaps in regulatory perimeter

Risks to consumers

Although the core elements of lending and investing on which P2PL is based are not new, novel aspects of P2PL platform arrangements and business models can mean that they sit outside a country's existing FCP regulatory perimeter. As a result, consumers may be exposed to risks even if these would already be addressed by existing regulation. For example in 2014 the Central Bank of Ireland felt compelled to warn consumers that crowdfunding, including P2PL, was not a regulated activity in Ireland and therefore complaints about it could not be made to the Financial Services Ombudsman.[431]

Some jurisdictions regulate traditional lending and investment activities under separate frameworks. However, in a P2PL context, gaps in the coverage of lending regulation, not just investment protection, can harm individual lenders/investors as well as borrowers. For example, the key obligation (discussed later in the chapter), typically imposed on traditional lenders under FCP

frameworks, to undertake creditworthiness assessments on prospective borrowers can protect individual lenders/investors' interests, as well as those of borrowers.

Gaps in regulatory coverage of credit activities undertaken through P2PL platforms can frequently arise when a regime regulates certain conduct, such as lending, only if undertaken by particular types of institutions—such as banks or licensed non-bank financial institutions. This is sometimes referred to as institution-based regulation, to be contrasted with activity-based regulation. While consumer P2P loans may be very similar to personal installment loans provided by traditional lenders such as banks and finance companies, they may not be regulated because of the nature of the lender.

In a P2PL context, however, gaps can also arise in regimes that adopt activity-based approaches. This depends on the nature and description of the regulated activities when using such an approach. For example, in some P2PL business models, platform operators may not be undertaking the core lending activity on which regulation frequently focuses—namely, being the legal lender—but they nevertheless control many important aspects of that activity, as well as being best placed to comply with relevant requirements.

By way of illustration, the EBA pointed out that the European Directive on Consumer Credit (which mandates a range of consumer protection requirements for consumer lenders) was unlikely to apply to a P2PL platform operator that was not itself acting as the lender but, rather, was intermediating lending by individuals. The Directive applied to a creditor defined as a "person who grants or promises to grant credit in the course of his trade, business or profession." This would be inapplicable to a platform operator operating under a business model where they are not the lender of record. The EBA also noted that the Directive was unlikely to apply to individuals lending through such a platform unless they were in fact undertaking a lending business, rather than investing for personal purposes.[432] In any case, from a practical perspective, they would be unlikely to be able to comply with relevant FCP requirements. Similarly, the European Commission noted that the fact that a platform may be carrying out activities normally undertaken by creditors, such as creditworthiness assessments and debt collection, may not matter in terms of attracting regulatory obligations if they were not the credit provider.[433] Without appropriate modification of domestic legislation based on the Directive, consumers would not receive the same level of protection when borrowing from a P2P lender as they would when borrowing from a traditional lender. In the context of home lending, the FCA expressed concern regarding a potential regulatory gap in its market. It noted that if P2PL platforms offered home loans in the United Kingdom using business models where the platform merely facilitated the finance, this could mean that nobody had responsibility from an FCP perspective. This meant that a home-finance consumer using a P2PL platform may not receive the same level of consumer protection that they would when dealing with an authorized home lender.[434]

From an investment regulation perspective, P2PL operators may provide a range of services for individual lenders/investors of a nature that functionally ought to be already covered by typical investment requirements.[435] Depending on the business model adopted, they may be providing an investment service, such as acting as an intermediary, operating a collective investment scheme, or issuing securities. If undertaking loan-related assessments, they may be providing a form of financial advice to their lenders/investors. Managing ongoing fulfilment by borrowers of their obligations on behalf of lenders/investors may involve providing services under a principal and agent relationship with the lender/investor. They may also provide account management–related financial services and custody services. However, the novelty of P2PL arrangements at times has seemed to generate uncertainty regarding whether and how P2PL-related investment services are subject to existing investor protection laws. In other instances, the nature of P2PL offerings meant that they may not have fit readily within existing investment regulation.

Regulatory approaches

Take an activity-based approach to FCP regulation

Applying FCP requirements by activity, rather than entity, type can assist in ensuring that P2PL platform operators are covered, particularly if reflecting concepts that are sufficiently broad and flexible to cover new and developing business models and entity roles. Some jurisdictions have found that broad concepts in existing legislation, such as relating to lending or investment activities, were effective in automatically extending regulation to new fintech offerings. For example, Australia's National Consumer Credit Protection Act already applied to any "credit activities" involving consumers carried out as part of a business, which included not only the provision of credit but also a range of credit-related assistance to consumers or acting as an intermediary between a lender and a consumer.[436] A P2PL operator acting as a lender to consumers would therefore be subject to the legislation, but so would an operator that acts

as an intermediary between individuals lending directly and their consumer borrowers or assists borrowers to apply for such credit. On the other hand, individual lenders/investors would not be subject to the legislation unless they are engaging lending as part of a business, which would usually not be the case. The Corporations Act similarly applies to the provision of a range of "financial services," including, relevantly to the investment side of P2PL platforms, dealing in or providing advice in connection with managed investment schemes.[437] In Japan, where the typical P2PL model involves the operator providing credit on behalf of investors,[438] businesses offering P2PL services have similarly been expected to register as moneylenders under the Money Lending Business Act,[439] as they are legally considered money lending businesses.[440]

Some authorities have considered it necessary to introduce brand new concepts into legislation to capture P2PL activities adequately. For example, in the United Kingdom, existing rules were amended[441] to cover the activity of "operating an electronic system in relation to lending."[442]

It is important to ensure that activity-based regulatory coverage is not indiscriminate and imposes FCP requirements to the entity that can most appropriately deal with them. Thus, for example, it has been suggested that in South Africa, P2PL may have initially been regulated too strictly by requiring individuals who lend directly through platforms (rather than the operator being the lender) to be registered with the National Credit Regulator and comply with related requirements, as opposed to focusing requirements on platform operators.[443]

Extend existing regulatory framework

Some jurisdictions have sought to extend the coverage of existing regulation to new P2PL business models. In the United Kingdom, a P2PL operator, even if merely intermediating loans without acting as the lender, is subject to key FCP requirements equivalent to those applying to traditional lenders. This is also reflective of the fact that a platform operator is likely to be in a better practical position to discharge compliance obligations than an individual who, technically, may be the lender.[444] In Brazil, the National Monetary Council issued a resolution prescribing P2PL entities (*sociedades entre pessoas*, or SEPs) as a new category of financial institution requiring them to be licensed by the Central Bank of Brazil.[445] SEPs may only facilitate direct loans between lenders and borrowers and not act as a lender using their own funds.[446]

Establish separate regulatory framework

Authorities in some jurisdictions have recently introduced new, separate regulatory frameworks to cover varied aspects of P2PL or both P2PL and investment-based crowdfunding.[447] The introduction of a separate framework may be undertaken for various reasons, such as an absence of sufficient existing regulation or preferring not to adapt or extend existing regulation for the sake of expediency or to avoid implementation difficulties. In China in 2015, the People's Bank of China and nine other government bodies jointly introduced a new framework by issuing "Guiding Opinions on Promoting the Healthy Development of Internet Finance," covering (among other things) P2PL.[448] Interim Measures for the Administration of the Business Activities of Online Lending Intermediary Institutions were subsequently issued in 2016 by the China Banking Regulatory Commission (CBRC)—now known as the China Banking and Insurance Regulatory Commission (CBIRC)—with several other authorities, to set out a regulatory perimeter of permitted, and prohibited, activities for P2PL operators (referred to as P2PL information intermediaries).[449] The P2PL models now permitted in China are limited to matching lenders/investors and loans for the purposes of direct lending.[450] The Korean authorities also recently passed a new law, the Online Investment-Linked Finance and Protection of Users Act, that will require entities intending to engage in P2PL to register with the Financial Services Commission of Korea and be a joint stock company.[451] Peru has similarly recently introduced new rules targeting P2PL and crowdfunding.[452]

Hybrid approaches

Some jurisdictions have adopted a hybrid approach, bringing P2PL within some existing frameworks—such as licensing frameworks—while developing separate sets of conduct rules. In 2018, Mexico, which already had a range of FCP legislation applying to traditional FSPs, introduced a new overarching Financial Technology Institutions Law[453] to cover a range of fintech areas. These include crowdfunding entities, and one of the specified categories is debt crowdfunding.[454] Authorities can issue FCP requirements under this Law as may be considered necessary. However, once regulated, P2PL operators also become subject to existing FCP requirements applicable to other financial institutions, such as the Law on Transparency for Financial Services.[455] In India, the RBI addressed the lack of P2PL regulation by deeming P2PL operators to be "non-banking financial companies".[456] Once regulated as such, operators were made subject to a set of conduct requirements specific to P2PL.[457] The approach in the United Kingdom is arguably somewhat similar, although the FCA has integrated dedicated P2PL requirements in existing rule sets.

In Indonesia OJK has adopted a different hybrid approach to regulating P2PL activities, incorporating an aspect of self-regulation. Providers of "information technology–based loan services" are required to be registered with and licensed by OJK[458] and are subject to rules issued by OJK, including existing regulations on FCP-related matters. However, applicants for licensing and registration are also required to provide proof of membership with an industry association appointed by OJK,[459] such as the Indonesian Joint Funding Fintech Association (AFPI), and confirmation from the association that the applicant pledges to comply with its code of ethics and has not previously breached it. The Fintech P2P Lending Code of Conduct recently issued by AFPI was drafted in consultation with OJK and is intended to address a number of FCP-related matters, such as information disclosure and complaints handling. AFPI can expel members for a violation of its code of conduct, which then renders the relevant entity ineligible to continue to hold their license from OJK.

Leverage regulatory guidance

Regulators may use guidance to address uncertainty regarding the coverage of P2PL by existing frameworks. In the United States, the securities regulator chose to send industry a strong signal with regard to the application of existing regulation to P2PL. Approximately a decade ago, the SEC entered into a cease-and-desist order against a major P2PL platform, signaling to the market that such platforms were making public offerings of "securities" and were therefore subject to the 1933 Securities Act[460] (thus incurring securities-related registration and reporting requirements, among others). According to commentators, one of the practical results of this intervention, besides the exit of some platform providers from the market, has been a change in business models to favor investment-based, rather than direct-lending, models.[461] In Japan, similarly, the typical P2PL model involves the operator providing credit funded by investors under "silent partnership contracts."[462] The regulator requires the operator to be registered as a so-called Type II Financial Instruments Business Operator under the Financial Instruments and Exchange Act[463] to be permitted to solicit investment from investors in the form of a collective investment scheme.[464] Australian authorities have not made significant reforms for the purposes of extending regulatory coverage to P2PL activities. As noted above, this is because federal consumer credit and financial services legislation already applies largely on an activities basis. However, given the novelty of P2PL arrangements in the market, ASIC considered it necessary to form a working group specifically focusing on P2PL matters[465] and to develop detailed guidance[466] to confirm how existing consumer credit and financial services legislation was likely to apply to P2PL activities. ASIC issued guidance to confirm that where a P2PL operator allows "retail investors" to invest in P2PL through a managed investment scheme, the operator is required by the Corporations Act to register the scheme and obtain an Australian financial service license. Providing ancillary financial services, such as financial product advice, would also require a license in Australia. As a license holder, the operator would also have a range of conduct obligations under the legislation.

b) Fraud or other misconduct

Risks to consumers

Consumers may suffer loss under a variety of circumstances involving poor conduct or outright misconduct by P2PL operators, including by their staff, their management, or service providers acting on their behalf. Loss of funds due to fraud is an extreme, if not infrequent, example. Losses may also result from negligence or lack of competence.

Such risks obviously are not unique to P2PL, but various aspects of P2PL's development, and its relative novelty, can contribute to their increase. A consumer may lack the ability, or information, to be able to assess the competence and integrity of the P2PL operator with which they are considering dealing. The EBA made the point that it might be difficult for lenders/investors and borrowers in a particular jurisdiction to find independent information about the reputation of platforms where operators do not require regulatory permissions to operate platforms and are not subject to legal information or disclosure requirements. The EBA also noted that a lender/investor is unlikely to be in a position to assess a platform's reputation or probity for themselves.[467] In China, it was similarly highlighted that, prior to recent reforms, low barriers to entry meant the quality of sector participants varied significantly, creating major risks for participants.[468] By the end of 2017, following a significant tightening of regulation (which some have criticized), 3,600 platforms had already discontinued operations, as many had difficulty in meeting clients' demands for cash withdrawals or had management abandon the business.[469]

Regulatory approaches

Licensing and vetting and competence requirements

Some regulators have sought to develop new requirements, or extend existing requirements, to ensure appropriate vetting of prospective P2PL operators, including their management and staff. The EBA recommends that mitigants to address these risks should include requiring platforms to be authorized by a national

financial supervisory authority or at least to be registered with an authority.

Mere registration, simply involving recording information about entities without any form of entity vetting, is unlikely to be sufficient to address relevant risks. As the EBA also notes, additional measures could comprise checking that the individuals managing a platform meet appropriate standards for competence, capability, integrity, and financial soundness.[470] This should be the case both when first applying for authorization and on an ongoing basis while they continue to be authorized. For example, the RBI requires P2PL operators to ensure that they meet fit and proper criteria at the time of their appointment as well as, importantly, on an ongoing basis. Periodic reporting to the regulator on such matters is required as well as supporting declarations and a deed of covenant.[471]

In China, recent reforms now mean that P2PL platform operators are required to go through multiple stages of authorization. These include obtaining a business license from the relevant branch of the State Administration of Industry and Commerce, followed by registration with the relevant branch of the financial regulatory authority, and then application for a telecommunications business permit from the relevant branch of the Ministry of Industry and Information Technology.[472] Some key vetting criteria seem to have been left to provincial governments to determine; one provincial government proposed a provision that would encourage, albeit not require, a P2PL platform to have strong shareholders and to engage senior management with rich work experience in financial institutions.[473] While it is of course important to ensure that authorization and vetting requirements for operators are sufficiently stringent to address the risks for consumers they deal with, it is also important that they be as efficient and transparent as practicable for participating entities.

Risk management and governance requirements

Regulators are increasingly subjecting P2PL operators to obligations to have in place adequate risk management and governance arrangements. In the United Kingdom, P2PL operators are subject to several overarching obligations (known as the "Principles for Businesses") that apply to authorized firms, one of which is that they must take reasonable care to organize and control their affairs responsibly and effectively, with adequate risk management systems.[474] Drawing from this principle, the FCA has issued more extensive general obligations and guidance with regard to risk management. As a result, P2PL operators are expected to have effective processes to identify, manage, monitor, and report the risks they might be exposed to and to have appropriate internal risk-control mechanisms.[475] Mexico's Financial Technology Institutions Law similarly makes demonstrating implementation of controls for operational risk a key aspect of being authorized as a P2PL operator, as well as more specifically fraud prevention.[476] As discussed in the next section, regulators have also increasingly imposed more specific risk management requirements targeting particular risks, such as with regard to information technology security.[477]

Client funds segregation and handling requirements

Regulatory requirements obliging P2PL operators to segregate client funds and deal with them only in prescribed ways could also assist in addressing risks of loss in this context, such as reducing opportunities of fraud. Such requirements are discussed in more detail below in the context of addressing the risks of operator insolvency and business failure.

Compensation funds

Some authorities and commentators have considered compensation funds as a potential mitigant in the event of loss. However, as discussed later in this chapter, their adoption for P2PL does not seem to be widespread, so it is difficult to discuss emerging approaches as to their structure or operational arrangements.

c) Platform/technology unreliability or vulnerability

Risks to consumers

Consumers frequently face some risk of harm or loss from interruptions or failures in an FSP's systems and processes, but in a P2PL context, the risk may be significantly higher, given the extent to which lenders/investors and borrowers rely on an operator's systems and technology. Relevant harms may include loss or inconvenience caused by platform malfunctions or delays. They may also comprise third-party fraud due to vulnerability to cyber risks. A working group of BIS' Committee on the Global Financial System noted that fintech credit platforms may be more vulnerable than banks to certain operational risks, such as cyber risk, due to their reliance on relatively new digital processes.[478]

As highlighted by the EBA, risk of loss from technical issues affecting a platform is relevant to both lenders/investors and borrowers due to factors such as unavailability of systems, networks, or data and loss of data integrity.[479] The extent of such risks to platforms is likely to depend on a number of factors, including the platform operators' level of sophistication, mechanisms used for storing client information, and the robustness of cybersecurity arrangements. Another aspect of platforms that can give rise to additional risk is significant reliance on third-

party providers, with potential disruption of outsourced services.[480]

Regulatory approaches

General risk management requirements

As discussed above, regulators are increasingly subjecting P2PL operators to general risk management and governance obligations. The expectations imposed by such requirements would clearly also target the need for operators to address risks related to platform/technology unreliability and vulnerabilities.

Targeted risk management and operational reliability requirements

To promote more effective risk management, P2PL operators are also being made subject to risk management obligations targeting specific categories of risk, such as technology-related risks. In Indonesia, OJK requires a P2PL operator to meet obligations with regard to its information technology and the security of that technology, risk management, and resilience to system interference and failures.[481] Detailed requirements prescribed by OJK include rules on establishment of a disaster-recovery center, acquisition and management of information technology, and incident management and implementation of security measures. OJK has also allocated specific responsibilities to a P2PL operator's board for information-technology risks. China's Interim Measures for the Administration of the Business Activities of Online Lending Intermediary Institutions require registration, testing, and implementation of P2PL platforms' information systems that are appropriately reliable and secure. The Interim Measures specify a range of matters that must be addressed by operators, such as firewalls, intrusion detection, and data encryption as well as broader concerns with regard to information-technology risk management and resourcing.[482]

Outsourcing-related risk management

Given the extent to which P2PL platforms tend to outsource a range of their functions to third parties,[483] an important risk management obligation on operators can be to take appropriate steps to avoid additional operational risk resulting from such outsourcing. The RBI's rules for P2PL operators set out obligations for operators to ensure sound and responsive risk management practices for effective oversight, due diligence, and management of risks arising from outsourced activities.[484] Ensuring that operators remain legally responsible to consumers for outsourced functions can also assist—as provided, for example, by the new EU regulation on crowdfunding (including P2PL for business purposes).[485]

Competence requirements

General competence requirements of the kinds already described above can assist to ensure that P2PL operators and their management and staff are appropriately competent with regard to relevant technical risks. Some regulators are also targeting such risks with more specific competence requirements. For example, OJK specifically requires a P2PL operator to have in place staff with expertise and background in information technology.[486]

d) Business failure or insolvency

Risks to consumers

A consumer lender/investor may risk losing their committed loan principal, or repayments owed to them, that are being held or administered by a P2PL operator who goes insolvent or whose business otherwise fails. When consulting on proposed regulatory reforms for P2PL, the FCA said it considered P2PL operators to present a high risk of consumer harm, given that they may hold or control client funds before lending these to borrowers. It also noted that, if an operator were to fail, it was extremely likely that there would be loan contracts that had not matured, resulting in the continued receipt and holding of funds on behalf of lenders/investors.[487] Indonesia's OJK similarly highlighted a concern with the need to protect investor funds against such loss.[488]

Borrowers can also face risks of losing funds under such circumstances. A borrower may miss out on receiving funds intended for them from lenders/investors as a result of the operator's insolvency. The EBA pointed out the risk of a lender/investor's funds not being transferred to the intended borrower if the platform is not required to hold appropriate regulatory authorizations, and have in place adequate arrangements, to safeguard such funds.[489] Depending on the legal relationships between the parties, borrowers may also suffer loss of funds that they are seeking to repay through the platform but do not reach lenders/investors.

Individual lenders/investors run the risk of suffering losses in the event of a P2PL operator's business failure (regardless of cause), even if their assets are ring-fenced from the operator's insolvency as discussed above. Both the International Organization of Securities Commissions and the European Commission have highlighted research that points to business failure and platform collapse as some of the biggest perceived risks for investors and, to some extent, borrowers, associated with P2PL.[490] Business cessation can mean that even individual loans that remain viable may not continue to be administered properly, causing corresponding loss. As the FCA

explains, even if the platform fails, existing loans and investments still need to be administered: repayments or dividends need to be allocated appropriately among lenders/investors, and late payments by borrowers have to be followed up on.[491] An investor can suffer considerable harm if a P2PL platform ceases to provide management and administration services. In practical terms, this can mean an individual lender/investor may not receive some or all of the repayments for the loans that they made or invested in through the platform unless they retrieve payments directly from borrowers themselves. This seems impracticable and uneconomical generally, but particularly where an individual's investment is across a portfolio of loans to which rights are also held by others.[492]

While it might be possible for an administrator or liquidator to direct a transfer of a platform's loan book and investor account portfolio to another platform operator, this can result in significant losses for investors.[493] Inadequacy of a P2PL platform's wind-down arrangements in the event of platform failure are certainly a key concern.[494] However, so is deficient recordkeeping even when the platform is operating, which can make it difficult at any time to determine which loans and repayment streams relate to which investors.[495]

Regulatory approaches

Segregation of consumers' funds

A key safeguard, already typically required to protect client funds in some other contexts internationally, is the requirement that investor and borrower funds be segregated from other funds held by a P2PL operator. In addition, such funds are typically required to be held by an entity appropriately regulated, including with regard to capital requirements, for the purposes of handling and safeguarding such funds.[496] As highlighted by the EBA, the main alternatives entail either the platform operator being appropriately authorized and regulated to hold such funds before it is permitted to undertake money-handling activities on investors' behalf, or the operator having to ensure that a separate, appropriately regulated entity handles those funds on investors' behalf.[497] Consistent with this, the European Commission's proposed regulations for crowdfunding (including certain P2PL) would allow P2PL operators, or their third-party providers, to hold client funds and provide related "payment services" only if the relevant entity is a regulated payment service provider. Alternatively, the P2PL platform arrangement would need to operate on the basis that client funds are dealt with through regulated third-party payment service providers.[498]

A range of regulators have mandated that P2PL platform operators administer segregated accounts within which to hold investor and borrower funds. Both the RBI in India and OJK in Indonesia have mandated that P2PL platforms operate escrow accounts for this purpose. The Indian regulator requires separate escrow accounts (to be held in trust with banks) for funds received from lenders/investors pending disbursal to borrowers and funds collected from borrowers. All fund transfers in each direction are required to be undertaken through bank accounts.[499] The Indonesian regulator requires having "virtual" accounts for each lender/investor as well as each borrower.[500] In Korea, new P2PL legislation also requires that operators keep investment funds and loan repayments separate from their own funds and hold these at a bank or other appropriate institution.[501]

In the United Kingdom, the FCA similarly confirmed that funds held by a P2PL platform from clients for the purposes of lending out to borrowers and, in turn, repayments from borrowers to be provided back to clients are regarded as client money held on behalf of clients in relation to investment business. Any firm that holds client money in connection with such business does so as trustee and is required to make adequate arrangements to safeguard it. Key requirements in this regard include that the platform operator would be required to deposit such funds at an appropriate institution (that is, a bank), keep records and accounts, and conduct appropriate internal and external reconciliations, so the platform operator can always distinguish between funds held for different clients.[502] Jurisdictions in the European Union take equivalent approaches.[503]

Recent reforms in China mandate separation of platform operators' funds from those of lenders/investors and borrowers. Commentators note that a significant driver for this requirement was scandals caused when P2PL operators absconded with consumers' funds.[504] The CBIRC's Guidelines for Online Lending Fund Depository Business[505] clarify that P2PL platforms must acquire custodian services for the purposes of holding segregated funds from commercial banks. (However, to encourage banks to provide such services and to address concern that they may be held liable for matters outside their control, it is also made clear that custodian banks will not be legally liable for matters such as lending assessments and defaults).[506] A P2PL platform may have only one custodian.

Client money handling requirements

Another at least partial mitigant to the risk of losing funds due to operator insolvency or business failure are client money-handling requirements that specify how, and within what time frames, funds must be transferred to lenders/investors from borrowers (for example, as repayments are made) and to borrowers

from lenders/investors (for example, at loan-funding stage). Such rules can be complementary to, and bolster, the benefit of ring-fencing requirements, minimizing the time during which funds may be subject so insolvency risk. For example, the Brazilian authorities require—in addition to the keeping of escrow accounts—that funds be transferred to lenders/investors within one day of funds being paid by borrowers and to borrowers within five days of funds being made available by lenders/investors, and to be segregated until such transfers are made.[507]

Business continuity and hand-over/resolution requirements

A regulatory measure that can also help to address potential loss due to business failure is the requirement for platform operators to have in place business continuity and resolution arrangements. In France, platform operators are required to enter into a contract with a third-party payment institution to ensure such business continuity.[508] To address relevant risks in the case of permanent, rather than temporary, platform failure, the EBA suggests that the platforms should be required to have resolution plans in place, to allow loans to continue to be administered.[509]

In the United Kingdom, rules imposed by the FCA require a P2PL operator to have arrangements in place to ensure that P2P loans will continue to be managed and administered on an ongoing basis and in accordance with the contract terms even if the platform ceases to carry out those functions. The FCA has issued detailed rules and guidance setting out the operational, legal, and financial aspects that such arrangements must take into account. It would also be important to document such arrangements effectively for parties that step in for the operator at the relevant time. The FCA's most recent reforms introduced rules requiring operators to prepare and maintain a manual containing information about their operations that would assist in resolving the platform in the event of its insolvency. The "P2P resolution manual" would have content similar to that required for so-called living wills required for systemically important financial institutions.[510] Depending on the P2PL business model, such arrangements should cover the management of both the loan portfolio and, if relevant, the corresponding investment portfolio.

Record-keeping requirements

Recordkeeping arrangements are also likely to be a key regulatory approach in this context, although they are obviously crucial more broadly to support the integrity of a P2PL platform's operations. For example, P2PL operators in the United Kingdom are subject to general requirements, as authorized firms, to keep orderly records of their business, including all the services and transactions undertaken. These must be sufficient to enable the FCA to monitor their compliance with all client obligations. Relevant to the risk discussed here, the FCA points out that such recordkeeping must adequately reflect and support the complexity of its business model, expressing an expectation that the granularity of information about individual clients' investments holdings should be immediately retrievable.[511] Such records could therefore better support a third party for business continuity purposes.

Risk management and competence requirements

Risk management and competence requirements described above to mitigate risk of loss due to platform unreliability or vulnerability can also assist in this context. They may not only assist with reducing the risk of business failure but also place a P2PL in a stronger position to address adverse consumer impacts of such a failure.

e) Inadequate credit assessments

Risks to consumers

Both P2PL borrowers and lenders/investors face significant risk of harm if appropriate credit assessments are not undertaken in relation to prospective borrowers. Providing unaffordable loans can result in over-indebtedness for borrowers and losses from borrower defaults for lenders/investors. Deficient credit risk assessments can also affect the appropriateness of pricing decisions by a platform operator; that is, lenders/investors may not be compensated commensurately with the level of credit risk they are exposed to. A micro or small enterprise, such as a sole trader or small partnership, borrowing for business-related purposes may also be assessed incorrectly by a P2PL platform and, as a result, attract less interest from potential lenders/investors.[512]

Consumers on both sides of P2PL arrangements can be heavily reliant on assessments by the platform to ensure that loans fit within parameters they are comfortable with.[513] As discussed in the chapter on digital microcredit, the use of algorithms for the purposes of credit assessments can give rise to various risks. Such risks could be even greater for a consumers dealing with P2PL platforms that rely on novel and untested credit assessment models.[514]

P2PL platforms have also been seeking to leverage big data analytics and non-traditional data sources. This is particularly the case in relation to platforms whose

business models focus on expanding credit access to borrowers. A recent WBG discussion note canvasses various potential consumer risks associated with uses of alternative data beyond traditional credit reporting sources.[515] There may be potential weaknesses and gaps in the context of such credit assessments undertaken by P2PL platforms. (This can depend in part on the credit reporting and broader data ecosystem in a particular jurisdiction.) The data used by platforms to assess borrower risk may not be as comprehensive as that used in traditional lending, or if platforms have expanded into new borrower segments, they may have access to poorer default data.[516] Expansion of credit access is of course an important aim with regard to financial inclusion and financial access. However, it is important that credit assessments be undertaken on a sufficiently rigorous basis regardless of the data and methods used.

Regulatory approaches

Creditworthiness assessment requirements for operators

Creditworthiness assessment requirements are a key mitigant against unaffordable lending, and in a P2PL context, it seems crucial that such obligations apply to the entity in the best practical position to undertake such assessments. This is usually the P2PL operator, rather than an individual consumer, regardless of whether they are technically the lender under a relevant arrangement.[517] The FCA introduced rules that require a P2PL operator to undertake creditworthiness assessments for non-mortgage P2PL equivalent to those that would need to be undertaken by a traditional licensed lender. The rules set out detailed requirements on the information that should be obtained and verified by the platform operator about the borrower's income, expenditures, and other circumstances for the purposes of such an assessment, and how the assessment should be made. Where the P2PL operator is a conduit for a licensed lender, both entities would have such obligations. Although the UK market for P2P consumer mortgage lending had not yet developed, the FCA more recently also extended its existing conduct rules for such lending to any P2PL platform that may offer home loans.[518] The FCA has also imposed obligations on P2PL operators to undertake a reasonable assessment of the credit risk of the borrower before the P2PL agreement is made where the operator determines the price of a P2P loan.[519] The RBI has similarly imposed obligations on P2PL operators to undertake credit assessment and risk profiling of borrowers and disclose the results of these to prospective lenders/investors.[520] The Act on Online Investment-Linked Finance and Protection of Users recently introduced in Korea requires P2PL operators to confirm borrowers' income, assets, and liabilities and prohibits them from lending in excess of the borrower's ability to repay.[521]

Access to adequate credit reporting and scoring arrangements for operators

The effectiveness of credit assessment obligations on P2PL platform operators could be diminished if operators do not have access to effective, fair credit reporting and scoring arrangements. For example, traditional lenders often have the advantage of being able to leverage long-term lending or other banking relationships to model credit risk. Newer entrants such as P2PL platforms may lack such data.[522] In the context of the P2PL crisis that developed in China, commentators noted that no comprehensive personal credit system was accessible to P2PL platforms. Platforms lacked access to the existing credit reporting system run by the central bank, and commercial credit reporting for P2P lenders was still being developed.[523] The importance of P2PL operators having access to such information was highlighted repeatedly, particularly given the lack of credit-related data held within the industry, in part impaired by its short track record.[524] While this paper is not intended to canvass the range of issues that need to be addressed to ensure effective credit reporting and scoring arrangements, this is an area of significant complementarity to creditworthiness assessment obligations. It is therefore important that regulators consider the adequacy of the credit reporting and scoring ecosystem in their jurisdiction alongside the development and implementation of FCP measures. The ICCR has recently issued a range of relevant guidance, including on the implementation and operation of credit reporting and scoring arrangements in developing countries lacking formal data sources.[525]

f) Conflicts of interest between platform operators and lenders/investors or borrowers

Risks to consumers

Conflicts of interest can affect many dealings between consumers and FSPs, but certain characteristics of particular P2PL business models can be especially conducive to conflicts of interest between operators and lenders/investors or borrowers.

Conflicts of interest leading to imprudent lending assessments by platform operator

Where a P2PL operator's revenue is heavily dependent on fees for generating new loans (as is often the case), a potential conflict of interest that can arise is a tendency to weaken credit assessment standards to increase loan approvals. This can result in higher risks of loss than expected by lenders/investors, as well as imprudent lending that can expose borrowers to subsequent hardship.

Many P2PL platforms earn fees from originating loans while their lenders/investors bear the burden of any loss, creating an inherent conflict of interest.[526] Fees frequently charged by platforms that can contribute to such a conflict include origination fees (for example, as a percentage of the loan amount) at the time of loan origination and servicing fees (for example, as a percentage of capital due) paid during loan reimbursement.[527] ASIC found in several periodic P2PL surveys that P2PL operators were generating most of their revenues from loan origination, while ongoing fees (such as linked to loan repayments) made up a much smaller proportion.[528] Platform operators themselves highlighted that they needed to manage the potential conflict between the interests of investors in not wanting credit assessment standards lowered and those of operators who want to enable more borrowers to qualify for loans to generate additional fees.[529] In addition, some platforms charge debt collection fees in relation to P2P loans, such as a percentage of the amount recovered, which can compound such conflicts of interests.

A bias toward making riskier loans can also be compounded when trying to satisfy demand for higher returns from investors.[530] The FCA and other commentators have also noted that a greater propensity to adopt looser credit assessment standards may be influenced by a platform's desire to grow their market share quickly to achieve commercial viability.[531]

Conflicts of interest leading to unfair or inappropriate loan pricing

P2PL operators are providing retail investors access to asset types to which many such investors have previously had limited, if any, exposure.[532] Even if investors understand the risks associated with such investments (an important issue discussed separately below), the rate of return they should expect remains a key issue. The FCA identified as a particular area of concern in its market P2PL models the situation in which the operator facilitates loans on behalf of investors and sets the loan price but it is not clear that the interest being paid by borrowers is appropriately linked to the credit risk they pose or that the return received by investors reflects the investment risk they are actually prepared to take. Given this potential disconnection between the risk taker and price setter, there was a greater risk of harm for lenders/investors if credit assessments and pricing decisions were not undertaken properly.[533]

Some P2PL platforms may transfer loans to investors in inappropriate ways, such as when reassigning loans between investors as part of an operator's ongoing administration of loan portfolios under its discretionary management. In the United Kingdom, such transfers were found to be taking place without taking into account the value of the loans at the time of transfer (in extreme cases, loans already in default were being added to an investor's portfolio without any consideration of what reduction in valuation would be required) or, when facilitating the transfer of prefunded loans arranged by the operator or related party, without considering conflicts of interests.[534]

Conflicts from intra-platform arrangements

Conflicts detrimental to lenders/investors may also arise from the structures behind certain platforms or from other arrangements internal to the platform. For example, in a business model where the operator, or an affiliated party, prefunds loans and then sells them through the platform to individual lenders/investors while retaining a stake, lenders/investors may be agreeing to receive only a portion of the interest that the borrower is paying.

Where the platform operator, or an affiliated party, can also invest in loans offered through the platform, they may have advantages over ordinary lenders/investors. Such advantages may include, for example, better or prior access to loan selection (allowing "cherry-picking") or access to information about prospective borrowers, and how they have been assessed, not available to other lenders/investors.[535]

Regulatory approaches

General conflict mitigation obligations

A key mitigant would be to require P2PL operators to implement adequate policies and procedures and effective organizational and administrative arrangements designed to prevent conflicts of interest from harming the interests of their clients. Such obligations would encompass expectations that operators take appropriate steps to identify and manage, or prevent, conflicts of interest within their organization, such as conflicts between the interests of their management, staff, or agents and those of their clients, or conflicts that the platform arrangements may create between different clients. For example, as a credit licensee under Australian legislation, a P2PL operator would be subject to a general obligation to have in place adequate arrangements to ensure that its borrower clients are not disadvantaged by any conflict of interest that may arise wholly or partly in relation to credit activities engaged in by the operator or its staff or agents.[536] As a financial services licensee, they would be subject to (slightly different) general obligation to have in place adequate arrangements for the management of conflicts of interest affecting lenders/investors arising from the operator's, or their staff or agents', provision of financial services.[537] In the United

Kingdom, one of the "Principles for Businesses" applying to all authorized firms would require a P2PL operator to manage conflicts of interest fairly, both between itself and its customers and between customers.[538] The new EU regulation on crowdfunding (including P2PL for business purposes) requires an operator to maintain and operate effective internal rules to prevent conflicts of interest and to take all appropriate steps to prevent, identify, manage, and disclose conflicts of interest between the operator, their shareholders, their managers or employees, and other related parties and their clients, or between one client and another client.[539]

Conflicted remuneration restrictions

Another important general mitigant is requiring P2PL operators to have in place policies to ensure that staff or management incentives do not encourage conflicted behavior. This would include ensuring that incentives for staff undertaking or overseeing credit assessments (or designing those credit assessments, such as where these are automated) are not based on volumes and take into account loan quality and overall performance.

Duties to act in consumers' best interests

An additional potential approach would be to impose duties on operators to act in accordance with the best interests of clients and prospective clients. Such as duty already exists in some jurisdictions. The new EU regulation on crowdfunding imposes such a duty toward both lenders/investors and borrowers.[540] In the United Kingdom, another "Principle for Businesses" to which authorized P2PL operators must adhere is to pay due regard to the interests of customers, as well as treating them fairly.[541] In Australia, a P2PL operator operating a managed investment scheme is required to act in the best interests of the members of that scheme.[542] However, imposing such an obligation with regard to borrowers remains less prevalent. For example, Australia recently introduced a best-interests obligation toward borrowers under its consumer credit legislation limited only to mortgage brokers.[543]

Obligations targeting specific conflicted circumstances

Authorities have also been implementing restrictions that target specific circumstances giving rise to conflicts, such as fee setting and loan pricing policies. In Brazil, P2PL operators are subject to an obligation to adopt fees and charges policies consistent with viable lending, to ensure convergence of their own interests and those of their clients.[544] In the United Kingdom, operators with responsibility for pricing loans have been obliged to have a mechanism in place to ensure that the pricing offered to lenders/investors accurately reflects the credit risk of the borrower. This was viewed as important both when setting the interest rate (for new loans) and when calculating the present value of a loan (interest and principal) for existing loans being transferred to a different investor.[545] The FCA has prescribed strict rules on, first, carrying out a reasonable assessment of the credit risk of the borrower before a P2P loan is made. Such rules cover a range of matters that the operator must, or may, have regard to when undertaking a risk assessment. They include such aspects as the information to use, whether and to what extent to verify such information, and the characteristics of the credit.[546] The rules then set out detailed requirements on loan pricing, loan allocation, and portfolio composition that include determining a fair and appropriate price having regard to the loan's risk profile and taking into account the time value of money and relevant credit spread. Operators are expected to use appropriate data and robust modelling for such purposes.[547] Relevant operators are also required to review loan valuations under prescribed circumstances, including when they facilitate an investor's exit before a loan has matured, as well as when loans default or seem likely to do so.[548]

In some jurisdictions, restrictions or prohibitions have been applied on P2PL operators or associates investing in loans facilitated by their platforms. Regulations in China—which limit P2PL operators to intermediating loans made directly between lenders/individuals and borrowers—prohibit operators from making any loans themselves (and from attempting to disguise any lending on their own account).[549] Indonesian regulations similarly prohibit operators from acting as lenders (or borrowers).[550]

Creditworthiness assessment requirements for operators

Obligations on P2PL operators to undertake appropriate creditworthiness assessments, already discussed above, can also mitigate against the risk of conflicts leading to inappropriate lending decisions. These would ensure that the operator's conduct would align with the interests of both lenders/investors and borrowers to make only loans assessed appropriately for affordability.

5.3 ADDITIONAL CONSUMER RISKS FOR LENDERS/INVESTORS

a) Inadequate investment-related information

Risk: Inadequate upfront information

The unavailability of adequate information about prospective P2P loans, or a P2PL operator's proposed services, can mean that lenders/investors lack an ade-

quate basis to make informed investment decisions. In addition to a P2PL operator's failure (intentional or otherwise) to provide such information, a range of factors affect this risk in a P2PL context.

Operators may lack information about loans and related arrangements necessary to produce appropriate disclosures regarding risks and returns. Platforms need to have the right systems and controls to gather necessary information.[551] This includes information about borrowers that is also needed for the purposes of creditworthiness assessments and loan pricing as discussed above. Even if P2PL operators are required or willing to publish such information, they may not necessarily have extensive historical data to publish or on which to base relevant disclosures.[552] Lenders/investors may not appreciate the significance of a lack of data in assessing the risk of their investments, particularly if a platform has operated only during more positive economy times.

In addition to a lack of adequate information about risks and returns, lenders/investors may not receive adequate information about the fees and charges associated with the services that the platform operator is providing. Charging structures in the P2PL sector can be opaque. Fees and charges may be incurred by lenders/investors for loan origination, for various aspects of ongoing servicing of loans, and for contingent events such as late payments. Operators' charging structures may be based not only on fees associated for individual services or events but also on receiving as a variable margin a differential between the money due to lenders/investors who take on the credit risk and the money paid by borrowers in interest. This can be particularly significant if the margin taken by the platform significantly erodes the return for the lender/investor taking on that risk.[553]

Investors/lenders may also lack awareness or appreciation of the illiquidity of their P2PL investments. A particular P2PL platform may not offer them the ability to exit their investment at any given point in time or to gain early access to the funds they have invested/lent.

Risks associated with a lack of information can be exacerbated by how lenders/investors' behavioral biases manifest themselves in relation to P2PL. P2PL can offer less experienced lenders/investors access to asset types to which many of them may have previously had limited or no exposure.[554] Such lack of familiarity can contribute to investors not understanding the true nature of the risks of such lending, even if they have experience investing in other assets. ASIC identified that in the Australian market a key risk was investors not having sufficient understanding of the marketplace lending product when deciding to participate.[555] Familiarity with traditional lending, including as a borrower, may also contribute to a false sense of confidence that the risks are understood.

Lenders/investors may also rely excessively on a platform operator's risk assessments or loan selection. This issue can be exacerbated under circumstances where the regulatory framework in fact does not impose sufficient obligations on the operator to undertake such assessments.[556] Even when the operator is subject to such obligations, it is important for lenders/investors to understand the practical limitations of these assessments and limitations on the legal responsibility of the operator for losses. A lack of standardization in Europe for information regarding credit assessment methods has been identified as one of the factors making it difficult for lenders/investors to assess and compare the quality of platforms.[557]

Regulatory approaches to address inadequate upfront information

Disclosure requirements

Disclosure rules covering key matters such as expected risks and factors affecting returns have been highlighted as a key regulatory measure to ensure that appropriate information is available up front to lenders/investors.[558] Regulators in wide-ranging jurisdictions, such as in China and the United Kingdom, have implemented information content requirements for disclosures that P2PL operators must provide in advance either to the public at large or to individual lenders/investors. In a recent survey of regulators on alternative finance, ensuring accurate and complete communications and providing standardized information were identified as some of the most prevalent regulatory measures.[559]

The Chinese authorities have recently prescribed extensive disclosure requirements for P2PL as part of major regulatory reforms to address some of the significant problems that arose in their market. Following the issuance of the Interim Measures for the Administration of the Business Activities of Online Lending Intermediary Institutions[560] discussed above, the then CBRC issued a Guide to the Disclosure of Information on Business Activities of Peer-to-Peer Lending Information Intermediaries.[561] The guide specifies requirements for P2PL operators to provide to investors, or the public more generally, a wide range of information.[562] Importantly, these disclosure requirements apply in a context where Chinese P2PL platforms are permitted to facilitate only direct lending between lenders/investors and borrowers. A P2PL opera-

tor is required to disclose an extensive range of information to the public, including the following:

- Registration information: This comprises a range of information recorded as part of its registration and licensing, such as details regarding that registration and license, and information about the bank where the funds managed in relation to the platform are held and about the operator's risk management arrangements (including its risk management framework, risk-assessment process, and collection methods, among other details).
- Organization information: This comprises a range of information about the entity and its business, such as name and address details, and information about its capital, key personnel, including directors and management, business scope, shareholders, branches (including contact details and complaints hotline number), and all of its electronic channels.
- Examination information: The operator is required to disclose annually information such as their financial audit and regulatory compliance examination reports (and update it if there are any changes from time to time).
- Information about past and current loans: This comprises a range of information relating to the P2P loans that the operator has intermediated previously, including total number of loans and borrowers and total amount of loans since formation, current number of loans and borrowers and total amounts outstanding, amount and numbers of loans overdue, proportion of outstanding loan balances that relate to the top 10 borrowers and the largest single borrower, similar information regarding loans made to related parties of the operator, as well as information about repayments made by another party as a result of the borrower's default, and details of the fees collected by the operator from borrowers and standards for the calculation of such fees.[563]

The Chinese authorities have also imposed detailed obligations on operators to provide various precontractual information about individual loans to prospective lenders/investors. (Such obligations would of course be relevant to P2PL business models allowing individual loan selection by a lender/investor, rather than a P2PL business model where the operator manages loan portfolios on an investor's behalf.) Prior to a lender/investor committing to lend, the operator is required by to provide them with information about the following matters:

- The borrower, such as type of entity and industry, revenue and liabilities, overdue payments in the last six months recorded on their credit report, and other P2P loans they hold.
- The relevant loan, such as the proposed amount, term, and purpose of the loan, the repayment method, annual interest rate, basis on which the borrower will repay the loan, and any guarantee.
- The operator's risk assessment and possible risk outcomes identified in relation to the loan.[564]

The FCA's progress in strengthening disclosure requirements in this context illustrates some important considerations. When it was first given responsibility for regulating P2PL in the United Kingdom, the FCA decided to treat investments on P2PL platforms in a manner similar to other investments, making them subject to the same generic disclosure rules.[565] These included obligations applying to all communications with retail investors, such as an obligation that they must indicate any relevant risks when referencing potential benefits.[566] They also included having to provide retail clients with the following kinds of information in good time before the operator provides a relevant service and their client makes a relevant transaction through the platform:

- Matters such as the operator's authorization and contact details, conflicts of interest policy and client money safeguards, performance reports the client should expect, and costs and charges.[567]
- A description of the nature and risks of the relevant investments in sufficient detail to enable the client to make investment decisions on an informed basis. Although, as discussed below, the FCA declined to mandate standardized form and content of disclosures (as was the case for collective investment schemes), the FCA did choose to provide guidance in its rules, offering detailed examples of information that P2PL operators advising on P2P loans or loan portfolio should provide to explain relevant specific nature and risks. The range of examples listed includes expected and actual default rates, a description of how loan risk is assessed, whether a P2P loan benefits from any security and, if so, what, and an explanation of procedures to deal with loans in default.[568]

Several years after P2PL operators became subject to these disclosure requirements, the FCA said that it had seen numerous examples of poor disclosures that needed to be addressed through more granular disclosure requirements.[569] In recently strengthening disclosure requirements, the FCA sought to focus further on the need for lenders/investors to have sufficient information about the risks they were exposed to by participating in P2PL, the nature of the investment opportunities, and the role of the platform operator. As a result, it has now imposed a range of additional detailed disclosure require-

ments on P2PL operators, including to provide lenders/investors with the following:[570]

- A description of the role of the platform operator, particularly so lenders/investors are able to understand the services being provided by the platform, including key matters in relation to which they have responsibility and how they will discharge that responsibility (such as price determination, assembly of loan portfolios, and dealing with late repayments or defaults).[571]
- Information about what could happen to the ongoing administration of P2P loans and portfolios in the case of platform failure.[572]
- Information about the investment that is made through a P2PL platform. The FCA mandates detailed minimum content requirements for information that a platform operator must provide in relation to P2PL agreements, varying (depending on the P2PL business model) according to whether loans are to be selected by the lender/individual investor directly or selected for the lender/investor by the operator.[573]

Some regulators have prescribed less detailed disclosure rules than found in China or the United Kingdom, but the rules they have implemented also contemplate that P2PL operators must provide the public or prospective lenders/investors with broad-ranging information. The RBI requires that P2PL operators disclose to lenders/investors details about the borrower, including relating to their identity, the amount sought, the interest rate sought, and the credit score determined by the operator, as well as details about all the terms and conditions of the loan, including likely return fees and taxes. In addition, operators are required to disclose publicly on their website an overview of their credit assessment/score methodology and factors considered, disclosures on usage/protection of data, information about grievance redressal mechanisms, portfolio performance, including share of non-performing assets on a monthly basis and segregated by age, and their business model.[574] Similarly, Indonesia's OJK mandates various disclosure requirements, such as regarding the required minimum content of agreements between a P2PL operator and individual lenders/investors, and regarding information about individual loans.[575] As discussed above, OJK also requires that applicants to become an online lender provide proof of membership in a fintech association, such as AFPI, whose code of ethics also mandates disclosure requirements.

Regulations made by the Mexican Banking and Securities Commission (*Comisión Nacional Bancaria y de Valores*, or CNBV) impose a general obligation on crowdfunding platforms (including P2PL operators) to disclose in relation to financing offers information about relevant analysis and other variables useful for lenders/investors to make informed investment decisions. In addition, the regulations prescribe items of information that must be disclosed by P2PL operators facilitating loans for personal purposes between individuals, including, in addition to loan details, risk ratings accompanied with a simple explanation of the methodology to determine them, arrangements related to risk sharing, and information about the applicant, such as income sources.[576] Mexico's National Commission for the Protection and Defense of Users of Financial Services (CONDUSEF) also recently introduced detailed mandatory content requirements for agreements below a prescribed monetary threshold.[577]

The Brazilian authorities have also implemented specific disclosure requirements for P2PL operators to provide to lenders/investors. Operators must display prominently on their website and other electronic channels and also include in contracts, advertising and promotional materials, and other consumer documents information about the nature and complexity of relevant P2PL services.[578] Operators must also provide prospective lenders/investors with expected rates of return, taking into account expected payment flows, taxes, fees, insurance, and other expenses.[579] To inform prospective lenders/investors of the performance of loans facilitated by a platform, an operator must publish on a monthly basis the average default rates over the last 12 months for loans they have facilitated, by risk classification.[580] They must also include a range of details to be provided to lenders/investors in P2P loan agreements regarding the loan and the rights, obligations, and responsibilities between the investor, borrower, and platform operator.[581]

Under new legislation on P2PL passed by Korean authorities in 2019, P2PL operators are required to provide lenders/investors with a range of information, including information relating to P2P loans, borrowers, risks relating to P2P loans, fees, rates of return, and debt collection procedures.[582] In addition, they must publicly disclose information regard their transaction structure, financial and business status, loan amounts, systems for evaluating borrowers' ability to repay loans, default rates, interest rates, fees and other changes, and repayment collection methods.[583]

Mandated warnings and disclaimers

As commentators often rightly note, warnings are not a substitute for other measures to assist lenders/investors to make informed decisions, but obliging P2PL operators to provide certain warnings or dis-

claimers in key contexts can nevertheless highlight risks for consumers and assist in balancing out inappropriately optimistic perceptions. A now common international practice is to require platform operators to warn lenders/investors that their returns are not guaranteed and that they could lose their investment if the borrower receiving the loan fails. Additionally, operators must also state that the funds invested are not protected by a deposit-guarantee scheme.[584] Focusing on another area of frequent concern, P2PL operators in the United Kingdom are subject to general rules on disclosure of past performance that include providing a prominent warning that past performance is not a reliable indicator of future results.[585] In the United Kingdom, platforms that offer contingency funds (to cover some losses that lenders/investors may suffer in investing through a platform) are also required to provide an up-front warning containing wording prescribed by the regulator.[586] The FCA has also prescribed where (in a prominent place on every page of each website and mobile application available to lenders/investors containing any reference to a contingency fund, or where relevant in other documents in good time before any business is carried out for that lender/investor) and how (contained within its own border and with bold text as indicated) such a warning must be displayed.[587] In a similar vein, the Brazilian authorities require that P2PL operators display on their website and other electronic channels, as well as in promotional materials, contracts, and other consumer documents, a prominent warning that P2P loans constitute risky investments and are not subject to deposit insurance.[588] P2PL agreements must also specify that the platform operator is not liable and does not provide any type of guarantee in connection with repayment of a loan.[589]

In some jurisdictions, warnings are also coupled with acknowledgments from lenders/investors. The RBI requires P2PL operators to obtain explicit confirmation from a prospective lender/investor that they understand the risks associated with the proposed transaction and that there is no guarantee of return and that there exists a likelihood of loss of the entire principal in case of default by a borrower, including a summary sheet.[590] The Brazilian authorities similarly require that P2PL agreements include an acknowledgment from the lender/investor that they are aware of the risks of the relevant transaction loan and financing.

It would be important to ensure, however, that any such warnings or acknowledgments are not seen by regulators or P2PL operators as reducing the need to address consumer vulnerabilities. For example, despite acknowledging otherwise—perhaps unwittingly—a consumer may not in fact have been made appropriately aware of relevant risks. It is also important to keep such measures from creating an erroneous perception in FSPs or consumers that they shift the onus to mitigate relevant risks from the former to the latter more generally.

Risk: Information is provided in an inadequate format

A lack of uniform, well-designed standards for conveying information may mean that information is not effectively conveyed by P2PL operators. Even if lenders/investors are provided with sufficient information when considering investing in P2PL, they may not be able to identify the most important information out of the range of accessible information. A commentator notes that in the United States, lenders/investors are offered dozens of categories of information that can be material or immaterial, verified or unverified, voluntary or mandatory.[591] A lack of standardization also makes it difficult to compare or assess the risks and returns of competing investment options.[592]

Shortcomings can relate to both the format of disclosure and the way content is formulated. A commentator noted that in Europe, platforms might publish details such as gross interest rates, bad debt rates, and default on their websites. However, methods used to calculate risk-adjusted net returns differed considerably between platforms due to a lack of common standards for performance of P2PL investments.[593] Of course, platform operators also may not make sufficiently clear the methodology used to make such calculations.

Regulatory approaches to address inadequate disclosure formats

To address risks that information may not be conveyed effectively to lenders/investors, or may not be easily comparable, some regulators have also imposed requirements for how information must be presented. However, these tend to be relatively general rules for matters such as how information should be displayed and positioned on websites. For example, disclosure requirements imposed by authorities in Brazil include an obligation that relevant information be displayed prominently on relevant electronic channels.[594] Requirements that apply in China include that mandated disclosures must be set out in a dedicated, conspicuous section of websites and equivalent electronic channels.[595]

Some regulators have implemented requirements for certain disclosure documents to be provided to lend-

ers/investors in a standardized format. CONDUSEF in Mexico has mandated a standardized format for a summary sheet that must be provided in or with P2PL agreements.[596] However, such requirements do not appear to be as widespread as information content requirements. Even regulators who have developed very detailed content requirements for P2PL disclosure, such as in China or the United Kingdom, do not seem to be mandating standardized formats for such disclosure yet. The FCA consulted publicly on whether it would be helpful to consumers and industry to have a standardized format for P2PL disclosures (such as the key investor information document it mandated for collective investment schemes). However, it concluded that, due to the range of views received from stakeholders and the perceived difficulty in standardizing information in a meaningful way for a diverse sector, it would not develop a standard template but would keep the issue under review. The FCA's view was that consumers' difficulties in comparing information across platforms was primarily due to the diverse nature of the sector, not to the lack of a standardized format. Avoiding mandating a standardized format would, in its view, ensure that disclosures would be appropriately tailored to the specific characteristics of a platform's business model and service offering and allow sufficient flexibility to accommodate the continued evolution of the sector.[597]

Risk: Unbalanced or misleading marketing

It is not unusual for P2PL operators, as is often the case with other FSPs, to highlight positive aspects to attract lenders/investors and expand their market share. At the most concerning end of the spectrum would be providing information that, by action or omission, is misleading to investors. It was observed during the development of the Chinese P2PL market that P2PL operators focused on aspects such as average returns if they appeared attractive, without highlighting associated risks sufficiently.[598] Similarly, the regulator and other commentators in the United Kingdom highlighted concerning practices such as promoting past performance without warning that it was not an indicator of likely future performance and making inappropriate comparisons between investing funds in P2PL and placing them on deposit.[599]

Regulatory approaches to address unbalanced or misleading marketing

General prohibitions against providing misleading information are an important measure in FCP regulatory frameworks generally[600] and clearly relevant in relation to P2PL. Where a separate regulatory regime is developed for P2PL, such general prohibitions would be appropriate. In China, the CBIRC's Guide to the Disclosure of Information on Business Activities of Peer-to-Peer Lending Information Intermediaries[601] states, among other things, that prescribed information must meet such general criteria as being accurate and not contain misleading statements or major omissions.[602]

Regulators have also sought to use more targeted regulations to address circumstances that present a higher risk of misleading lenders/investors. For example, a P2PL operator in the United Kingdom is subject to rules on the disclosure of past performance to mitigate the risk of inappropriate reliance by lenders/investors (for example, a restriction on giving it prominence in a communication, parameters regarding how indicators of such performance may be determined, and a prominent warning as to its value).[603] They are also subject to rules on disclosure of comparative information in relation to investments. As an example of inappropriate comparisons that would be in breach, the FCA cites making direct comparisons between investing money in P2PL and holding money on deposit.[604]

Some regulators have sought to leverage general misleading conduct and fair treatment prohibitions to target specific issues affecting P2PL through associated guidance. This is particularly important where, given the novelty of the business models and offerings involved, it could be less clear to industry whether communications may mislead consumers. For example, the Financial Markets Authority of New Zealand issued a guidance note titled "Fair Dealing in Advertising and Communications—Crowdfunding and Peer-to-Peer Lending" for licensed crowdfunding and P2PL platforms. The note is intended to give guidance on the application to crowdfunding and P2PL products of the general fair dealing requirements in the New Zealand Financial Markets Conduct Act. The guidance focuses on matters such as the need to balance representation about risk and reward in the context of such platforms and providing performance information appropriately, giving contextualized examples.[605] In the United Kingdom, in addition to implementing detailed regulatory requirements with regard to the disclosure, the FCA has repeatedly issued guidance on P2PL practices that could mislead consumers and thus should be adjusted. For example, it has highlighted P2PL platforms that offer a target rate of return promoting maximum target rates in ways that lenders/investors might easily mistake for fixed or guaranteed returns.[606] In Australia, ASIC has highlighted similar issues in guidance targeted at P2P lenders that also relies on existing obligations under FCP legislation of general application to consumer credit and other financial products.[607]

Risk: Inadequate ongoing information

Even if lenders/investors receive adequate information prior to entering into P2PL credit and investment agreements, they may not be provided with adequate ongoing disclosure of material changes to their loans, such as borrower defaults.[608] As a result, they may be less able to make appropriate ongoing decisions regarding their investments and to react to adverse changes.

Regulatory approaches to address inadequate ongoing information

Jurisdictions are increasingly requiring P2PL operators to provide lenders/investors with ongoing information about their individual loans/investments, as well as other matters relating to the platform that may affect those loans. In China, a P2PL operator must provide to lenders/investors, on a monthly or quarterly basis (depending on loan term), prescribed ongoing information in relation to their individual loans, including changes to the borrower's financial circumstances and repayment ability, any overdue repayments and additional charges imposed on the borrower, and other matters that may affect their position.[609] In Brazil, lenders/investors must similarly be provided with ongoing information about defaults relating to their loans.[610] The regulations in Mexico also mandate the ongoing provision of information to lenders/investors regarding their loans, such as the current status of the loan and the borrower's repayment performance.[611] In the United Kingdom, operators must ensure that, at any point in time, a lender/investor is able to access a range of details about each of their loans, such as pricing, the borrower's interest rate, a fair description of the likely actual return, taking into account fees, default rates and taxation.[612] These are in addition to existing general obligations to provide lenders/investors with written confirmations of transactions and periodic statements.[613]

Lenders/investors may also benefit from periodic updates regarding the general performance of the P2PL operator, as well as notices of adverse events. P2PL operators in the United Kingdom that set the price of loans/loan investments must publish an annual "outcomes statement" that includes the expected and actual default rate of all P2P loans by risk category, a summary of the assumptions used in determining expected future default rates, and actual returns achieved (where a platform offered a target rate).[614] Operators in China are required to disclose publicly within 48 hours if they have been affected by any of a range of adverse circumstances, such as bankruptcy events, cessation or suspension of business operations, significant litigation, fraud, or other incidents affecting its operations in a manner that may damage borrowers' interests, or if their management or other key staff or representatives are subject to circumstances such as litigation, investigation by law enforcement, or criminal or major administrative sanctions.[615] Such disclosures must include the possible impact of an event and measures being taken to address it.

b) Harm due to lenders'/investors' lack of sophistication or inexperience

Risks to consumers

Even if lenders/investors are provided with adequate information about P2PL, they may be exposed to harm due to a lack of investing skills or sophistication. This risk can be exacerbated by the fact that, as already discussed above, P2PL often entails more complex and riskier aspects than widespread or simpler types of investments that consumers may be familiar with. For example, as noted by the EBA, the assessment of a P2PL opportunity can require a fairly thorough and profound analysis and understanding of a potential borrower. A lender/investor would need a certain level of financial literacy to be able to make a fully educated decision about a specific investment opportunity.[616] Even assuming, as discussed earlier, that the P2PL operator undertakes a credit assessment of a borrower, to make effective decisions an investor must be able to understand sufficiently both the implications of the operator's assessment and its limitations. It may also be the case that a P2PL operator does not have sufficient information or understanding about an individual investor/lender's lack of skills or sophistication. This may be due to a lack of effort or the unavailability of data.

Regulators have also expressed concern about the risk that P2PL may expose lenders/investors to excessive losses having regard to their financial and other personal circumstances. The FCA noted recently (but pre-COVID-19) that, while losses and defaults in their P2PL sector had been low, it was important to recognize that the sector both was relatively new and had not been through a full economic cycle. When economic conditions tighten, losses on loans could increase.[617] While the FCA could not quantify the number of lenders/investors at risk of overexposure, in a survey of 4,500 investors, 40 percent said they had invested more than their total annual income, and, of those, half had invested more than double their annual income.[618] Unfortunately, the impact that the COVID-19 crisis is having on P2PL is demonstrating the potential impact of downturns.[619]

Regulatory approaches

Lending/investment caps and appropriateness requirements

Many jurisdictions have implemented investment or lending caps for lenders/investors.[620] These limits frequently apply only to lenders/investors that are considered less sophisticated or otherwise more vulnerable. Lending/investing caps can be implemented on a variety of bases, such as permitting a lender/investor to invest a maximum amount per borrower, within a certain period of time or depending on their income or assets.[621] Internationally, the level of such caps varies significantly.

As is the case with other retail investor protection measures, a lender/investor's income or assets are often used as proxies to indicate greater vulnerability or lesser sophistication. This link may not necessarily always be borne out in practice. Nevertheless, setting caps on such a basis can also assist to protect lenders/investors from losses that may have a greater financial impact on lower levels of assets or income.

Another approach to address such risk can be to require a P2PL operator to evaluate the financial literacy, and relevant experience and knowledge, of individual lenders/investors and categorize them accordingly. A lender/investor would be permitted to invest only in lending deemed suitable for their risk categorization.[622]

The FCA recently decided to extend to P2PL marketing restrictions that already applied to investment-based crowdfunding.[623] The application of the restrictions depends on both prospective clients' experience and sophistication, as well their financial circumstances. The restrictions also take into account whether clients may be receiving regulated investment advice that could also act as a mitigant against lack of experience or sophistication. The new rules mean that P2PL operators are permitted to promote P2PL opportunities to retail clients only under one the following circumstances:

- If clients are certified or self-certified as "sophisticated investors" or are certified as "high-net-worth investors".
- If the operator confirms before a promotion is made that, in relation to the investment being promoted, the retail client will receive regulated investment advice or investment-management services from an authorized person.
- If the retail client will be certified as a "restricted investor," which means that they will not invest more than 10 percent of their net investible assets in P2P loans in the 12 months following certification.[624]

In addition, where no advice is given to a retail client in relation to investing in P2PL (which itself would need to comply with regulatory requirements as to its appropriateness), the operator must undertake an appropriateness assessment before the client can invest in P2PL. The operator is required to determine whether the client has the necessary experience and knowledge in order to understand the risks involved in relation to the P2PL opportunity being offered.[625] The FCA has included guidance with its new rules suggesting a range of multiple-choice questions (avoiding binary yes/no answers) that operators should consider asking clients. They relate, for example, to the client's exposure to the credit risk of the borrower, their potential loss of capital, and their understanding that investing in P2PL is not comparable to depositing money in a savings.[626]

The FCA's decision to apply these restrictions appears to reflect its evolving views—drawing from its monitoring of the lending market—regarding the risks that P2PL presents for more vulnerable lenders/investors. In 2013, the FCA had indicated that its approach to mitigating relevant risks was to place a particular focus on the quality of P2PL operators' disclosure, including financial promotions. However, following a review in 2018, the FCA expressed views that many of the risk characteristics inherent in the investment-based crowdfunding market also existed in the P2PL sector, and that those characteristics could similarly expose lenders/investors to potentially unsuitable, risky assets.[627] There was significant industry resistance to the application of these restrictions to P2PL. Respondents to public consultations argued that imposing a marketing restriction was a disproportionate and "blunt tool" to achieve the FCA's stated consumer protection objective.[628] However, the regulator maintained its view that the restrictions—particularly the investment cap for restricted lenders/investors—were an important means of ensuring that retail investors who are new to the P2PL asset class do not overexpose themselves to risk. Investors could always be reclassified as sophisticated investors (removing the 10 percent investment limit) when they had more experience. The FCA also considered whether it would be possible to apply the proposed marketing restrictions in a targeted way, only to platforms with the riskiest investment strategies. However, it dismissed this option, finding significant practical challenges in doing so.[629]

Concerns that P2PL opportunities should be made available only to lenders/investors for whom they are deemed appropriate were echoed recently by commentators in China given adverse developments in that market. [630] The Chinese authorities similarly introduced rules requiring P2PL operators to apply restric-

tions on lenders/investors' access to P2PL opportunities depending on their personal circumstances. However, they have not prescribed particular categories of investor restrictions based on which such restrictions should apply. Rather, the Interim Measures for the Administration of the Business Activities of Online Lending Intermediary Institutions require an operator to carry out an assessment of the age, health, financial status, investment experience, risk preference, and risk-bearing capacity of a prospective lender/investor. The operator is required to establish its own lending limits and restrictions on lending subject matter that it applies to individual lenders/investors based on their risk-assessment results.[631] Such an approach places a significant onus on P2PL operators to identify appropriate investor categories that will not subsequently be viewed as in breach of requirements by the authorities. They may also result in significant variation in approaches, potentially leading to gaps in protection or differences in market performance.

The RBI has imposed a general obligation on P2PL operators to undertake due diligence on lenders/investors without prescribing restrictions based on specific characteristics.[632] However, it has also imposed both a cap on the total loans that a lender/investor may make of ₹1 million and a cap of ₹50,000 on a lender/investor's exposure to any individual borrower.[633] The rules introduced by the Brazilian authorities take a similar approach, imposing a cap for unsophisticated investors of R$15,000 per borrower on the same platform.[634] They also impose a general obligation on operators to analyze the risk profile of prospective lenders/investors to determine if P2PL is suitable for that risk profile.[635]

The implementation of monetary caps on lending appears to be widespread in the European Union[636] and growing internationally.[637] For example, in France, caps for individual lenders/investors apply of €2,000 per loan if interest-paying or €5,000 if interest free, while Spain has prescribed limits on a per-loan and total annual basis (of €3,000 and €10,000, respectively) for unaccredited investors. Accredited investors not subject to such limits include (in addition to institutional investors and companies that meet certain asset and turnover thresholds) individuals with €50,000 of annual income or €100,000 of financial assets or companies.[638] Regulations made by the Mexican Banking and Securities Commission under Mexico's Financial Technology Institutions Law impose limits on the percentage of a lender/investor's total investment in a platform that can be allocated to a single borrower. For loans between individuals, the limit is 7.5 percent.[639] The Korean authorities recently passed a new law, the Act on Online Investment-Linked Finance and Protection of Users, that on commencement was to provide an overall investment cap of ₩50 million. However, prior to the legislation coming into effect, the responsible authorities under the legislation (the Financial Services Commission and Financial Supervisory Service) announced new regulations under the law that would impose a new lower limit for individual lenders/investors of ₩30 million, taking into account increased levels of credit risk amid the COVID-19 crisis.[640]

Borrowing limits

Some jurisdictions have implemented caps on the amount that individual borrowers may borrow through P2PL platforms, as another way to reduce credit risk and thus ultimately risk of loss to lenders/investors on a platform. The Chinese authorities' Interim Measures for the Administration of the Business Activities of Online Lending Intermediary Institutions impose a general obligation on P2PL operators to set limits on individual borrowers' total loan balances with individual platforms and across platforms. In addition, they specify caps on the total loan balances a borrower may hold through any single platform of ¥200,000 for natural persons and ¥1 million for legal persons. Limits of ¥1 million and ¥5 million have been set for total loan balances of a natural person or a legal person, respectively, across multiple platforms.[641] Commentators in China have noted that these lending limits are viewed as a key regulatory tool introduced under the Interim Measures, consistent with the policy view (stated in the Interim Measures themselves) that P2PL is generally intended to be undertaken for small-value finance. They are also aligned with limits under separate regulation prohibiting illegal public fundraising. However, industry participants have also complained that the limits that have been set may unduly restrict the amount of credit being made available.[642]

The RBI has imposed a cap of ₹1 million on the aggregate P2P loans taken out by a borrower at any point in time.[643] It is notable that some jurisdictions have implemented aggregate borrowing caps across P2PL platforms. Of course, a key element in facilitating P2PL platforms' ability to monitor and adhere to such caps would be ensuring availability of reliable credit reporting information across those platforms (as noted earlier in the context of creditworthiness assessment requirements). OJK in Indonesia has limited itself to prescribing a loan cap for P2PL platforms of Rp 2 billion per borrower.[644]

Compensation funds

A measure considered by some authorities and commentators is the implementation of contingency funds to provide compensation to lenders/investors in the event of loss. Such a fund would be relevant, for example, where a P2P loan is unsecured or realization of the

security would be insufficient to cover potential losses. However, their adoption—at least as a regulatory measure—does not seem widespread. Most jurisdictions currently do not appear to regulate such funds that may be offered for individual P2PL platforms.[645]

Authorities have expressed concerns regarding the effectiveness of such funds as well as their potential downsides. The FCA noted that some P2PL platforms operating in its jurisdiction offered contingency funds intended to top up payments made to lenders/investors in the event of a borrower's default. While acknowledging the intention to protect lenders/investors, the FCA expressed concern (echoed by other commentators)[646] that such funds can lead them to misunderstand that platforms are providing a guaranteed return on the loans they facilitate, driven by potentially misleading advertising or claims with regard to such funds. Another concern raised relates to the variation in the ongoing level of funding for such funds. As a result, while the FCA decided not to prohibit P2PL platforms from operating a contingency fund, it made clear its expectations that operators not rely on them in place of good risk management and that operators run them appropriately and explain their operation and limitations properly to potential investors. It also noted that in the United Kingdom, if a contingency fund is designed to provide lenders/investors with an enforceable right to claim against it for losses arising on borrower default, then providing the fund could constitute the provision of insurance, attracting corresponding regulatory requirements.[647] This issue would also be relevant under other jurisdictions' insurance regulatory regimes.

c) Borrower fraud

Risks to consumers

Lenders/investors could suffer the loss of their funds if these are provided to fraudulent borrowers. This may result not only where an applicant is an impostor intending to abscond with the funds as soon as an application is approved but also if aspects of an application from a genuine borrower are fraudulent, such as their declared income.

Regulatory approaches

Risk management requirements

The risk management requirements already discussed above could also act as a mitigant against borrower fraud. Obligations on a P2PL platform operator to obtain not only appropriate identification information about borrowers but also information about matters such as their financial status and potential criminal background would obviously assist in this context, as would requiring the operator to deny access to their platform if they have reason to believe that a borrower might potentially act fraudulently.[648] Such measures should also be partial elements of compliance with broader obligations discussed earlier in the chapter to have in place appropriate risk management systems.

Beyond FCP requirements, P2PL operators should of course be subject to mitigating obligations under a jurisdiction's AML/CFT laws. These would require them to apply "know your customer" systems and processes to prospective borrowers.

Creditworthiness assessment requirements

The creditworthiness assessment requirements also already discussed above could act as a mitigant against borrower fraud. As a commentator notes, an additional benefit of requiring appropriate verification of borrower information for the purposes of credit-risk and creditworthiness assessments is that such verification can also assist in mitigating against the risk of fraudulent borrowers.[649]

5.4 ADDITIONAL CONSUMER RISKS FOR BORROWERS

a) Inadequate loan-related information

Risks to consumers

Regulators in a range of jurisdictions, such as the European Union[650] and China,[651] have recognized the risks of borrowers on P2PL platforms not receiving adequate information or being misinformed with regard to their loans. This can lead borrowers to unwittingly take up unsuitable loans or not to understand their rights or obligations in relation to such loans. Such risks can arise in part if, as discussed above, P2PL is not adequately covered by existing FCP requirements addressing transparency and disclosure, as well as product design and suitability requirements for credit products. Such requirements may also require tailoring to P2PL activities to be effective.

Regulatory approaches

Extend application of existing traditional credit disclosure requirements

Existing borrower disclosure requirements that already apply to credit provided by traditional lenders could address at least some information needs of P2PL borrowers. For example, in the United States, the lender of record for a P2P loan is subject to the provisions of TILA. TILA requires lenders to provide borrowers with specified information regarding the T&C of their loans as well as changes to these in a prescribed standardized format. The prescribed information differs depending

on the nature of the loan being made. Commentators noted that previously it would have been more difficult to ensure compliance with the TILA requirements in a P2PL context where the lender of record were the individual lenders/investors. However, the registration requirements imposed by the securities regulator discussed above have effectively forced P2PL operators to issue loans to borrowers in the operator's own name, making them subject to TILA disclosure requirements.[652] P2PL operators that offer credit to Australian consumers would similarly be subject to precontractual and contractual disclosure requirements. They include, among other things, obligations to provide to consumers documents known as "credit guides" when proposing to provide credit-related services. A credit guide must provide a range of information about the credit services, such as details of the relevant credit licensee, potential fees, charges, and commissions, and complaints-resolution mechanisms.[653] They also include content and form requirements for "precontractual statements" and "information statements" to be provided to a consumer before a credit contract is entered into, as well as for final credit contracts.[654]

Tailored disclosure requirements

Some jurisdictions have sought to address gaps in existing borrower disclosure regimes by developing requirements specific to P2PL. The Indian[655] and Indonesian[656] authorities, for example, have obliged P2PL operators to provide borrowers specific information relating to their loan T&C; Indonesia's OJK prescribes a list of content requirements for P2PL agreements. CONDUSEF has mandated a standardized format for a summary sheet that must be provided in or with P2PL agreements.[657] On the other hand, while, as discussed above, the Chinese authorities have implemented an extensive disclosure regime for P2PL as part of recent reforms, particularly with regard to disclosures to lenders/investors, the regime does not appear to set out significant prescriptive requirements for disclosures to borrowers (although it does require disclosure of a range of information to the public more generally).[658]

b) Risks from digital provision of P2PL credit

Chapter 4 (on digital microcredit) discusses a range of important risks that arise from, or are exacerbated by, the provision of credit through digital means. They include, for example:

- Obstacles to conveying information effectively via digital means (see section 4.2).
- Significant risks emerging from greater reliance on automated decision-making and the use of algorithms (see section 4.5).

Such risks and corresponding regulatory approaches are also highly relevant to the provision of credit through a P2PL platform.

NOTES

406 Balyuk, "Financial Innovation and Borrowers," 7.
407 ASIC, *Survey of Marketplace Lending Providers* (Report 526), para 17–18.
408 See, for example, ASIC, *Marketplace Lending.*
409 See, for example, FCA, *FCA's Regulatory Approach to Crowdfunding (and Similar Activities),* para 1.14.
410 See, for example, EC, *Crowdfunding Explained*, 14.
411 Karakas and Stamegna, "Defining an EU-Framework," 107.
412 Such as "P2P marketplace lending"—see, for example, Owens, "Responsible Digital Credit."
413 Committee on Global Financial System and Financial Stability Board Working Group, *FinTech Credit,* 11.
414 Committee on Global Financial System and Financial Stability Board Working Group, *FinTech Credit,* 11–13.
415 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20), para 3.9–3.2.
416 CCAF, *Global Alternative Finance Market Benchmarking Report*, 24.
417 *Financial Times*, "Ant Posed Threat to China's Centralised Control."
418 Duoguang, "Growing with Pain," 42; Huang, "Online P2P Lending," 65–68. See also World Bank Group, *Capital Markets and SMEs,* 60–61.
419 Liu, "Dramatic Rise and Fall."
420 Cornelli et al., *Fintech and Big Tech Credit*, 9–10.
421 World Bank Group and CCAF, *Regulating Alternative Finance*, 59.
422 Owens, "Responsible Digital Credit," 8–9.
423 See Huang, "Online P2P Lending," 77.
424 Hornby and Zhang, "China's Middle Class."

425 *Financial Times*, "Ant Posed Threat to China's Centralised Control."
426 Megaw, "Peer-to-Peer Groups Battle"; Makortoff, "Peer-to-Peer Lender Funding Secure."
427 FCA, *FCA's Regulatory Approach to Crowdfunding (and Similar Activities)*, para 1.14.
428 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20), para 3.2–3.3.
429 See, for example, Rahman, "'They Terrorized Me Every Day.'"
430 See, for example, Faridi, "P2P Fintech Lending Sector in Indonesia."
431 Central Bank of Ireland, *Consumer Notice on Crowdfunding.*
432 EBA, "Opinion of the European Banking Authority," para 118–119.
433 EC, *Crowdfunding in the EU Capital Markets Union,* 27.
434 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP19/14), para 4.1–4.4.
435 Davis and Murphy, "Peer-to-Peer Lending," 37.
436 See National Consumer Credit Protection Act 2009 (Cth) (Australia), ss. 6 and 29 (requirement to be licensed if undertaking credit activities). The Act also applies a broad range of conduct and disclosure obligations when engaging in credit activities involving consumers.
437 See Corporations Act 2001 (Cth) (Australia) s. 911A and Chapter 7, Division 4 (requirement to be licensed if providing financial services) and s. 601ED (requirement to register a management investment scheme). The Act also applies a broad range of conduct and disclosure obligations, primarily when providing financial services to retail clients.
438 Samitsu, "Structure of P2P Lending and Investor Protection."
439 Money Lending Business Act No. 32 of May 13, 1983 (Japan).
440 Money Lending Business Act No. 32 of May 13, 1983 (Japan), Chapter II; CCAF, *Third Asia Pacific Region Alternative Finance Industry Report*, 80–81.
441 As part of the transfer of responsibility for consumer credit regulation from the Office of Fair Trading (which had licensed a limited number of P2P lending platforms) to the FCA.
442 Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (SI 2001/544) (UK), art. 36H, and FCA, *FCA's Regulatory Approach to Crowdfunding (and Similar Activities)*, para 2.8.
443 Intergovernmental Fintech Working Group, *IFWG Fintech Workshop 19–20 April 2018,* 22.
444 See, for example, FCA Consumer Credit Sourcebook—October (UK), 4.3 and 5.5A.
445 National Monetary Council Resolution Number 4,656 of April 26, 2018 (Brazil).
446 National Monetary Council Resolution Number 4,656 of April 26, 2018 (Brazil), art. 14.
447 See Ehrentraud et al., *Policy Responses to Fintech*, 17.
448 Guiding Opinions on Promoting the Healthy Development of Internet Finance 2015 (China), art. 2.
449 Interim Measures for the Administration of the Business Activities of Online Lending Intermediary Institutions 2016 (China).
450 Interim Measures for the Administration of the Business Activities of Online Lending Intermediary Institutions 2016 (China), art. 10. See also Duoguang, "Growing with Pain," 52–53.
451 Online Investment-Linked Finance and Protection of Users Act 2019 (Korea); Shin & Kim, "National Assembly Passes New Law."
452 Emergency Decree No. 013-2020-JUS/DGTAIPD 2020 (Peru), Title IV.
453 Financial Technology Institutions Law 2018 (Mexico).
454 Financial Technology Institutions Law 2018 (Mexico), art. 15–16.
455 Law on Transparency for Financial Services, 15 June 2007 (Mexico).
456 Reserve Bank of India, *Report of the Working Group on FinTech and Digital Banking*, para 5.1.1.
457 RBI NBFC—Peer to Peer Lending Platform Directions 2017 (India).
458 Regulation of the Financial Services Authority Number 77/POJK.01/2016 Concerning Information Technology-Based Loan Services (Indonesia), Chapter II Part 4.
459 Regulation of the Financial Services Authority Number 77/POJK.01/2016 Concerning Information Technology-Based Loan Services (Indonesia), art. 48.
460 Securities Act 1933 15 USC § 77a.
461 See, for example, Lo, "If It Ain't Broke," 88–89.
462 Samitsu, "Structure of P2P Lending and Investor Protection."
463 Financial Instruments and Exchange Act No. 25 of 1948 (Japan).
464 Financial Instruments and Exchange Act No. 25 of 1948 (Japan), Chapter III; CCAF, *Third Asia Pacific Region Alternative Finance Industry Report*, 80.
465 ASIC, *Survey of Marketplace Lending Providers* (Report 526), para 150–151.
466 See, for example, ASIC, *Marketplace Lending*.
467 EBA, "Opinion of the European Banking Authority," para B2 and C6.
468 Duoguang, "Growing with Pain," 50.
469 Duoguang, "Growing with Pain," 44.
470 EBA, "Opinion of the European Banking Authority," para 70 and 71.
471 RBI NBFC—Peer to Peer Lending Platform Directions 2017 (India), para 15.

472 Interim Measures for the Administration of the Business Activities of Online Lending Intermediary Institutions 2016 (China), Chapter II; Guide to the Administration of Recordation and Registration of Peer-to-Peer Lending Information Intermediaries (issued on October 28, 2016 by the China Banking Regulatory Commission and other authorities). See also Huang, "Online P2P Lending," 73–74.

473 Peer-to-Peer Lending Information Intermediaries of Guangdong Province—Detailed Implementation Rules for Recordation and Registration (Exposure Draft issued on 14 February 2017). See also Huang, "Online P2P Lending," 73–74.

474 FCA Principles for Businesses—October 2020 (UK), 2.1.1R (Principle 3).

475 FCA Senior Management Arrangements, Systems and Controls Sourcebook—October 2020 (UK), 4.1.1R and 7.1.3R.

476 Financial Technology Institutions Law 2018 (Mexico), art. 37.

477 This paper is not intended to cover prudential concerns and requirements. Of course, it is the case, however, that these overlap with consumer risks and FCP rules. For example, for a discussion of the relevance of capital requirements to P2PL entities' operational risks, see World Bank Group, *Prudential Regulatory and Supervisory Practices,* 17–19.

478 Committee on Global Financial System and Financial Stability Board Working Group, *FinTech Credit,* 26.

479 EBA, "Opinion of the European Banking Authority," para F1, 45, and 83.

480 Committee on Global Financial System and Financial Stability Board Working Group, *FinTech Credit,* 26.

481 Regulation of the Financial Services Authority Number 77/POJK.01/2016 Concerning Information Technology-Based Loan Services (Indonesia), art. 25; Financial Services Authority Circular Number 18/SEOJK.02/2017 Regarding Information Technology Risk Management and Management in Information Technology-based Lending (Indonesia).

482 Interim Measures for the Administration of the Business Activities of Online Lending Intermediary Institutions 2016 (China), art. 18.

483 See, for example, ASIC, *Survey of Marketplace Lending Providers: 2016–2017*, para 21.

484 RBI NBFC—Peer to Peer Lending Platform Directions 2017 (India), annex .

485 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 9(3).

486 Regulation of the Financial Services Authority Number 77/POJK.01/2016 Concerning Information Technology-Based Loan Services (Indonesia), art. 14.

487 FCA, *FCA's Regulatory Approach to Crowdfunding (and Similar Activities)*, para 3.19.

488 OJK, "OJK Issues Regulation on IT-Based Lending Services," 2.

489 EBA, "Opinion of the European Banking Authority," para D3 and 43.

490 IOSCO, *IOSCO Research Report,* 16; EC, "Inception Impact Assessment," 2.

491 FCA, *FCA's Regulatory Approach to Crowdfunding (and Similar Activities)*, para 2.24.

492 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20), para 3.51–3.52.

493 Davis and Murphy, "Peer-to-Peer Lending," 40.

494 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20), para 3.50–3.52.

495 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20), para 4.55.

496 See, for example, Owens, "Responsible Digital Credit," 5, 31.

497 EBA, "Opinion of the European Banking Authority," para 79–80.

498 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 10.

499 RBI NBFC—Peer to Peer Lending Platform Directions 2017 (India), para 9(1).

500 Regulation of the Financial Services Authority Number 77/POJK.01/2016 Concerning Information Technology-Based Loan Services (Indonesia), art. 24.

501 Online Investment-Linked Finance and Protection of Users Act 2019 (Korea) art. 26; Shin & Kim, "National Assembly Passes New Law."

502 FCA, *FCA's Regulatory Approach to Crowdfunding (and Similar Activities),* para 3.34–3.36. Also see FCA Client Assets Sourcebook—October 2020 (UK), 7, and FCA Senior Management Arrangements, Systems and Controls Sourcebook—October 2020 (UK) 4.1.8ER.

503 See Havrylchyk, *Regulatory Framework*.

504 Huang, "Online P2P Lending," 74–75; Duoguang, "Growing with Pain," 52, 54.

505 Guidelines for Online Lending Fund Depository Business (issued on February 22, 2017 by the China Banking Regulatory Commission).

506 Huang, "Online P2P Lending," 78–79.

507 National Monetary Council Resolution Number 4,656 of April 26, 2018 (Brazil), art. 13.

508 Havrylchyk, *Regulatory Framework*, 26.

509 EBA, "Opinion of the European Banking Authority," para 69.

510 FCA Senior Management Arrangements, Systems and Controls Sourcebook—October 2020 (UK) 4.1.8DBR-4.1.8DDR. See also FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP19/14), para 2.29–2.32; FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20), para 5.55–5.61; ASBA and IDB, *Global Fintech Regulation and Supervision Practices,* 22.

511 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20), para 4.55–4.57.

512 EBA, "Opinion of the European Banking Authority," para C7 and 48.

513 See, for example, the discussion of auto-bids and auto-selections based on parameters specified by investors and assessed by the platform against loans in Ziegler et al., *Shifting Paradigms*, 41.

514 See Committee on Global Financial System and Financial Stability Board Working Group, *FinTech Credit*, 26; Havrylchyk, *Regulatory Framework*, 22.
515 Grady et al., *Financial Consumer Protection and New Forms of Data*.
516 Committee on Global Financial System and Financial Stability Board Working Group, *FinTech Credit,* 26.
517 FCA Consumer Credit Sourcebook—October 2020 (UK) 5.5A.
518 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP19/14), para 4.1–4.6.
519 FCA Conduct of Business Sourcebook—October 2020 (UK), 18.12.5R–18.12.10R.
520 RBI NBFC—Peer to Peer Lending Platform Directions 2017 (India), para 6(1).
521 Online Investment-Linked Finance and Protection of Users Act 2019 (Korea), art. 20; Shin & Kim, "National Assembly Passes New Law."
522 Havrylchyk, *Regulatory Framework*, 23.
523 Xiao, "Improving China's P2P Lending Regulatory System," 462, and Huang, "Online P2P Lending," 88.
524 Huang, "Online P2P Lending," 88, and Duoguang, "Growing with Pain," 50.
525 See World Bank Group and International Committee on Credit Reporting, *Credit Scoring Approaches Guidelines,* and ICCR, *Use of Alternative Data*.
526 Owens, "Responsible Digital Credit," 18.
527 Havrylchyk, *Regulatory Framework*, 14.
528 ASIC, *Survey of Marketplace Lending Providers* (Report 526), para 67; ASIC, *Survey of Marketplace Lending Providers: 2016-2017*, para 45–46; ASIC, *Survey of Marketplace Lending Providers: 2017–2018*, para 46.
529 ASIC, *Survey of Marketplace Lending Providers* (Report 526), para 11–12 and 124.
530 *The Economist*, "Created to Democratise Credit."
531 Oxera, *Crowdfunding from Investor Perspective,* 25; FCA, *FCA's Regulatory Approach to Crowdfunding (and Similar Activities)*, 43 and 45.
532 Davis and Murphy, "Peer-to-Peer Lending," 40.
533 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20), para 4.36–4.37.
534 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20), para 4.42–4.46.
535 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20), para 5.39–5.40.
536 National Consumer Credit Protection Act 2009 (Cth) (Australia), s. 47(1)(b).
537 Corporations Act 2001 (Cth) (Australia), s. 912A(1)(aa).
538 FCA Principles for Businesses—October 2020 (UK),2.1.1R (Principle 8).
539 See, for example, EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 8(3)-(4).
540 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 12(2).
541 FCA Principles for Businesses—October 2020 (UK), 2.1.1R (Principle 6).
542 Corporations Act 2001 (Cth) (Australia), s. 601FC(1)(c).
543 National Consumer Credit Protection Act 2009 (Cth) (Australia), s. 158LE.
544 National Monetary Council Resolution Number 4,656 of April 26, 2018 (Brazil), art. 23.
545 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20), para 4.38–4.41.
546 FCA Conduct of Business Sourcebook—October 2020 (UK), 18.12.5R-18.12.10R.
547 FCA Conduct of Business Sourcebook—October 2020 (UK), 18.12.11R–18.12.15G.
548 FCA Conduct of Business Sourcebook—October 2020 (UK), 18.12.16R–18.12.17R.
549 Interim Measures for the Administration of the Business Activities of Online Lending Intermediary Institutions 2016 (China), art. 10.
550 Regulation of the Financial Services Authority Number 77/POJK.01/2016 Concerning Information Technology-Based Loan Services (Indonesia), art. 43.
551 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20), para 4.14–4.19.
552 IOSCO, *IOSCO Research Report,* 17.
553 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20), para 4.28–4.33.
554 Davis and Murphy, "Peer-to-Peer Lending," 40.
555 ASIC, *Marketplace Lending*.
556 EBA, "Opinion of the European Banking Authority," para C3 and 37; also see 47.
557 Lenz, "Peer-to-Peer Lending," 695.
558 Lenz, "Peer-to-Peer Lending," 695-696.
559 World Bank and CCAF, *Regulating Alternative Finance*, 47.
560 Interim Measures for the Administration of the Business Activities of Online Lending Intermediary Institutions 2016 (China), Chapter V.
561 Banking Regulatory Commission Guide to the Disclosure of Information on Business Activities of Peer-to-Peer Lending Information Intermediaries 2016 (China).
562 Banking Regulatory Commission Guide to the Disclosure of Information on Business Activities of Peer-to-Peer Lending Information Intermediaries 2016 (China), Chapter II and Attachment—Explanation on the Content of the Disclosure of Information.

563 Banking Regulatory Commission Guide to the Disclosure of Information on Business Activities of Peer-to-Peer Lending Information Intermediaries 2016 (China), art. 7–8 and Attachment—Explanation on the Content of the Disclosure of Information.
564 Banking Regulatory Commission Guide to the Disclosure of Information on Business Activities of Peer-to-Peer Lending Information Intermediaries 2016 (China), art. 9 and Attachment—Explanation on the Content of the Disclosure of Information.
565 FCA, *FCA's Regulatory Approach to Crowdfunding (and Similar Activities)*, para 3.1–3.5.
566 FCA Conduct of Business Sourcebook—October 2020 (UK), 4.5.2R–4.5.5G; FCA, *FCA's Regulatory Approach to Crowdfunding (and Similar Activities)*, para 3.56–3.60.
567 FCA Conduct of Business Sourcebook—October 2020 (UK), 6.1; FCA, *FCA's Regulatory Approach to Crowdfunding (and Similar Activities)*, para 3.62.
568 FCA Conduct of Business Sourcebook—October 2020 (UK), 2.2 and 14.3; FCA, *FCA's Regulatory Approach to Crowdfunding (and Similar Activities)*, para 3.64–3.68.
569 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20), para 5.65–5.66.
570 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP19/14), para 2.36–2.49. See also corresponding discussion of original proposals in FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20).
571 FCA Conduct of Business Sourcebook—October 2020 (UK), 18.12.24R.
572 FCA Conduct of Business Sourcebook—October 2020 (UK), 18.12.28R.
573 FCA Conduct of Business Sourcebook—October 2020 (UK), 18.12.26R–18.12.27R.
574 RBI NBFC—Peer to Peer Lending Platform Directions 2017 (India), para 9(1).
575 Regulation of the Financial Services Authority Number 77/POJK.01/2016 Concerning Information Technology-Based Loan Services (Indonesia), art. 19.
576 Banking and Securities Commission—General Provisions Applicable to Financial Technology Institutions, 10 September 2018, as amended 25 March 2019 (Mexico), art. 89–90.
577 Banking and Securities Commission—General Provisions of CONDUSEF on Transparency and Sound Practices Applicable to Financial Technology Institutions, 9 July 2019 (Mexico).
578 National Monetary Council Resolution Number 4,656 of April 26, 2018 (Brazil), art. 17.
579 National Monetary Council Resolution Number 4,656 of April 26, 2018 (Brazil), art. 18.
580 National Monetary Council Resolution Number 4,656 of April 26, 2018 (Brazil), art. 19.
581 National Monetary Council Resolution Number 4,656 of April 26, 2018 (Brazil), art. 12.
582 Online Investment-Linked Finance and Protection of Users Act 2019 (Korea), art. 22; Shin & Kim, "National Assembly Passes New Law."
583 Online Investment-Linked Finance and Protection of Users Act 2019 (Korea), art. 10; Shin & Kim, "National Assembly Passes New Law."
584 ASBA and IDB, *Global Fintech Regulation and Supervision Practices*, 21.
585 FCA Conduct of Business Sourcebook—October 2020 (UK), 4.6; FCA, *FCA's Regulatory Approach to Crowdfunding (and Similar Activities)*, para 3.72.
586 "The contingency fund we offer does not give you a right to a payment so you may not receive a pay-out even if you suffer loss. The fund has absolute discretion as to the amount that may be paid, including making no payment at all. Therefore, investors should not rely on possible pay-outs from the contingency fund when considering whether or how much to invest."
587 FCA Conduct of Business Sourcebook—October 2020 (UK), 18.12.33R–18.12.34R.
588 National Monetary Council Resolution Number 4,656 of April 26, 2018 (Brazil), art. 17.
589 National Monetary Council Resolution Number 4,656 of April 26, 2018 (Brazil), art. 12.
590 RBI NBFC—Peer to Peer Lending Platform Directions 2017 (India), para 12(2).
591 Lo, "If It Ain't Broke," 107.
592 Owens, "Responsible Digital Credit," 3.
593 Lenz, "Peer-to-Peer Lending," 695.
594 National Monetary Council Resolution Number 4,656 of April 26, 2018 (Brazil), art. 17.
595 Banking Regulatory Commission Guide to the Disclosure of Information on Business Activities of Peer-to-Peer Lending Information Intermediaries 2016 (China), art. 3.
596 Banking and Securities Commission—General Provisions of CONDUSEF on Transparency and Sound Practices Applicable to Financial Technology Institutions, 9 July 2019 (Mexico), art. 7 and Appendix 2.
597 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP19/14), para 2.40 and para 2.50–2.51.
598 Duoguang, "Growing with Pain," 49.
599 FCA, *FCA's Regulatory Approach to Crowdfunding over Internet*, para 3.75.
600 See World Bank Group, *Good Practices*, B1.
601 Banking Regulatory Commission Guide to the Disclosure of Information on Business Activities of Peer-to-Peer Lending Information Intermediaries 2016 (China).
602 Banking Regulatory Commission Guide to the Disclosure of Information on Business Activities of Peer-to-Peer Lending Information Intermediaries 2016 (China), art. 3–6.
603 FCA Conduct of Business Sourcebook—October 2020 (UK), 4.6; FCA, *FCA's Regulatory Approach to Crowdfunding (and Similar Activities)*, para 3.72.

604 FCA Conduct of Business Sourcebook—October 2020 (UK), 4.5.6R; FCA, *FCA's Regulatory Approach to Crowdfunding (and Similar Activities)*, para 3.74–3.75.
605 Financial Markets Authority of New Zealand, *Fair Dealing in Advertising.*
606 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20), para 4.9–4.12; Owens, "Responsible Digital Credit," 18.
607 ASIC, *Marketplace Lending.*
608 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20), para 4.26.
609 Banking Regulatory Commission Guide to the Disclosure of Information on Business Activities of Peer-to-Peer Lending Information Intermediaries 2016 (China), art. 9 and Attachment—Explanation on the Content of the Disclosure of Information.
610 National Monetary Council Resolution Number 4,656 of April 26, 2018 (Brazil), art. 24.
611 Banking and Securities Commission—General Provisions Applicable to Financial Technology Institutions, 10 September 2018, as amended 25 March 2019 (Mexico), art. 94.
612 FCA Conduct of Business Sourcebook—October 2020 (UK), 18.12.31R.
613 FCA Conduct of Business Sourcebook—October 2020 (UK), 16.2 and 16.4; FCA, *FCA's Regulatory Approach to Crowdfunding (and Similar Activities)*, para 3.76.
614 FCA Conduct of Business Sourcebook—October 2020 (UK), 18.12.21R–18.12.23R.
615 Banking Regulatory Commission Guide to the Disclosure of Information on Business Activities of Peer-to-Peer Lending Information Intermediaries 2016 (China), art. 10.
616 EBA, "Opinion of the European Banking Authority," para A1 and 28.
617 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20), para 5.45–5.47.
618 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20), para 5.48.
619 See, for example, Faridi, "P2P Fintech Lending Sector in Indonesia."
620 IOSCO, *IOSCO Research Report,* 20.
621 EBA, "Opinion of the European Banking Authority," para 62.
622 EBA, "Opinion of the European Banking Authority," para 60.
623 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20), para 1.34.
624 FCA Conduct of Business Sourcebook—October 2020 (UK), 4.7.
625 FCA Conduct of Business Sourcebook—October 2020 (UK), 10.
626 FCA Conduct of Business Sourcebook—October 2020 (UK), 10.2.9G.
627 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20), para 1.34 and 4.61–4.63.
628 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP19/14), para 2.23–2.27.
629 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP19/14), para 2.28.
630 Huang, "Online P2P Lending," 74.
631 Interim Measures for the Administration of the Business Activities of Online Lending Intermediary Institutions 2016 (China), art. 26.
632 RBI NBFC—Peer to Peer Lending Platform Directions 2017 (India), para 6(2).
633 RBI NBFC—Peer to Peer Lending Platform Directions 2017 (India), para 7.
634 National Monetary Council Resolution Number 4,656 of April 26, 2018 (Brazil), art. 16.
635 National Monetary Council Resolution Number 4,656 of April 26, 2018 (Brazil), art. 20.
636 Lenz, "Peer-to-Peer Lending," 699.
637 See also Havrylchyk, *Regulatory Framework*, 14.
638 See Lenz, "Peer-to-Peer Lending," 699; Ehrentraud et al., *Policy Responses to Fintech*, 56.
639 Banking and Securities Commission—General Provisions Applicable to Financial Technology Institutions, 10 September 2018, as amended 25 March 2019 (Mexico), art. 49.
640 Bae, "S. Korea to Place Investment Cap."
641 Interim Measures for the Administration of the Business Activities of Online Lending Intermediary Institutions 2016 (China), art. 17.
642 Huang, "Online P2P Lending," 74, 87–89.
643 RBI NBFC—Peer to Peer Lending Platform Directions 2017 (India), para 7.
644 Regulation of the Financial Services Authority Number 77/POJK.01/2016 Concerning Information Technology-Based Loan Services (Indonesia), art. 6.
645 See, for example, Havrylchyk, *Regulatory Framework*, 25.
646 Havrylchyk, *Regulatory Framework*, 25.
647 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20), para 4.66–4.71.
648 EBA, "Opinion of the European Banking Authority," para 66.
649 Lo, "If It Ain't Broke," 108.
650 EC, *Crowdfunding in the EU Capital Markets Union,* 16.
651 Duoguang, "Growing with Pain," 52–55.
652 Lo, "If It Ain't Broke," 95.
653 See National Consumer Credit Protection Act 2009 (Cth) (Australia), Part 3-1, Division 1 and Part 3-2, Division 2.

654 See National Consumer Credit Protection Act 2009 (Cth) (Australia), Schedule 1 (National Credit Code) Part 2.

655 RBI NBFC—Peer to Peer Lending Platform Directions 2017 (India), para 9(1)(b)(ii).

656 Regulation of the Financial Services Authority Number 77/POJK.01/2016 Concerning Information Technology-Based Loan Services (Indonesia), art. 20.

657 Banking and Securities Commission—General Provisions of CONDUSEF on Transparency and Sound Practices Applicable to Financial Technology Institutions, 9 July 2019 (Mexico), art. 7 and Appendix 2.

658 Banking Regulatory Commission Guide to the Disclosure of Information on Business Activities of Peer-to-Peer Lending Information Intermediaries 2016 (China); Interim Measures for the Administration of the Business Activities of Online Lending Intermediary Institutions 2016 (China).

INVESTMENT-BASED CROWDFUNDING

6

INVESTMENT-BASED CROWDFUNDING

6.1 INTRODUCTION

a) What is investment-based crowdfunding?

Investment-based crowdfunding (equity and debt) is an alternative finance solution that can address financing gaps not addressed by regulated capital markets and venture capital/private equity funds. It is typically offered through a fintech platform business model that connects investors with small businesses looking to raise capital or borrow by issuing securities to the "crowd." The basic premise behind crowdfunding is to enable small businesses to reach out to a large number of potential investors and offer investments in their companies.

Crowdfunding opened up a new source of equity capital for small businesses in addition to their usual investors such as family and friends, angel and venture capital/private equity investors. Small businesses seeking to raise equity through crowdfunding are usually early-stage start-ups with no or limited access to other forms of equity funding due to their small size and immaturity. Investment-based crowdfunding also offers an opportunity to raise funds by offering debt securities to the crowd as an alternative to borrowing from an incumbent credit provider or through a P2PL platform. According to the Cambridge Center for Alternative Finance's recent report, the volume of equity-based crowdfunding and debt-based crowdfunding in 2018 was $1.515 billion and $852 million, respectively. The United States, the United Kingdom, and Europe were the largest markets.[659]

While crowdfunding has grown in major markets, the volume of capital raised through crowdfunding is still small compared to its potential. The diversification of potential investors also remains limited. Its development in a country appears to depend on a combination of factors, including favorable market circumstances, a facilitative regulatory framework, and a positive and internet-friendly business culture. The existence of an investing culture among retail investors, together with a steady stream of investment opportunities (start-ups supported by accelerators and incubators coming to market), is also crucial. Markets with low rates of returns on traditional investments show higher promise for the development of crowdfunding, as it can represent an alternative and potentially more lucrative investment opportunity. However, this can also give rise to risk—discussed in this chapter—for the consumers who make up the crowd; they may be choosing between crowdfunding opportunities and more familiar or lower-risk investments.

Investment-based crowdfunding typically comprises the following elements:

- The core product/service offered is an offer of securities.
- This activity takes place through internet-based platforms that typically are not standard regulated trading facilities for providers of investment services.

b) Framing the risks

When considering consumer/investor protection risks related to crowdfunding activities, and the potential approaches to address these, it is necessary to focus on two distinct activities. The first is issuing and offering (promoting) securities to retail investors (the crowd). The second is providing trading-facility services (platform operations) for crowdfunded securities and potential risks arising from such activities.

Crowdfunding activity is typically exempt from the application of traditional capital markets rules, but certain limits and thresholds are placed on the activities of issuers, platform operators, and investors as a counterbalance to such exemptions. In the absence of modifications to traditional capital markets regimes, or a bespoke regime, to offer an investment service a crowdfunding platform would usually have to satisfy regulatory requirements whose applicability depends on the type of services offered (for example, placing of securities, operating secondary markets, providing investment advice, holding client assets and managing collective investment schemes). Satisfying relevant standards, such as with regard to capital, management, information technology, and so forth, can be onerous and may affect development of investment-based crowdfunding platforms.

If standard capital markets rules applied, small business issuers would also typically be required to follow a specific regime for offering securities to the public (for example, publishing a prospectus, acquiring necessary authorizations, meeting reporting and corporate-governance requirements, and so on). In such cases, relying on "traditional" exemptions—for example, no need to issue a prospectus if an offer is made only to accredited (sophisticated) investors—or offering securities up to some very small threshold could nevertheless be so restrictive that it would hamper the development of crowdfunding. This is primarily due to the compliance costs faced by small business issuers.

Growing realization of the potential for investment-based crowdfunding to allow small businesses increased access to finance has meant that regulators around the world have been seeking to adjust their regimes to facilitate crowdfunding without compromising investor protections. The SEC in the United States, when adopting regulations on crowdfunding, emphasized that the "crowdfunding provisions of the JOBS Act[660] were intended to help provide start-ups and small businesses with capital by making relatively low dollar offerings of securities, featuring relatively low dollar investments by the 'crowd,' less costly."[661] ASIC similarly indicated that amendments introduced by the 2017 Corporations Amendment Act were intended to provide a legislative framework to facilitate flexible and low-cost access to capital for small- to medium-sized unlisted public and proprietary (private) companies by reducing the regulatory requirements for making public offers of shares, while ensuring adequate protections for retail investors.[662] When the European Commission decided to introduce a special regulation for European crowdfunding service providers, it observed similarly that existing capital markets rules in the European Union might be disproportionate for small activities and not fit for purpose.[663]

Similar sentiment has been leading regulators in developed and emerging economies to create customized regulatory treatments for investment-based crowdfunding activities. This has typically been achieved either by introducing a specific crowdfunding exemption in the existing capital markets regulatory framework (the US or Australian approach referred to above) or by introducing bespoke stand-alone crowdfunding regulations (the approach in the European Union). A range of countries have introduced or are in the process of introducing crowdfunding-specific rules.[664] The Brazilian Securities and Exchange Commission enacted Instruction 588[665] in 2017, regulating the activity of crowdfunding in Brazil. Other examples include Mexico's Financial Technology Institutions Law and accompanying regulations, the Malaysian Guidelines on Recognized Markets[666] (on equity crowdfunding), and the Dubai Financial Services Authority's (DFSA) Rulebook, Conduct of Business Module,[667] Chapter 11. Although investment-based crowdfunding is only in the early stages of development in Africa, Nigeria, for example, is currently developing crowdfunding regulations.[668]

In developing appropriate enabling rules for crowdfunding, regulators also continue to face the need to ensure appropriate protection for consumers/retail investors. Relevant risks can be heightened by two important aspects of crowdfunding. First, investment-based crowdfunding gives entities that were previously unlikely to offer investments to the public, given standard capital markets requirements, the ability to do so. Second, they can make such offers to a crowd of investors that may not have made these kinds of investments previously. In a crowdfunding context, factors that can increase risks for consumers acting as investors—including the risk of losing their entire investment—can be grouped into the following four categories:

- Investor inexperience and higher-risk nature of investee companies.
- The nature of securities being issued—illiquid and hybrid.
- Lack of reliable information and misleading marketing practices.
- Platform business-conduct issues.

c) Summary of risks and regulatory approaches discussed in this chapter

Table 5 summarizes the new manifestations of consumer risks and corresponding regulatory approaches discussed in this chapter.

TABLE 5: Consumer Risks and Regulatory Approaches: Investment-Based Crowdfunding

RISKS TO CONSUMERS	REGULATORY APPROACHES	SEE PAGE
Investor inexperience and higher-risk nature of investee companies • Small business and start-up investee companies may constitute a riskier investment for retail investors • Investors are often unlikely to possess sufficient knowledge or experience, or lack access to financial advice, to assess offers • Investees may have majority shareholder and management arrangements that present risks for minority shareholders such as external crowdfunding investors	• Require risk warnings and disclosures about key aspects of crowdfunding • Impose issuer caps—limitations on the size of an issue • Impose investor caps—limitations on individual investments/exposures • Require investor-suitability assessments to be undertaken by platform operators • Establish cooling-off periods for investors	108
Risks relating to the nature of securities offered on crowdfunding platforms • Securities rarely traded on any kind of organized market and may have limitations on transferability—investors may not understand or are unable to deal with risk of being unable to exit their investment • Creation of complex hybrid securities by incorporating rights and restrictions for security holders to match issuer's needs	• Prescribe disclosure requirements focused on emphasizing the illiquid nature of issued securities • Restrict the types of securities that can be issued • Impose targeted product intervention • Require targeted warnings • Introduce rules facilitating information exchanges and secondary trading	112
Consumers are not provided with adequate information • Crowdfunding issuers often tend to be small businesses or in their start-up phase with a limited track record, limiting the availability of information • High separation between ownership by crowdfunding investors and parties that control issuers—potential lack of information provided to crowdfunding investors • Retail investors in crowdfunding securities are also at risk of misleading marketing practices, potentially exacerbated as a result of issuers being new to making public offers	• Introduce investment-related disclosure requirements • Introduce regulation of bulletin boards and crowdfunding trading facilities (including secondary market) to assist information accuracy • Apply fair marketing rules to investment-based crowdfunding activities	115
Platform operator misconduct or failure • Platform operators and related parties may engage in misconduct under a range of circumstances that affect investors, from outright fraud to incompetent administration to undertaking unfair conflicted behavior • Failure of a platform can leave investors without services essential to the continued integrity of their investment	• Introduce authorization and vetting requirements • Require business/service-continuity arrangements • Require segregation of client funds • Apply management requirements of the kinds summarized above in the context of P2PL	119
Issuer fraud: Consumers investing on crowdfunding platforms may suffer losses due to issuer fraud, such as sham offers or concealing or providing misleading information	• Require platform operators to undertake due diligence	122

6.2 INVESTOR INEXPERIENCE AND HIGHER-RISK NATURE OF INVESTEE COMPANIES

a) Risks to consumers

Crowdfunding facilitates opportunities to invest in smaller entities that may be at early stages of development. In some jurisdictions, the ability to use crowdfunding is even limited by law to small companies and start-ups. For example, in Australia, to be eligible an issuer has to be an unlisted company with consolidated gross assets and annual revenue not exceeding A$25 million.[669]

Such entities, however, may constitute an unsuitable, excessively risky investment for some consumers. Little reliable information may be available about their business operations and financial status, even less if they are small or in their start-up phase. Ordinary consumers may also be unlikely to have sufficient knowledge, experience, or resources to conduct a satisfactory level of due diligence on the issuer to make an informed decision when investing, or to have access to financial advice to be able to do so.

Crowdfunding issuers themselves also usually do not benefit from the professional guidance and know-how offered by venture capital/private equity investors.

This can make them even riskier investments than start-ups that do receive such support.

Crowdfunding issuers can frequently be closely held entities either within a family or a close group of entrepreneurs. This can make them less accepting of minority shareholders' rights. The risk that minority shareholders' interests might be underestimated, overlooked, or diluted can be exacerbated by separation between ownership and control over the company. Compared to concentrated holdings held by founders, for example, highly dispersed crowdfunded holdings can result in high separation between crowd investors and management decisions that affect their holdings. Large numbers of small and inexperienced investors, without collective influence or effective oversight, increase the risk of agency risks, moral hazard and even fraud and misappropriation of investors' funds.[670]

b) Regulatory approaches

Regulatory investor protection measures to address risks for consumers due to investor inexperience and the potentially riskier nature of investees in a crowdfunding context include the following:

- Requiring risk warnings and disclosures about key aspects of crowdfunding.
- Imposing issuer caps—limitations on the size of an issue.
- Imposing investor caps—limitations on individual investments/exposures.
- Requiring investor appropriateness or suitability assessments to be undertaken by platform operators.
- Establishing cooling-off periods for investors.

Risk warnings and information about crowdfunding

To assist prospective investors to have a clear understanding of the nature, risks, and costs of crowdfunding services, regulators typically require crowdfunding platform operators to provide their clients with a range of information.

Regulators usually require platform operators to warn potential investors regarding the risky nature of crowdfunding. The purpose of these warnings is to alert potential investors to specific features of crowdfunding that contribute to risk, such as emphasizing high failure rates of start-ups and small businesses. Platform operators are frequently also required to provide the following:

- General information about a platform's business model.
- Prominent confirmation of the regulatory status of the platform.
- Transparency in relation to fees and other charges that a platform might charge investors.
- Explanations of safeguards implemented to protect client funds.
- Contact and complaints-channel details.
- Conflicts of interest policies, including the platform's remuneration policy.
- Educational materials for prospective investors.

In Dubai, the DFSA Rulebook specifies a detailed list of information to be available on platforms' websites for prospective investors.[671] Investors must receive warnings about the main risks of using a crowdfunding platform, a description of how the platform functions, what happens if the issuer defaults, general information on default and failure rates, how the platform operator is remunerated, information about safeguarding client funds, and details about fees and charges. Similarly, crowdfunding investors in the United Kingdom must be provided general information about their platform, a confirmation that the company has been authorized, contact details, the platform's conflicts of interest policy, and its policy on safeguarding client funds.[672] Platform operators also have a general obligation to warn clients about the risks associated with investing in financial instruments.[673] In the United States, platform operators (regulated as "funding portals")[674] must cause prospective investors to demonstrate that they understand the risks of crowdfunded investing.

New EU regulation on crowdfunding requires that a range of information, including marketing communications from platforms operators to clients or potential clients, is fair, clear, and not misleading and is available to all clients and potential clients in a non-discriminatory manner on a clearly identified section of the website of the crowdfunding platform.[675] This includes information about the platform operator, the costs and charges related to crowdfunding services or investments, the crowdfunding conditions, including crowdfunding project-selection criteria, and the nature of and risks associated with their crowdfunding services.

Issuer caps: Limits on size of an issue of securities

By limiting the maximum size of an issue—in practical terms, usually the maximum amount of money that can be raised through a single crowdfunding issue or over a certain time period without having to comply with standard capital markets requirements—regulators can effectively seek to lower the potential number of retail investors exposed to loss from a particular company/issue of securities.

A range of jurisdictions have implemented such caps. The new EU regulation on crowdfunding highlights the perceived importance of such caps. It explains that, given the risks associated with crowdfunding investments and in the interest of the effective protection of investors, it was considered appropriate to impose a limit of €5 million in total consideration for crowdfunding offers made by a particular project owner.[676] In the United States, the crowdfunding regulations permit an issuer to raise a maximum aggregate amount of $1.07 million over a 12-month period. This limit is significantly lower than the amount of $5 million that usually triggers the need to register securities with the SEC.[677] In Dubai, an issuer can offer securities through a crowdfunding platform without the need to issue a prospectus if the offer is made to and directed at investors who are already clients of the platform operator and the total size of offered securities is not more than $5 million calculated over a period of 12 months.[678] Similarly, in Australia, eligible companies are able to offer ordinary shares to raise up to A$5 million in any 12-month period.[679] In Brazil the threshold is set at R$5 million,[680] and in Japan the threshold is ¥100 million.[681]

Malaysia takes a somewhat different approach. Instead of limiting a particular issue, an issuer is limited in how much it can raise from equity crowdfunding over its lifetime. An issuer may raise, collectively, a maximum amount of RM 10 million in its lifetime, excluding the issuer's own capital contribution or any funding obtained through a private placement exercise.[682]

Deciding on appropriate amounts and other bases for such caps can be difficult. If limits are set too low, they can act as an unjustified barrier to the development of crowdfunding in a market. Some regulators have thus been considering adjustments to existing caps. The Brazilian Securities and Exchange Commission issued a consultation document in March 2020 proposing an increase of the existing threshold from R$5 million to R$10 million.[683] Similarly, in March 2020 the SEC proposed increasing the issuer cap in the United States from $1.07 million to $5 million (while at the same time increasing the trigger for the need to register securities with the SEC to $10 million).[684] This was proposed after public consultations revealed that, while few offerings were reaching the existing limit, many issuers were choosing not to utilize the crowdfunding exemption because the limit was too low.[685] Similarly, after conducting public consultations the European Commission raised the originally proposed cap of €1 million to €5 million.[686] However, at the same time the caps should not be set too high to allow for effective regulatory arbitrage by issuers.

Investor caps: Limits on how much an investor can invest

In order to limit exposure of inexperienced investors to risky crowdfunding investments, some regulators are introducing limits on how much they can invest. Amounts and approaches to applying such limits vary. Some regulators have decided to forgo investment caps altogether and to focus instead on requiring platforms to assess the appropriateness or suitability of investments for retail investors.

There are generally two main approaches to setting investment limits: imposing a fixed monetary amount or requiring the cap to be calculated by reference to a prospective investor's circumstances, such as their income or assets. These limits may be further qualified as being absolute or relating only to an investment in a single company and may be calculated over a period of time (for example, 12 months). Examples include the following:

- A limit on the amount an investor can invest through crowdfunding over a period of time expressed as a percentage of annual income/net assets/investable assets.
- A fixed amount an investor can invest through crowdfunding in a year, with an additional limit on exposure per an individual company.
- A cap set as an absolute amount for all investments made through a single platform in a year with no caps per issuer.
- A cap set as a maximum amount for investment in a single company in a year.

In the United States, a limit is set in relation to the lesser of either annual income or net worth. Individuals with an annual income or net worth less than $107,000 can invest up to the greater of either $2,200 or 5 percent of the lesser of annual income or net worth during any 12-month period. If both annual income and net worth are equal to or more than $107,000, then, during any 12-month period, an individual can invest up to 10 percent of annual income or net worth, whichever is lesser, but not to exceed $107,000. The SEC has published a proposal to increase this cap by using instead the higher of either annual income or net worth to allow more flexibility to investors and to align the approach with another exemption. The amendments would also remove investor caps for accredited investors altogether.[687]

A similar approach is found in the United Kingdom. The UK rules on direct financial promotions[688] allow platforms to communicate financial promotions directly only to retail investors that confirm that they will not invest

more than 10 percent of their net investable assets in investments sold via investment-based crowdfunding platforms unless receiving regulated financial advice.[689] The FCA explained that the rules were introduced to ensure that clients are assessed as having the knowledge or experience to understand the risks involved before they can invest.[690]

On the other hand, countries such as Malaysia have set cap based in absolute amounts. The investment limit for retail investors has been set to a maximum of RM 5,000 per issuer, and the total amount to be invested is limited to RM 50,000 over 12 months.[691] In Dubai, an investment-based crowdfunding operator must maintain effective systems and controls to ensure that a retail client does not invest more than $50,000 in total in any calendar year using its service.[692] In Australia, the cap is set at A$10,000 per annum per company, but without maximum investable amounts per year for an investor. In Japan, the cap is ¥500,000.[693] In Brazil, the limit is set at R$10,000 on all platforms. If a platform can satisfy itself that an investor has an annual income exceeding R$100,000, the platform can accept the increase of this amount up to the limit of 10 percent of the investor's annual income.[694]

The effectiveness of investment limits as an appropriate risk mitigant is not universally accepted. Arguments against such investment limits include that net worth of an individual may not be an effective indicator of their acumen as an investor, that arbitrary limits may not result in commensurate protection for all retail investors, and that some of these limits are hard to control and enforce.

Some regulators have recognized the difficulty of policing investment limits and tried to balance investor protection with cost impacts on platforms required to investigate clients' income and existing exposures. This made some regulators (for example, in the United Kingdom, the United States, and Dubai) settle on allowing platforms to rely on investors' representations regarding income or assets unless the platform operator has a reason to question the reliability of such representations. On the other hand, EU regulation requires platform operators to ensure, if an unsophisticated investor invests an amount that exceeds the higher of either €1 000 or 5 percent of that investor's net worth, that the investor receives a risk warning, provides explicit consent, and proves that they understand the investment risk.[695] There are no such limits on investments made through *conseillers en investissement participatif* (crowdfunding advisors)[696] in France[697] or through crowdfunding platforms in Italy (established under the regulation on the collection of capital via online portals).[698]

Investor-appropriateness assessments by platform operators

An FCP measure implemented in a range of consumer contexts that can assist to target individual consumer inexperience in a crowdfunding context is an obligation on platform operators to conduct investor-assessment testing before allowing retail investors to invest using their services. This typically involves having a process in place to assess if crowdfunding investments, or a particular crowdfunding investment, is appropriate for a particular consumer's circumstances. Common techniques employed include running an entry knowledge test or simulations to gauge ability to bear losses.

Regulators that impose entry knowledge tests typically require platform operators to conduct remote equivalents of interviews with investors. These would be based on a series of questions posed through the platform's website. Collecting this information helps to establish whether the client understands the risks involved and whether the selected project is appropriate given their circumstances. When conducting such assessments, platform operators typically take into account matter such as the following:

- The type of services, transactions, and investments with which the prospective investor is familiar.
- The nature, volume, and frequency of the investor's investments and the period over which they have been carried out.
- The investor's level of education and profession or former profession (for example, if the client has experience in financial services).

Circumstances vary under which such assessments are applied. In France, among other prerequisites, investors may invest only after the completion of the assessment.[699] In the United Kingdom, when a retail client is not receiving investment advice, a platform operator must comply with rules on appropriateness. These include checking that the client has sufficient knowledge and experience to understand the risks of investing.[700] In Japan, platform operators[701] are required to suggest suitable financial instruments in light of clients' financial knowledge, wealth, and risk tolerance.

Some jurisdictions have mandated both investor tests and loss simulation for prospective investors. New EU regulation requires not only an entry knowledge test for prospective investors[702] but also that operators require prospective investors to simulate their ability to bear loss.[703] This would be calculated as 10 percent of their net worth. Interestingly, this threshold is similar to

the one used in the United States and United Kingdom when establishing investment limits for retail investors. Italian regulation requires platform operators to ensure that nonprofessional investors may access sections of the platform where they can invest only if they have read the investor-education information provided, have provided information about their knowledge and experience to understand the essential features and risks involved with investing, and have declared that they can financially sustain the possible loss of the entire investment they intend to make.[704]

Some regulators require platform operators to warn investors if the result of the testing shows that particular investments might not be appropriate for them. However, they are not necessarily prevented from going ahead with the investment.

Some regulators have not mandated testing. For example, in the United States, a prohibition on funding portals[705] providing investment advice and recommendations to investors has effectively barred them from introducing such testing.[706] However, funding portals are required to offer educational materials to help investors understand this type of investing, ensure that investors review such materials, and ask investors to confirm that they understand that they can lose all of their investment and that they can bear such a loss. In Dubai, the DFSA Rulebook also does not mandate running tests, but the lack of assessment needs to be disclosed clearly to investors if they are using an auto-investment system provided by the platform.[707]

Cooling-off periods

Cooling-off periods are intended as an additional layer of protection for inexperienced investors that proceed with an investment that may be unsuitable. Cooling-off periods give investors the right to withdraw from an investment within a specified time window without detriment. While many regulators seem to agree on the value of a cooling-off period, there seems to be no common approach on the time frame within which such a right should be allowed to be exercised. In Italy, the cooling-off period starts on the day an investor subscribes to the offer and lasts seven days.[708] Also, in case of a material change (for example, if any new fact arises that could influence the decision on the investment), the investor has a further seven days to withdraw starting from when notified of the change. In Australia, the cooling-off period lasts up to five days after subscribing to the offer (making an application),[709] while in Malaysia, it is six days.[710] In addition, in both countries, if there is any material adverse change relating to the issuer, investors must be notified and given the option to withdraw within 14 days of the notification.

The timing of cooling-off periods relative to closure of an issue, as well as their length, needs to be carefully balanced with the potential harm for issuers. Crowdfunding campaigns are usually created with a specific investment target, and subscribing investors are bound only if the target is reached. Giving investors the ability to withdraw late in the offer process can cause the aggregate amount of investment commitments to fall under such a target and effectively cancel the whole issue. Different regulators have taken different approach in this regard. In the United States, investors are allowed to withdraw up to 48 hours prior to the deadline identified in the issuer's offering materials.[711] Once the offering period is within 48 hours of ending, they are not able to cancel for any reason, even if they made their commitment during this period. However, if the company makes a material change to the offering terms or other information is disclosed, investors are given five business days to reconfirm their investment commitment. According to new EU regulation, a platform operator must provide a four days' cooling-off period (a precontractual reflection period), during which the prospective unsophisticated investor may, at any time, revoke the offer to invest without giving a reason and without incurring a penalty. The four-day period starts the day the offer is made.[712] On the other hand, in Dubai, retail investors may withdraw during a 48-hour cooling-off period that starts at the end of the commitment period.[713] This somewhat unusual approach allows withdrawals after the offer closes.

6.3 RISKS RELATED TO THE NATURE OF SECURITIES OFFERED ON PLATFORMS

a) Risks to consumers

Consumers investing in crowdfunding face a potentially unexpected, or misunderstood, greater risk of being unable to exit their investment—that is, to sell securities on the secondary market at any point in time. Unlike investing in securities listed on a regulated market, where consumers may usually expect to be able to exit their investment by reselling their securities on an organized secondary market, crowdfunded securities are rarely traded on any kind of organized market. Even where organized secondary trading is in place, market depth, and thus ease of trading, is often lacking. This effectively means that investors need to understand and be willing to accept the risk of being locked into their positions indefinitely (in case of equity) or until the full repayment of the debt (in case of debt).

Consumers may also lack experience and ability to understand complexities associated with the nature of securities typically offered on crowdfunding platforms. Consumers may be offered hybrid securities incorporating rights and restrictions intended to cater to the issuer's needs. These may include hybrid securities that mix properties of debt and equity, or securities that restrict voting rights. Sometimes crowdfunded securities are also issued with limitations on their transferability. This can be a contractual limitation or a legal requirement. For example, in the United States or Australia, shares may be traded only after 12 months from the issue (with some exceptions—for example, sale to accredited investors in the United States or sale with a prospectus in Australia). Similarly, in Malaysia, this limit is set at six months.

The more complex and greater the mix of such issuer rights and investor restrictions, the more difficult it may be for retail investors to understand the risks involved with investing in those securities.

b) Regulatory approaches

Regulatory investor protection measures to address such risks include the following:

- Prescribing disclosure requirements focused on emphasizing the illiquid nature of issued securities.
- Restricting the types of securities that can be issued.
- Targeted product interventions.
- Targeted warnings.

As discussed below, regulators are also introducing enabling measures that, while not strictly FCP measures, facilitate information exchange and secondary trading.

Disclosure of illiquidity risks

To mitigate the risk that retail investors lack awareness of the illiquidity of crowdfunding investments, regulators typically require platform operators to disclose this risk to investors. This includes clearly warning potential investors of the possibility that they will be unable to exit their investment at any given point of time. In a 2015 review of the UK regulatory regime for crowdfunding,[714] the FCA found that comparisons were sometimes being made between crowdfunding investments and retail bonds (such as corporate bonds listed on the stock market) without clarifying to crowdfunding investors that their money could effectively be locked in until maturity. In a more recent consultation, the FCA reiterated the importance of investors understanding there may be limited liquidity.[715] In Italy, a platform operator must disclose in a brief and easily comprehensible form the risk that it may be impossible to cash in an investment immediately.[716] The key investment information sheet contemplated under the new EU crowdfunding regulation will have to state clearly that investors may not be able to sell their investment instruments when they wish.[717] Similarly, in Dubai, an operator must disclose prominently on its website that the investor may not be able to sell their investment when they wish.[718] The Japan Securities Dealers Association's code of conduct for equity crowdfunding obliges its members to make sure that clients understand that the liquidity of shares will be quite low once the primary market has closed.[719]

Some regulators have also changed the terminology used in crowdfunding regulation to convey a clear message about the illiquid nature of relevant securities. In order to emphasize the illiquidity of securities on crowdfunding platforms, the FCA decided to change the terminology previously used, replacing the phrase "unlisted share and unlisted debt security" with a newly defined term: "non-readily realizable security."[720]

Regulators also publish warnings on their own websites. The SEC warns investors that they need to be ready to hold their investment for an indefinite period of time, because, unlike investing in companies listed on a stock exchange, investors may have to locate an interested buyer when seeking to resell their crowdfunded investments.[721] The warning is especially apt since crowdfunding regulations ban the resale of crowdfunded securities during the first year.[722] The SEC believes that restricting the transfer of securities for one year allows investors time to observe the performance of the business and, potentially, to obtain more information about the potential success or failure of the business before trading occurs.

Restricting the type of securities that can be issued

Some regulators are responding to the risk of retail investors not being capable to deal with the more complex nature of some securities by limiting the types of securities that can be offered through crowdfunding platforms. In Australia, eligible companies can offer only fully paid ordinary shares for (equity) crowdfunding. Offers of other types of securities (for example, partly paid shares, preference shares, options, or debentures) are not currently permitted. However, the legislation allows ASIC to extend this to a broader range of securities in the future if it sees fit to do so.[723] Similar restrictions are found under new EU regulation, where crowdfunding platforms are limited to offering investment only in transferable securities[724]—that is, "vanilla" bonds and shares.[725] The transferability of a security was considered an important safeguard for investors. Finan-

cial instruments other than transferable securities are prohibited from being offered; the European Commission explained when the regulation was proposed that they were viewed as entailing risks for investors that could not be properly managed within the proposed framework.[726] Similarly, in France, platforms may offer only plain vanilla bonds and ordinary shares.[727] In Dubai, all platforms are restricted from facilitating investments in products considered to be higher risk. These include derivatives or structured products, while shares, certificates, debentures, or sukuk are allowed.[728] In the United States, the SEC recently proposed amendments that would introduce limitations on the types of securities eligible under crowdfunding regulations. The proposal aims to limit crowdfunding to equity securities, debt securities, securities convertible or exchangeable for equity interests, and guarantees of any of these securities.[729]

Targeted product interventions

Regulators may address specific instances of risk from complex offerings through product intervention powers. In the United Kingdom, a pressing need for regulatory intervention was identified in the context of so called "mini-bonds." The FCA defines mini-bonds as debentures or preference shares that include one or more of the following features: They are typically issued by an authorized person who is not subject to FCA oversight and therefore generally not covered by the Financial Services Compensation Scheme; they are unlisted and commonly issued through a special purpose vehicle; the investment offers a high fixed rate of interest (8 percent or more) to investors if they commit to invest for a specific period of time (for example, three or five years) with limited or no opportunity to sell or transfer the investment before the end of that period; the issuer uses the capital raised to fund speculative and high-risk activities; and they often involve high costs or third-party payments that are made from the proceeds of the bond issuance. To address risks of harm for retail investors from the promotion of these highly speculative mini-bonds, the FCA introduced temporary product intervention measures starting from January 1, 2020.[730] The FCA explained the intervention reflected concerns with the widespread marketing of mini-bonds in spite of their high-risk nature and difficulty for retail investors to understand. The FCA was concerned that investors may be attracted to the lucrative returns offered, but that such promotions downplayed the key risks and implied that these products were "safer" than was the case in practice. The FCA's intervention comprised strengthening its financial promotions rules, on a temporary basis, to restrict the marketing of speculative illiquid securities for 12 months to ensure they can be promoted only to individual retail investors who have been pre-categorized as either sophisticated or high net worth, and where the product has been initially assessed as likely to be suitable for them. The FCA also mandated including a specific risk warning, as well as disclosing any costs or payments to third parties that are deducted from the money raised by an issuer, in any financial promotion for these products regardless of the type of investors.

Targeted warnings

Regulators may also seek to address specific instances of risky securities by mandating targeted warnings in addition to standard disclosures. The SEC in the United States identified so-called "SAFE" (simple agreements for future equity) securities as being of particular concern.[731] A SAFE security was a quasi-equity security that differed significantly from traditional equity securities. It was an option, or an agreement between an investor and the issuing company, in which the company generally promised to give the investor a future equity stake in the company if certain trigger events occurred. Historically, SAFEs were designed as a way for venture capital investors to invest in start-ups quickly without burdening the start-up with the more labored negotiations that an equity offering may entail. According to the SEC, it was often more important for the venture capital investor to get the investment opportunity, and possible future opportunities, with the start-up than it was to protect the relatively small investment represented by the SAFE. In addition, the various mechanisms of the SAFE, from the triggering events to the conversion terms, were designed to operate best in the context of a fast-growing start-up likely to need and attract additional capital from sophisticated venture capital investors. Since this may not be the case in a crowdfunding context, the SEC considered it important to warn investors specifically about these securities.[732] In March 2020, the SEC also proposed changes that would limit types of securities eligible to be offered under crowdfunding regulations, recognizing the need to simplify the type of securities offered to retail investors through crowdfunding platforms.[733]

Facilitating information exchanges and secondary trading

Regulators around the world seem to be introducing enabling regulatory frameworks to incentivize the development of crowdfunding secondary markets in part as a response to concerns regarding illiquidity. Strictly speaking, such frameworks go beyond FCP measures, but it would be important that they are administered, where introduced, in ways that do not introduce additional risks.

The European Commission noted an emerging trend in the European Union of organized secondary markets for securities or loans in crowdfunding projects, although such services were not being provided systematically.[734] In order to improve access to information about securities and support creation of secondary markets, platform operators started introducing online bulletin boards to encourage information exchanges between investors. Some platforms have gone even further to facilitate secondary trades by offering a form of trading service or partnering with licensed third-party trading facilities—for example, with licensed intermediaries under the Markets in Financial Instruments Directive (MiFID) in the European Union or broker dealers in the United States. Such practices are currently more prevalent in the United States and United Kingdom, but regulators are increasingly developing regulatory frameworks to incentivize such development (for example, in Dubai, Australia, Malaysia, and Brazil).

Recognizing the need to facilitate the development of transparent information exchanges and, indirectly, secondary markets, new EU crowdfunding regulation introduces the concept of a bulletin board that would allow investors to interact directly with each other to buy and sell securities that were originally crowdfunded on these platforms.[735] However, these bulletin boards will not be allowed to facilitate trading; this will still have to be done privately or using a MiFID-authorized intermediary. Under existing regulations in Italy,[736] for example, platform operators are allowed to offer, in a separate section of the platform, an electronic board for the publication of the information about crowdfunded securities. This is possible only for securities issued in the scope of a crowdfunding campaign carried out on their own platform, and the platforms are not to carry out activities aimed at facilitating the trade.

A range of regulators outside of the European Union have also taken action in this context, and some go even further by allowing platform operators to run secondary markets. US platform operators (either a funding portal or a broker-dealer) are required to provide communication channels that would allow information exchange between investors and the issuer, and that need to be publicly available for viewing (that is, by those who may not have opened accounts with the platform). If a platform operator is registered as a broker-dealer, then it can facilitate trade as well, but not if it is registered as a funding portal (a specific license created to facilitate development of crowdfunding). Similarly, in Australia, a platform operator is required to provide a communication facility for any offer on its platform to allow the issuer and potential investors to communicate with each other about the issuer's offer.[737] The facility must enable a person who accesses the offer document to post comments about the offer, see posts made by others, and ask the issuer and the platform operator questions about the offer. In order to provide a trading facility, an Australian platform operator must hold an Australian market license. Regulations in Dubai and Malaysia go a step further than those in the European Union, the United States, or Australia and allow platform operators to run secondary markets in addition to providing forums for information exchange. While secondary trading of securities offered through crowdfunding platforms is currently prohibited in Brazil, the Brazilian Securities and Exchange Commission proposed revising the current regulation in March 2020, introducing the possibility of a crowdfunding platform acting as a trading facility (an intermediary between investors).[738]

While allowing platform operators to introduce organized information exchanges and even to run trading facilities is definitely a step forward in developing liquidity, regulators also need to pay attention to the risks arising from potential market abuse. Platform operators should have appropriate mechanisms to prevent, detect, and respond to any potential market manipulation on their platforms. Eventually, for secondary markets to function properly, more comprehensive regulation proportional to the risks of trading unlisted securities is likely to be necessary. These issues are discussed further below in the context of regulation of bulletin boards and crowdfunding trading facilities.

6.4 CONSUMERS NOT PROVIDED WITH ADEQUATE INFORMATION

a) Risks to consumers

Crowdfunding issuers often tend to be small businesses in their start-up phase with limited track records, limiting the availability of information. Small businesses typically do not disclose information as frequently or as extensively as public companies and, unlike public companies, are generally not under obligation to have an independent audit of their financial statements. This also means consumers investing through crowdfunding will likely have significantly less information about the issuer's prospects than the issuer's management or owners, especially when compared to other types of public securities offerings.

When information about an issuer is difficult to obtain or the quality of the information is uncertain, investors are at risk of making poorly informed investment decisions. Unlike listed companies that are valued pub-

licly through market-driven prices, valuations of small private companies can be much more difficult and investors risk overpaying, particularly given the investment risks taken on. Loss risks connected with poor information are amplified for retail investors, who may not have the resources necessary to gather and analyze information about issuers before investing or to monitor issuers effectively after investing.

The fact that the majority of crowdfunding investors are likely to have smaller, non-controlling stakes in issuers may mean that issuers—including their controlling stakeholders—do not consider the need to be transparent. For example, they may use capital to fund riskier projects than originally disclosed without updating.

Retail investors in crowdfunding securities are also at risk of misleading marketing practices, potentially exacerbated as a result of issuers being new to making public offers. The resulting misconduct may include promotional activities that lack balance, where benefits are emphasized without equally highlighting potential risks; selectively choosing information to create unrealistically optimistic impression of the investment; or watering down important information by making comforting statements based on past records.

b) Regulatory approaches

Regulators seek to reduce information asymmetries and address information and marketing-related abuses through a variety of disclosure, information integrity, and marketing requirements. Regulatory measures aimed at addressing such risks associated with crowdfunding include the following:

- Investment-related disclosure requirements.
- Regulation of bulletin boards and crowdfunding trading facilities.
- Fair marketing rules.

(Requiring platform operators to conduct due diligence on issuers, discussed in the next section, is also an important measure for investors wanting to locate and verify information relating to issuers.)

Investment-related disclosure requirements

In order to decrease information asymmetry and assist investors to make sensible and informed decisions, regulators have prescribed a range of minimum disclosure standards. These standards require disclosure of general information about issuers as well as information about particular offers. Approaches differ, but issuers are typically required to disclose the following:

- Key characteristics of the issuer.
- A description of the issuer's ownership and capital structure.
- Financial information about the issuer with or without an independent audit requirement.
- The main risks facing the issuer's business.
- The purpose of the fundraising and the targeted offer total.
- Information about the issuer's business plan.
- A description of the securities being issued and the investor's rights linked to them.
- Arrangements in place for holding the shares and exercising investors' rights after investment (for example, any nominee arrangements).

Regulators impose requirements for issuers to provide information to investors, including by providing such information to the platform. In the United States, the issuer must disclose information about the company, its business plan, the offering, and its anticipated use of proceeds, among other things. It needs to specify the terms of the securities being offered and each other class of security of the issuer, including the number of securities being offered and/or outstanding, whether such securities have voting rights, any limitations on such voting rights, how the terms of the securities being offered may be modified, and a summary of the differences between such securities and each other class of security of the issuer, and how the rights of the securities being offered may be materially limited, diluted, or qualified by the rights of any other class of security of the issuer. Under crowdfunding regulations, issuers are also required to publish financial statements that at a minimum need to be certified by the company or reviewed by an independent public accountant and, for offerings of a certain size, also audited.[739] In Malaysia, an issuer needs to submit to the platform operator, to be appropriately passed on, general information about the company, information explaining the purpose of the fundraising and the targeted offering amount, as well as the business plan. The issuer also needs to publish financial information whose extent depends on the size of the funds raised in the previous 12 months.[740]

Requirements are also placed on platform operators to source and provide relevant information. In Italy, a platform operator must make available to investors, in a detailed manner and without omissions, all information about the offer provided by the issuer so that investors can understand the nature of the investment, the kind

of financial instrument offered, and the risks related to them. The platform operator must ensure that the information provided via the portal is updated, accessible for at least 12 months after the closure of the offer, and made available to interested parties upon request.[741] In the United Kingdom, the FCA requires platform operators to provide appropriate information to investors on the nature and risks of an investment.[742] The information disseminated to the client must give a fair and prominent indication when referencing the potential benefits of an investment.

Some regimes impose standardized format requirements to assist investor comprehension. In addition to prescribing the information to be disclosed, platform operators in the European Union are required under the new crowdfunding regulation to present this information in a standardized key investment information sheet.[743] This document has to take into account the specific features and risks associated with early-stage companies and focus on material information about the issuers, the investors' rights and fees, and the type of securities offered. As issuers are considered to be in the best position to provide that information, they will have to draw up the information sheet. However, as platform operators will be responsible for informing prospective investors, they will have to ensure that the sheet is complete. In order to keep down associated costs, the key investment information document will not have to be approved by a competent authority. In Australia, ASIC prepared a template of the offer document as a guide and is strongly encouraging issuers and platform operators to present and format the offer document in a way that enhances the readability and accessibility of the document for retail investors.[744] Public companies and proprietary companies in Australia that have completed a successful offer must comply with certain financial reporting obligations, including independent audit requirements.[745]

Regulation of bulletin boards and crowdfunding trading facilities

As briefly discussed earlier, a recent trend is for platforms to host information exchanges (bulletin boards) about crowdfunded securities and even secondary markets for such securities. Regulators have recognized the potential for abuses that may occur through such bulletin boards and trading platforms if these are not already regulated under existing capital markets rules (for example, MiFID-regulated intermediaries in the European Union or broker dealers in the United States). Therefore, in parallel to encouraging the development, regulators are developing standards aimed at reducing such information-related and market-abuse risks. Regulatory requirements differ depending on the service provided or function undertaken by a platform operator. Typical regulatory requirements for crowdfunding platform operators in this context include the following:

- Limiting the posting of comments on bulletin boards only to clients using the platform service.
- Ensuring that all clients using the bulletin board have equal access to information posted.
- Requiring a person posting a comment to disclose clearly if they are affiliated in any way with the issuer.
- Mandating that platform operators take reasonable steps to monitor and prevent posts that are potentially misleading or fraudulent.
- Ensuring that the secondary-market trading activities are conducted in a fair, orderly, and transparent manner and that all procedures in place enable safe, transparent, and legal trade in securities (if acting as an intermediary).

In a recent review of relevant crowdfunding practices, the FCA found that platforms were often allowing investors to comment on investment opportunities, but that market intelligence suggested negative comments on some platforms tended to be deleted, which could lead to relevant risks being overlooked by investors. The FCA therefore determined that platforms should have mechanisms to detect, prevent, and respond to any potential market manipulation. (The FCA also concluded that, eventually, for secondary markets to function properly, a more comprehensive regulation for the trading of unlisted securities should be developed.[746] For the time being, crowdfunding platform operators cannot provide trading services in the United Kingdom. If one wants to provide trading services, it would need to be licensed under the existing regime.)

In the United States, a platform operator (a funding portal or a broker-dealer) is actually required to provide communication channels on its platform[747] that will allow investors with an account with the platform operator and the representatives of the issuer to interact and exchange comments. The operator must require any person posting a comment to disclose clearly with each posting whether they are a founder or an employee of an issuer.

Regulators are imposing a range of specific obligations on operators offering bulletin boards or, more broadly, secondary trading, to safeguard the integrity of the information that investors may receive on such facilities and to make them aware of poten-

tial shortcomings. In Dubai, if an operator provides a means of communication (a "forum") for users to discuss funding proposals made using the service, the operator must refer investors to the forum as a place where they can discuss proposals, while clearly stating that the operator does not conduct due diligence on information on the forum. The operator also needs to restrict posting of comments on the forum only to persons who are clients using the service; to ensure that all clients using the forum have equal access to information posted on the forum; to require a person posting a comment on the forum to disclose clearly if they are affiliated in any way with the issuer; and to take reasonable steps to monitor and prevent posts on the forum that are potentially misleading or fraudulent.[748] In Malaysia, a platform operator can become an operator of the secondary market under a regime specifically developed for crowdfunding. In order to do that, it needs to have arrangements addressing how the secondary market will operate and to ensure that the secondary market trading activities on its platform are conducted in a fair, orderly, and transparent manner. It also has to ensure that access to its secondary market is fair, transparent, and objective, and that all users are treated fairly. This includes providing equal access to information; having policies and procedures for the trading, clearing, and settlement of securities on the platform; having sufficient financial, technological, and human resources to operate its secondary market; monitoring and ensuring compliance of its rules, including conducting ongoing market surveillance; and having in place mechanisms to help ensure the resiliency, reliability, and integrity of the system, including the security of critical systems.[749] The Brazilian regulator recently proposed allowing crowdfunding platforms to operate secondary market under certain specific conditions.[750] According to the Brazilian proposal, platform operators, in addition to adopting necessary measures to ensure trading integrity, will have to maintain a public history of trades, enabling investors to monitor prices and quantities traded.

Fair marketing rules

Advertising and marketing more generally play an important role in crowdfunding. Regulators are trying to ensure that issuers, platform operators, and other promoters give clear, accurate, and balanced messages when advertising crowdfunding offers. To achieve these aims, regulators place obligations, as relevant, on issuers, operators, and promoters to do the following:

- Restrict and regulate advertising outside of platforms.
- Indicate clearly that relevant communications are advertising.
- Include a statement directing investors to check the relevant offer document before subscribing to securities.
- Include general risk warnings to balance promotional messages.
- Ensure that advertisements do not mislead or deceive by doing the following:
  - Overstating or giving unbalanced emphasis to potential benefits.
  - Creating unrealistic expectations.
  - Omitting or giving less prominence to information about the risks facing the issuer's business or adverse information about issuer.
  - Presenting views about an offer as those of investors or unrelated parties.

Some regulators restrict advertising outside of platforms. In the United States, an issuer may not advertise the terms of an offering outside of their intermediary's platform except in a notice that directs investors to the intermediary's platform.[751] An issuer may also communicate with investors and potential investors about the terms of the offering through communication channels provided on the intermediary's platform. The issuer must identify itself, and persons acting on behalf of the issuer must identify their affiliation with the issuer, in all communications on the intermediary's platform. In Dubai, a platform operator must not advertise a specific offer that is available on its platform and has to take reasonable steps to ensure that issuers and sellers that use its platform do not advertise offers unless the advertisement is made on the platform and is accessible only to existing clients who use the platform. If an offer is advertised to potential investors who are not clients of the platform, this may constitute an offer of securities to the public, which would trigger an obligation to prepare a prospectus.[752] This does not prevent an operator from generally promoting its crowdfunding service to potential clients, provided it does not advertise a specific proposal.

According to new EU regulation on crowdfunding, platform operators have to ensure that all marketing communications to investors are clearly identifiable as such.[753] Marketing communications may indicate only where and in which language clients can obtain information about individual projects or offers.

In the United Kingdom, entities that communicate or approve crowdfunding offers must comply with financial promotion requirements, including ensuring that such promotions are fair, clear, and not misleading. The rule is applied in a way that is appropriate and proportionate taking into account the means of communication, the

information that the communication is intended to convey, and the nature of the client, where a higher standard is expected for retail clients.[754]

6.5 PLATFORM OPERATOR MISCONDUCT OR FAILURE

a) Risks to consumers

Platform misconduct

Platform operators and related parties may engage in misconduct under a range of circumstances that affect investors. These may range from outright fraud by platform operators, such as siphoning customer funds; or offering fraudulent investments through the platform, to undertaking unfair conflicted behavior that favors the operator's interests to the detriment of investors. Operators that lack experience or competence can exacerbate such risk, which can be more likely in a market involving many new entrants.

While the propensity to act fraudulently is directly linked to the integrity of the platform operators and their employees, some business models can increase the likelihood of conflict of interest and detrimental operator conduct toward investors. For example, conflict can arise between platform operators' obligations toward investors and potential financial benefits the operator derives from ensuring the success of crowdfunding offers. This conflict is heightened with models where an operator's remuneration depends on the success of an offer. This can then have a negative impact on an operator's responsibilities, such as to:

- Facilitate investors' ability to exercise their cooling-off rights and receive a refund, even though this may lead to the offer being unsuccessful (as it reduces the amounts raised), which can in turn have a negative impact on the operator's income.
- Manage a bulletin board with integrity, knowing that negative factual information or opinions may detract from the success of the offer and consequently harm operator's revenue.
- Perform due diligence on issuers to a required standard, which may result in the need to decline to publish certain offers and in turn harm operator's ability to generate revenue.
- Review disclosure documents to the required standard, with the same negative result for the platform operator.

A platform operator may also act as nominee for investors in relation to the securities in which they invest. In this capacity, they may exercise rights, such as voting rights, on behalf of the investor. If the operator or related parties have potentially conflicting interests (such as their own shareholdings) in the issuer, they may exercise such rights inconsistently with the investor's interests.

Platform failure

The failure of a platform can leave investors without services essential to the continued integrity of their investment. The significance of this risk depends on what kind of post-investment services a platform provides to an investor. These could include holding or receiving client money, undertaking payment services (for example, channeling payments from issuers to investors), acting as a nominee representative for retail investors in relation to the issuer, and providing a bulletin board or running a secondary market for crowdfunded securities. Losing access to these services can cause operational and financial detriment to investors. If investors' funds held by a failing platform are not well protected, they might also be lost in an operator's resulting insolvency.

Platforms may fail for a variety of reasons, including financial distress caused by mismanagement or internal or external fraud and technology failures caused by inadequate infrastructure or cyberattacks. Inadequate capitalization and resourcing may contribute to failures by causing inadequate systems and arrangements. Also, a platform in financial distress might be more susceptible to risky behavior, increasing the probability of financial demise and potential detriment to investors.

b) Regulatory approaches

Current and emerging regulatory frameworks for investment-based crowdfunding seek to address platform misconduct and failure risks through a combination of approaches, including some or all of the following:

- Authorization and vetting requirements.
- Requirements for business/service-continuity arrangements.
- Segregation of client funds.
- Imposing rules and policies to mitigate conflicts of interest.

Other requirements might include minimum capital and adequacy of financial resources, organizational competence, dispute resolution, and outsourcing standards.

Authorization and vetting requirements

Authorization and vetting requirements are intended to act as a mitigant to a variety of risks that are caused

or increased if incompetent or dishonest operators are allowed to operate in a market. Having authorization requirements in place enables regulators both to take action against unauthorized platform operators and to use enforcement of authorization conditions as a means of ensuring good behavior by authorized entities.

Different jurisdictions have taken different approaches to authorization requirements for crowdfunding platform operators. Some jurisdictions have brought operators within existing licensing regimes (some with adjustments), while others have bespoke licensing frameworks. Jurisdictions where authorization requirements for crowdfunding sit within an existing licensing and regulatory framework, with some crowdfunding-specific adaptations, include Australia, Dubai, and Nigeria. In Dubai, a crowdfunding platform operator needs to be licensed as an authorized firm and to have a specific endorsement on its license if providing crowdfunding services to retail investors.[755] Under rules proposed in Nigeria, only entities registered with the regulator as one of several preexisting categories (for example, Exchange, Dealer, Broker, Broker-Dealer, or Alternative Trading Facility) may be registered as a crowdfunding intermediary.[756] In Australia, a platform operator needs to acquire an Australian financial services license, which authorizes a person who carries on a financial services business to provide a crowdfunding service.[757] On the other hand, the European Union and United States have created a specific framework for crowdfunding platform operators. In the European Union, operators have to be licensed as crowdfunding service providers under a new regime introduced by EU regulation.[758] In the United States, operators must be licensed as funding portals under the Regulation Crowdfunding.[759]

Regulators should also make sure that they have the necessary regulatory mandate, powers, and resources to monitor and prevent any unauthorized cross-border promotion of crowdfunded securities. The environment of evolving regulatory approaches and the absence of internationally set standards open doors for regulatory arbitrage. Issuers in a jurisdiction with a weaker regulatory framework for crowdfunding may try to promote issues of securities across borders. In order to be able to uphold the standards of investor protection, including protection from fraud and other platform misconduct, regulators need to make sure they have the means to prevent active promotion of crowdfunding securities by locally unauthorized operators.

When it comes to vetting standards to establish the fitness of operators and their employees and management, a range of approaches are taken, but regulations generally focus on good reputation and adequate knowledge as the main principles to be followed. In the European Union, for example, the management of a platform must be of good reputation and have adequate knowledge and experience.[760] Similar requirements apply in Italy,[761] Dubai,[762] Nigeria,[763] and Malaysia.[764]

Business continuity arrangements obligations

In order to ensure the ongoing administration of investments in the event of platform failure, platforms could be required to put arrangements in place to allow continuation of post-investment services even in the event of business failure. Such business continuity plans are typically expected to take into account the nature, scale, and complexity of the crowdfunding services being provided and to establish measures and procedures that ensure, in the event of the failure of a platform operator, the continuity of critical services related to existing investments and the sound administration of agreements between the platform operator and its clients. Platform operators are usually required to do the following:

- Provide regulators with a business overview.
- Provide regulators with a specific analysis of the critical functions of the business.
- Determine the trigger events that might cause a wind-down of the business.
- Present an analysis of what functions are required and need to be undertaken for an orderly wind-down of the business.
- Create a plan for communicating with investors and other business partners during the wind-down period.

Platform operators can also be required to put in place third-party measures to support such contingency arrangements if risks eventuate—for example, by entering into an agreement with a third party to provide certain services. In Dubai, an operator must maintain a business-cessation plan that sets out appropriate contingency arrangements to ensure the orderly administration of investments in the event that it ceases to carry on its business, and the operator must review its business-cessation plan at least annually to take into account any changes to its business model or to the risks to which it is exposed.[765] According to the new EU regulation on crowdfunding, a platform seeking authorization must provide information to the regulator showing that the platform has business continuity arrangements in place.[766] In the United Kingdom, investment-based platforms are subject to existing business continuity rules applicable to investment firms generally.[767]

Segregation of clients' funds

The protection of investors' assets (securities and money) that are held at any point by a service provider is a key consideration of an investor protection framework. Investors' assets need to be protected from a platform operator's insolvency and not be a part of the platform operator's assets.

Regulators have been approaching this issue in two ways in a crowdfunding context. The first is to prohibit crowdfunding platforms from dealing with investors' funds and to require that operators have arrangements with other regulated institutions that are allowed to provide such services (for example, deposit-taking institutions or payment-services providers). The second approach is to allow crowdfunding platforms to deal with client funds by either requesting them to be authorized as payment-services providers or simply to apply similar funds-protection standards without necessarily requesting specific licenses. For example, in the United States, funding portals are prohibited from holding, possessing, or handling investor funds or securities.[768] They therefore would usually engage a third-party broker-dealer to deal in client payments on their behalf. In Italy, platforms are similarly required to work alongside a bank or registered investment company to support their operations. This includes the handling and retaining of investors' money (with funds flowing directly into the bank account of the issuer from the account of the investor, rather than through the account of the platform).[769] In Dubai, an additional permission is required to hold or control investors' money or securities.[770] Under new EU regulation, platform operators have to be licensed as a payment-service provider if they wish to hold client funds.[771]

Obligations to mitigate conflicts of interest

Regulators have prescribed a range of obligations for platform operators to mitigate against conduct inconsistent with the interests of investors. Typical requirements include the following:

- A duty to act honestly, fairly, and professionally in accordance with the best interests of investors.
- Requirements to have in place effective policies for the mitigation of conflicts of interest.
- Restrictions on investments hosted on platforms by operators and their staff.
- Requirements for operators to disclose any financial interest in issuers.
- Requirements for disclosures of the manner in which operators are compensated.
- Bans on solicitations by platforms.

While formulations of the obligations to act appropriately and in the interests of investors and, specifically, to mitigate conflicts of interest vary internationally, they tend to reflect common elements. In Italy, platform operators must operate with diligence, correctness, and transparency, preventing any conflicts of interest that may arise in the management of platforms from harming the interests of investors and ensuring equal treatment of recipients of offers who are in identical conditions. The manager has to prepare, implement, and maintain an effective policy on conflicts of interest, formulated in writing, that supports identification of circumstances that generate or could generate a conflict of interest detrimental to one or more investors and defines the procedures to be followed and measures to be taken to prevent or manage such conflicts.[772] New EU crowdfunding regulation requires operators to act honestly, fairly, and professionally in accordance with the best interests of investors.[773] In Dubai, platform operators must take reasonable steps to ensure that conflicts and potential conflicts of interest between themselves and their clients, and between one client and another, are identified and then prevented or managed in such a way that the interests of a client are not harmed, and to ensure that all its clients are treated fairly and not prejudiced by any such conflict of interest. Where a platform operator is aware of a conflict or potential conflict of interest, it must prevent or manage that conflict of interest. If it is unable to prevent or manage a conflict or potential conflict of interest, it must decline to act for that client.[774]

Many regulators take the view that prohibiting operators from investing in offers they host on their platforms is a good way of mitigating a key driver of potential conflicts of interest risk. For example, under new EU regulation, crowdfunding service providers are prevented from having any financial participation in the crowdfunding offers on their platforms. Such a prohibition also applies to their shareholders who hold 20 percent or more of share capital or voting rights, managers, employees, or any person directly or indirectly controlling crowdfunding platforms: they are not allowed to act as investors in relation to the crowdfunding services offered on that crowdfunding platform.[775] It is envisaged that platform operators should operate as neutral intermediaries between clients on their crowdfunding platform.[776] In Dubai, officers and employees of a platform operator (and their family members) are also restricted from investing/issuing via the platform or from having financial interest in any issuer or investor.[777] On the other hand, there is a line of thought that holds that allowing the platform operators to invest shows skin in the game and increases trust in crowdfunding. For example, in the United States, operators (but not their directors or

officers) may invest in issuers selling securities through their platform so long as they receive the financial interest as compensation for their services and it consists of the same class of securities with the same terms that the public is receiving.[778] This was allowed based on the view that platforms investments can raise the profile of crowdfunding campaigns and increase the appeal of crowdfunding in general. However, any director, officer, or partner of the operator, or any person occupying a similar status or performing a similar function, may not have a financial interest in an issuer that is offering or selling securities through the operator's platform, or receive a financial interest in an issuer as compensation for the services provided to or for the benefit of the issuer in connection with the offer or sale of such securities. In Malaysia, a platform operator is permitted to have shareholding in the issuers hosted on its platform, but that shareholding must not exceed 30 percent.[779]

Requirements to disclose potential sources of conflicts are frequently implemented as a regulatory approach, often in addition to other substantive measures. Jurisdictions such as the United States require operators to disclose clearly the manner in which they are compensated in connection with offers and sales of securities.[780] In Malaysia, a platform operator, including their directors and shareholders, must disclose to the public on their platform if they hold any shares in any issuers hosted on the platform. The operator also needs to disclose if they pay any promoters or receive payment in whatever form, including payment in the form of shares, in connection with an issuer hosted on their platform.[781]

Risk management requirements

Investment-based crowdfunding operators have been made subject to a range of risk management obligations of the kinds described in chapter 5 as applicable to P2PL platform operators. The expectations imposed by such requirements would also target the need for operators to address risks related to platform failure.

6.6 ISSUER FRAUD

a) Risks to consumers

Consumers investing on crowdfunding platforms may suffer losses due to issuer fraud in a range of scenarios. Issuers (which may be genuine or sham issuers) may attempt to defraud potential investors by showcasing fraudulent business plans, by concealing facts about their history or their management, or by using misleading promotion techniques. It can be difficult for an unsophisticated investor to detect a sham offering and, perhaps even more so, fraudulent aspects of an otherwise seemingly genuine offering. This is amplified by the fact that, unlike with traditional public offers, the regulator's role in reviewing the offer-related information is minimal or nonexistent.

b) Regulatory approaches

A common approach taken by regulators is placing the onus on platform operators to conduct due diligence on issuers and their offerings, although the minimum required level of due diligence varies significantly in different jurisdictions. This can range from platforms being requested simply to satisfy themselves that a fraud is highly unlikely in a particular case to expecting platform operators to examine the soundness of issuers' business plans.

In the United States, a funding portal needs to deny access to an issuer if it has a reasonable basis for believing that the issuer or the offering presents the potential for fraud or otherwise raises concerns about investor protection, or that the issuer or any of its officers, directors, or 20 percent beneficial owners were subject to a disqualification. The funding portal must also conduct a background and securities-enforcement check on each of these persons. However, there is no obligation for a funding portal to fact-check the business plan of an issuer.[782]

The FCA does not prescribe due diligence requirements for platform operators but requires that platforms disclose to investors the level of due diligence undertaken. However, platform operators are under a general duty to exercise skill, care, and diligence as well as to act in customers' best interests. The FCA recently expressed an opinion that platform operators' resulting due diligence obligations include assessing whether they are legitimate. At a minimum, all platform operators should conduct obvious checks—such as ensuring that the company exists and that the founders are who they say they are. In addition, the FCA stated that it would consider it unlikely that a platform operator could argue that it has met its obligations of exercising skill, care, and diligence if it had not undertaken enough due diligence to satisfy itself on the essential information on which any communication or promotion is based.[783] In Australia, platform operators have to check the identity and eligibility of the issuer, the fitness and properness of managers and employees, and the completeness and legibility of offer documents.[784] The European Union's new crowdfunding regulation requires platform operators to undertake a minimum level of due diligence in respect to project owners who propose their projects to

be funded through the crowdfunding platform. At a minimum, this includes checking that the project owner has no criminal record in respect to infringements of national rules in fields of commercial law, insolvency law, financial services law, anti-money-laundering law, fraud law, or professional liability obligations.[785]

In Dubai and Malaysia, platform operators are subject to even more stringent and, at times, prescriptive due diligence requirements. In Dubai, an operator must conduct due diligence on each issuer before allowing it to use its service. This due diligence, among other things, must include, at a minimum, taking reasonable steps to verify the issuer's identity, financial strength (which includes checking financial statements, financial history, and past performance), credentials or expertise it claims to have, valuation of its business, current borrowing or funding levels (if any), and source of any existing borrowing or funding. Platform operators are also required to check the business proposal; the issuer's commitment, including that of the management (for example, how much capital they have provided and any potential flight risk); and that its business is being carried on in accordance with applicable laws in the jurisdiction where it is based (that the owner has the necessary permits and that the activity is lawful).[786] The regulations in Malaysia are less detailed than in Dubai, but they place obligations on platform operators to take reasonable steps to verify the business proposition of the issuer as well as to conduct background checks on the issuer, its management, and owners.[787] Nigeria's draft regulation provides that a platform operator is to carry out due diligence on prospective issuers, taking reasonable steps to verify the business proposition of the issuer, conduct background checks on the issuer to ensure fit and properness, and satisfy applicable KYC and AML/CFT requirements.[788]

NOTES

659 "Global Volume by Model in 2018, USD," figure 1.8 in CCAF, *Global Alternative Finance Market Benchmarking Report,* 39.

660 Title III of the JOBS Act added Securities Act s. 4(a)(6), which provides an exemption from registration for certain crowdfunding transactions. To qualify for the exemption under s. 4(a)(6), transactions must meet a number of statutory requirements, including limits on the amount an issuer may raise, limits on the amount an individual may invest, and a requirement that the transactions be conducted through an intermediary that is registered as either a broker-dealer or a "funding portal."

661 SEC. "Final Rule: Crowdfunding", p.6 (USA), Supplementary Information (USA), 6.

662 Explanatory Memoranda, A Corporations Amendment (Crowd-sourced Funding for Proprietary Companies) Bill 2017 (Cth) (Australia).

663 Proposal for amending EU Directive 2014/65/EU on markets in financial instruments 2018.

664 World Bank and CCAF, *Regulating Alternative Finance: Results from a Global Regulator Survey, 2019*.

665 Brazilian Securities and Exchange Commission Instruction No. 588, of July 13, 2017 (ICVM 588/2017).

666 Guidelines on Recognized Markets SC-GL/6-2015(R3-2019) (Malaysia), Chapter 13.

667 Conduct of Business Module (COB) [VER36/04-20] (Dubai).

668 SEC Proposed Rules on Crowdfunding (Nigeria).

669 Corporations Act 2001 (Cth) (Australia), s. 738G(1)(b), s. 738H.

670 See *SEC v. Ascenergy LLC et al*. Case No. 15-1974 (D. Nev.).

671 DFSA Rulebook (Dubai), COB 11.3.1 to COB 11.3.2 COB/VER36/04-20.

672 FCA Conduct of Business Sourcebook—January 2018 (UK), 8A.

673 FCA Conduct of Business Sourcebook—July 2019 (UK), 4.5, 4.5A.

674 SEC's Regulation Crowdfunding introduced a new category of registered intermediary, a funding portal, which may facilitate transactions under the exemption subject to certain restrictions. The statute and the rules provide a safe harbor from broker-dealer registration under which funding portals can engage in certain activities conditioned on complying with the restrictions imposed by Regulation Crowdfunding. For example, a funding portal may not offer investment advice or make recommendations; solicit purchases, sales, or offers to buy securities offered or displayed on its platform; compensate promoters and others for solicitations or based on the sale of securities; or hold, possess, or handle investor funds or securities.

675 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 19.

676 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, preamble para 16.

677 Regulation Crowdfunding, General Rules and Regulations 17 CFR (USA), Rule 230.501.

678 DFSA Rulebook (Dubai), MKT 2.3.1, MKT/VER15/07-19.

679 Corporations Act 2001 (Cth) (Australia), s. 738G(1)(d), s. 738G(2).

680 Brazilian Securities and Exchange Commission Instruction No. 588 of July 13, 2017 (ICVM 588/2017).

681 Morita, "Crowdfunding in Japan."
682 Guidelines on Recognized Markets SC-GL/6-2015(R4-2020), 13.9.
683 Brazilian Securities and Exchange Commission Public Hearing Notice SDM No. 02/2020.
684 SEC, "SEC Proposes Rule Changes to Harmonize, Simplify and Improve the Exempt Offering Framework."
685 SEC, Facilitating Capital Formation and Expanding Investment Opportunities by Improving Access to Capital in Private Markets, A Proposed Rule.
686 See Proposal for a EU Regulation on European Crowdfunding Service Providers (ECSP) for Business, 2018/0048 (COD), 5.
687 SEC, Facilitating Capital Formation and Expanding Investment Opportunities by Improving Access to Capital in Private Markets, A Proposed Rule.
688 FCA Conduct of Business Sourcebook—July 2019 (UK), 4.7.
689 Platforms in the United Kingdom are required to classify investors to determine whether direct financial promotions for unlisted securities can be communicated to them (for example, links to an investment website or to an investment subscription form). Only retail investors who are certified as sophisticated investors, who certify as high-net-worth investors, who confirm that they will receive regulated advice, or who confirm that they will not invest more than 10 percent of their net investable portfolio in unlisted securities may be targets of direct offers.
690 FCA, *FCA's Regulatory Approach to Crowdfunding over the Internet*.
691 Guidelines on Recognized Markets, Rule 13.24.
692 DFSA Rulebook (Dubai), COB 11.5.3, COB/VER36/04-20.
693 FSA Japan, Financial Services Agency (Japan), Amendment of Financial Instruments and Exchange Act, and so on (Act No.44 of 2014) [Briefing Materials], May 2014.
694 Brazilian Securities and Exchange Commission Instruction No. 588.
695 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 21(7).
696 On *conseillers en investissement participatif*, only plain-vanilla bonds and ordinary shares are allowed. However, under the preexisting Investment Service Provider status (ISP) pursuant to MiFID regulation, a platform can offer complex products.
697 Order 2014-559 of 30 May 2014 (France).
698 Resolution no. 18592 of 26 June 2013 (Italy).
699 Order 2014-559 of 30 May 2014 (France).
700 FCA Conduct of Business Sourcebook—December 2019 (UK), 10.2.
701 Financial Instruments and Exchange Act, (FIEA 29-4-2IX) (FIEA 29-4-3III) (Japan).
702 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 21 (2).
703 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 21 (2).
704 Resolution No. 18592, June 26, 2013 (Italy).
705 The SEC's Regulation Crowdfunding (USA) introduced a new category of registered intermediary, a funding portal, which may facilitate transactions under the exemption subject to certain restrictions. The statute and the rules provide a safe harbor from broker-dealer registration under which funding portals can engage in certain activities conditioned on complying with the restrictions imposed by Regulation Crowdfunding. For example, a funding portal may not offer investment advice or make recommendations; solicit purchases, sales, or offers to buy securities offered or displayed on its platform; compensate promoters and others for solicitations or based on the sale of securities; or hold, possess, or handle investor funds or securities.
706 However, if crowdfunding is offered through broker-dealers, then suitability requirements apply.
707 DFSA Rulebook (Dubai), COB 11.3.13 COB/VER36/04-20.
708 Resolution no. 18592 of 26 June 2013 (Italy).
709 Corporations Amendment (Crowd-sourced Funding) Act 2017 (Australia), s. 738ZD and ASIC, Crowd-Sourced Funding: Guide for Companies (Regulatory Guide 261), June 2020, 261.83.
710 Guidelines on Recognized Markets SC-GL/6-2015(R3-2019) (Malaysia), Rule 13.08.
711 Regulation Crowdfunding, Crowdfunding General Rules and Regulations 17 CFR, (USA), Rule 227.402(a) (USA), Rule 227.402(a).
712 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 22.
713 DFSA Rulebook (Dubai), COB 11.5.2, COB/VER36/04-20.
714 FCA, "Review of the Regulatory Regime for Crowdfunding."
715 FCA, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms* (CP18/20).
716 Resolution no. 18592 of 26 June 2013 (Italy), art. 15.
717 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 23(6)(c).
718 DFSA Rulebook (Dubai), COB 11.3.1, COB/VER36/04-20.
719 Morita, "Crowdfunding in Japan."
720 FCA, *FCA's Regulatory Approach to Crowdfunding over the Internet*.
721 SEC, "Updated Investor Bulletin: Crowdfunding for Investors."
722 Regulation Crowdfunding, General Rules and Regulations 17 CFR, (USA), Rule 227.402(a) (USA), Rule 227.501.
723 Corporations Act 2001 (Cth) (Australia), ss. 738G(1)(a) and s. 738G(1)(c), Corporations Regulations 2001 (Cth) (Australia), r. 6D.3A.01.

724 Directive 2014/65/EU on markets in financial instruments, 2014, art. 4(1) 44.
725 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 2(1)a (ii).
726 EC 2018/0048 Proposal for a Regulation on European Crowdfunding Service Providers (ECSP) for Business, Preamble, para 11, 14.
727 Platforms that have Investment Service Provider status (ISP) pursuant to MiFID can offer complex products.
728 DFSA Rulebook (Dubai), GEN 2.2.10 F, GEN/VER44/07-19.
729 SEC Facilitating Capital Formation and Expanding Investment Opportunities by Improving Access to Capital in Private Markets (Proposed Rule, March 31, 2020) (USA).
730 FCA, "Temporary Intervention."
731 SEC, "Be Cautious of SAFEs."
732 SEC, "Be Cautious of SAFEs."
733 SEC, "SEC Proposes Rule Changes to Harmonize, Simplify and Improve the Exempt Offering Framework"
734 EC, *Crowdfunding in the EU Capital Markets Union*.
735 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 25.
736 Resolution no. 18592 of 26 June 2013 (Italy), art. 25.
737 Corporations Amendment (Crowd-sourced Funding) Act 2017 (Cth) (Australia), s. 738ZA.
738 Brazilian Securities and Exchange Commission Public Hearing Notice SDM No. 02/2020.
739 Regulation crowdfunding, General Rules and Regulations 17 CFR, (USA), Rule 227.402(a) (USA), Rule 227.201.
740 Guidelines on Recognized Markets, Rule 13.21–13.23 (Malaysia).
741 Resolution no. 18592 of 26 June 2013 (as amended).
742 FCA Conduct of Business Sourcebook—July 2019 (UK), 4.5, 4.5A.
743 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 23.
744 "Template CSF Offer Document," appendix in ASIC, *Crowd-Sourced Funding*.
745 ASIC, Crowd-Sourced Funding: Guide for Companies (Regulatory Guide 261), June 2020, 261.279-261.283.
746 FCA, "Review of the Regulatory Regime for Crowdfunding."
747 Regulation crowdfunding, General Rules and Regulations 17 CFR, (USA), Rule 227.402(a) (USA), Rule 227.303 (c).
748 DFSA Rulebook (Dubai), COB 11.3.15.
749 Guidelines on Recognized Markets SC-GL/6-2015(R3-2019), 13.27–13.30.
750 Brazilian Securities and Exchange Commission Public Hearing Notice SDM No. 02/2020.
751 Regulation crowdfunding, General Rules and Regulations 17 CFR, (USA), Rule 227.402(a), Rule 227.204.
752 DFSA Rulebook (Dubai), COB 3.2.4.
753 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 27(1).
754 FCA Conduct of Business Sourcebook—July 2019 (UK), 4.2.
755 Regulatory Law No. 1 of 2004, July 2012, art. 42(1), and DFSA Rulebook (Dubai), GEN 2.2.8.
756 SEC Nigeria Proposed Rules on Crowdfunding (Nigeria), art. 4 (e).
757 Corporations Act 2001 (Cth) (Australia), s. 738C.
758 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 12-13.
759 Regulation crowdfunding, General Rules and Regulations 17 CFR, (USA), Rule 227.402(a), Rule 227.400.
760 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 12.
761 Resolution no. 18592 of 26 June 2013 (as amended).
762 Regulatory Law No. 1 of 2004, art. 42, and DFSA Rulebook (Dubai), GEN 5.3.19, GEN/VER48/04-20.
763 SEC Nigeria Proposed Rules on Crowdfunding (Nigeria), art. 6 (a).
764 Guidelines on Recognized Markets SC-GL/6-2015(R3-2019), 4.01.
765 DFSA Rulebook (Dubai), COB 11.3.17, COB/VER36/04-20.
766 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 12 (2).
767 FCA Senior Management Arrangements, Systems and Controls Sourcebook—March (2016), 4.1.6.
768 Regulation crowdfunding, General Rules and Regulations 17 CFR, (USA), Rule 227.402(a), Rule 227.303 (e).
769 Resolution no. 18592 (as amended).
770 DFSA Rulebook (Dubai), COB 6.11–6.14.
771 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 10.
772 Resolution no. 18592 (as amended), art. 13.
773 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 8.
774 DFSA Rulebook (Dubai), COB 3.5.1.
775 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 8(1)-(2).
776 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 8 and preamble, para 26.
777 DFSA Rulebook (Dubai), COB 3.5.1.
778 SEC Regulation Crowdfunding, Rule 227.300.

779 Guidelines on Recognized Markets SC-GL/6-2015(R3-2019), Rule 13.12.
780 Regulation crowdfunding, General Rules and Regulations 17 CFR, (USA), Rule 227.402(a), Rule 227.201.
781 Guidelines on Recognized Markets SC-GL/6-2015(R3-2019), Rule 13.11.
782 Regulation crowdfunding, General Rules and Regulations 17 CFR, (USA), Rule 227.402(a), Rule 227.301.
783 FCA, Consultation Paper 18/20, 4.21 and 4.22.
784 Corporations Act 2001 Pt 6D.3.A—Crowd Sourced Funding, 738Q (5).
785 EU Regulation 2020/1503 of 7 October 2020 on European crowdfunding service providers for business, art. 5.
786 DFSA Rulebook, COB 11.3.6, COB/VER36/04-20.
787 Guidelines on Recognized Markets SC-GL/6-2015(R3-2019), Rule 13.05.
788 SEC Nigeria Proposed Rules on Crowdfunding (Nigeria), Rule 10.

E-MONEY

7

E-MONEY

7.1 INTRODUCTION

This chapter identifies consumer risks arising from electronic money (e-money), which in some cases are new manifestations of traditional financial consumer risks, together with their related regulatory approaches implemented across a range of countries. E-money is arguably the best established of the fintech products discussed in this paper. The examples in this chapter are drawn from countries that have either significant e-money regulatory frameworks in place or payments frameworks applicable to e-money. In most cases, these frameworks apply to both bank and non-bank issuers of e-money.

For completeness, it is noted that the focus of this chapter is on e-money as a payments product. Accordingly, consideration is not given to the increasing role of e-money as a gateway to other products, including savings, credit, and investment products (such as investments in government bonds or wealth-management products).

a) The significance of e-money in a consumer and inclusion context

E-money is significant in the fintech landscape for a number of reasons. They include the following:

- **Increases in the breadth and diversity of innovative fintech-enabled e-money issuers and related partnerships, products, use cases, and technologies suggest a need to focus on related FCP issues.** This is especially the case since many of the new providers are fintech entities that may be unregulated under licensing rules or FCP rules.[789]
- **E-money and financial-inclusion levels are intertwined.** The World Bank Group's *Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Agenda* (WBG Global Findex 2017) reported that around 1.7 billion adults lack an account at a financial institution or through a mobile money provider; nearly all living live in developing economies.[790]
- **The scale of mobile money adoption and usage is on the increase, along with digitization of payments.** WBG Global Findex 2017 noted increases in the use of digital payments; the share of adults making or receiving digital payments rose 12 percent.[791] The GSM Association's (GSMA) *State of the Industry Report on Mobile Money 2019* also noted two key trends in 2019 indicating that the industry had reached a "digital threshold": (1) For the first time, digital transactions represented the majority of mobile money flows (57 percent), and (2) for the first time, more value was circulating in the mobile money system than exiting.[792]
- **Regulatory reforms suggest that e-money is "coming of age" in the sense of being accepted by regulators as a critical part of national payments system architecture.** The GSMA's *State of the Industry Report on Mobile Money 2019* notes the evolution in the regulatory landscape to treating mobile money under licensing regimes for payments systems and refers to developments in jurisdictions such as Ghana, Malawi, India, Pakistan, and Tunisia.[793]

- **The increased availability and reduced cost of smartphones is likely to increase the availability of e-money services, although more could be done for women.** The GSMA's *State of the Industry Report on Mobile Money 2019* predicts that smartphone adoption in emerging markets will reach 79.4 percent by 2025.[794] However, the Global Partnership for Financial Inclusion's *Report on Advancing Women's Digital Financial Inclusion* stresses the need to facilitate women's universal ownership of mobile phones, along with supporting official identity systems.[795]
- **Finally, and importantly, the impact of the COVID-19 pandemic has increased the demand for digital payments (including e-money) in preference to cash.** Many commentators have noted this phenomenon, which is caused by a multitude of factors. They include the impact of lockdowns on both consumers and merchants; the dissemination of emergency relief, social welfare payments, and other forms of support via digital platforms; reductions in fees for payment services; and a disincentive to use cash because of the perceived risk of infection transmission from paper money.[796]

b) Relevance of FCP to address e-money consumer risks

Some potentially new consumer risks have arisen in connection with e-money, but there are also new manifestations of existing consumer risks. The more significant of these risks relate to the risk of dealing with unregulated e-money issuers; unauthorized and mistaken transactions; agent-related risks, such as agent fraud; the liquidity and solvency of the provider of the e-money product (and potentially the bank holding safeguarded funds); and operational unreliability. Traditional risks of consumers not receiving adequate information are also considered as they have particular implications when it comes to e-money.

A wide variety of regulatory approaches applicable to e-money consumer risks are well recognized, but country context is important. The more common regulatory approaches are highlighted in the discussion. However, as discussed in section 3.2 above, the suitability of a particular approach for a consumer risk will depend on country-specific factors, including the nature and scope of the relevant risk, the existing regulatory framework and especially that applicable to e-money, payments, and FCP generally, and the capacity and resources of regulators and supervisors.

c) Key definitions

There are some common characteristics in the various definitions of e-money adopted by international organizations and in regulatory frameworks. [797] For the purposes of this paper, e-money is considered to be a store-of-value product with the following characteristics: (i) it is a digital representation of a fiat currency (legal tender); (ii) it is a claim against the provider; (iii) it can be redeemed at face value on demand; and (iv) it is accepted as a means of payment by persons other than the provider. This definition does not focus on how e-money might be accessed, which could include, for example, a mobile phone, a PC, a card, or a wearable device, such as a watch.

The most common form of e-money in a financial inclusion context is probably "mobile money." This is generally understood to be a service where e-money (and other financial services) are accessed via a mobile phone.[798] The phone may be either a simple feature phone with limited internet connectivity or a smart phone. Probably the most famous of e-money examples is M-Pesa (Kenya), but there are many others.

d) Risks and approaches

The sections below discuss the more significant new manifestations of consumer risks identified as relevant to e-money and their related regulatory approaches. Consideration has been given to risks identified by national regulators, as well as guidance from international standard setters, development agencies, and other international commentators. The regulatory frameworks considered have been those focusing on e-money and/or mobile money and related payments systems, rather than, for example, general banking or consumer protection laws. For the reasons already discussed in section 2.1 above, risks relating to data protection (or other areas such as AML/CFT or competition) are not discussed in this chapter.

e) Summary of risks and regulatory approaches discussed in this chapter

Table 6 summarizes the new manifestations of consumer risks and corresponding regulatory approaches discussed in this chapter.

TABLE 6: Consumer Risks and Regulatory Approaches: E-Money

RISKS TO CONSUMERS	REGULATORY APPROACHES	SEE PAGE
Gaps in regulatory perimeter: Current requirements may not apply to all entities offering e-money products, and even if the licensing rules are "activities based," consumer protection rules may not apply to e-money as a product given innovative differences.	• Allow e-money activities to be undertaken only by licensed entities (including non-banks) • Ensure consumer protection rules also apply on an activities basis to providers of e-money • Ensure that e-money is covered by any relevant definition of financial product or service	131
Fraud or other misconduct resulting in consumer loss • Fraud or misconduct by issuers or related parties, including agents • Fraud by third parties	• Impose licensing/registration and vetting and competence requirements on e-money issuers and related parties • Impose rules specifically for agents, including requirements for agents to be trained and monitored; agent due diligence, agency agreements; publication of details of authorized agents; and clear provider responsibility and liability for agent conduct • Require operators to have in place adequate risk management and governance arrangements • Mandate transaction-authentication standards • Limit consumers' liability for an unauthorized transaction except—for example, in case of fraud or gross negligence by the consumer • Require warnings and information about security risks to be provided to consumers • Require consumers to advise providers of matters relevant to potential fraud, such as lost or stolen devices or security credentials • Place the burden of proof on providers to show transactions were unauthorized • Require reporting of large-scale fraud/security breaches • Prohibit agents from charging unauthorized fees *(Also, see below for approaches to deal with platform/technology vulnerability risks that may facilitate fraud)*	132
• Conflicts between interests of providers or agents and consumers (such as perverse incentive arrangements for agents), leading to consumer harms	• Impose conflict mitigation obligations on providers to avoid conduct to their advantage inconsistent with consumers' interests, or equivalent conduct engaged in by agents	
E-money platform/technology vulnerability or unreliability: Platform/technology unreliability or vulnerability that causes or facilitates loss, inconvenience, or other harms	• Mandate technology risk and cybersecurity management requirements • Place obligations on operators to ensure appropriate/minimum levels of operational reliability • Require notice to users of anticipated/actual service interruptions • Make a payer's institution liable for transactions not being completed as instructed	136
Mistaken transactions: A consumer's funds are misdirected to an incorrect account/recipient as a result of error, rather than fraud	• Require a mechanism that enables the consumer to verify transaction details before transaction completion • Require providers to explain how to stop transfers • Require FSPs involved in a transaction to make reasonable efforts to recover funds involved • Place the burden of proof on providers to show a transaction was authenticated and recorded accurately	137
Provider insolvency or illiquidity • A provider may become insolvent, with insufficient funds to meet the demands of e-money holders • A provider or their agents may not have enough liquid funds to meet consumer demand, such as for cash-out transactions	• Require an e-money issuer to isolate and ring-fence funds equal to e-money balances outstanding • Limit activities that e-money issuers can carry out to minimize insolvency risk • Mandate initial and ongoing capital requirements • Require issuers to maintain sufficient liquidity and to ensure that agents have sufficient liquidity to honor cash-out obligations	138

TABLE 6, *continued*

RISKS TO CONSUMERS	REGULATORY APPROACHES	SEE PAGE
E-money not covered by deposit-insurance schemes: E-money balances may not have the benefit of deposit insurance that applies to traditional accounts, in the event of insolvency of either the e-money issuer or a custodial institution holding an e-money float (such as a bank holding a trust account)	• Deposit insurance may be extended to e-money balances or to custodial accounts holding the e-money float depending on availability of scheme in the country. An alternative policy approach is to exclude e-money balances from deposit insurance schemes. (The arguments for and against each of these options are beyond the scope of this paper but are covered in other publications referenced later in this chapter)	139
E-money not permitted to be redeemed for face value: Providers may seek to apply a discount beyond transaction-processing fees	• Require funds to be redeemed at face/par/equivalent value	140
Consumers not provided with adequate information		140
• Key product information is not disclosed/available up front to consumers	• Require compliance with general transparency and/or disclosure • Require public up-front disclosure of T&C and fees and charges through all applicable channels, as well as provision of written agreements at contracting stage • Require consumers to be given notice of changes • Require standard form agreement to be lodged with regulator	
• Inadequate ongoing information, such as about ongoing transactions, changes to the product, or product suspensions or withdrawals	• Require written notice of changes to be provided to consumers • Require transaction receipts to be issued • Require periodic statements to be issued and/or that consumers are able to access details of previous transactions	
• Disclosed information cannot be easily retained by a consumer	• Require information be in a form that the customer can access and keep for future reference	
• Disclosure format risks in a digital context	• See approaches for equivalent risks summarized above in the context of digital disclosure for digital microcredit	
• Misleading marketing	• Prohibit misleading marketing in relation to e-money account • Require disclosure of provider's details in marketing materials, to assist with recourse • Impose specific rules—for example, making risk statements prominent	
Unsuitable e-money products: E-money products may not be designed to be suitable for the consumer segments they are marketed to, particularly some previously unserved or underserved consumers	• Require providers to design and distribute e-money products to meet the needs and capabilities of users in their target market • Impose individual suitability assessment requirements	144

7.2 GAPS IN THE REGULATORY PERIMETER

a) Risks to consumers

There is a risk that current financial services licensing or registration requirements do not apply to fintech entities offering e-money products.[799] In some cases, this may be as a result of a policy decision not to regulate a particular type of e-money product (such as a closed-loop e-money system). However, the concern here is with an "institutions-based" approach to licensing, where relevant rules apply only to traditional forms of financial service institutions (such as those offering banking services). Under this approach, there may be gaps in relation to existing non-financial institutions, such as MNOs, that decide to offer financial products such as e-money. The latter type of entity may be regulated by a telecommunications authority, but not by the financial services regulator (such as a central bank responsible for the payments system). A leading example of these challenges existed with the M-Pesa product in Kenya when it was initially offered by an MNO. The result may be to create a risk of regulatory arbitrage in the sense that the preferred form of an e-money issuer may depend on whether it is required to be licensed or registered or supervised by a financial services regulator. However, it is to be acknowledged that more and more countries have started to regulate e-money issuers on an activities basis, so that any entity issuing "e-money" (however it is defined) must be licensed or registered (depending on the relevant regulatory framework).

Even if financial sector licensing rules are activities based, it may be the case that FCP rules do not apply to innovative products such as e-money. This may be because of a narrow definition of the products and services covered by the consumer protection rules. For example, the relevant definition could refer to traditional payments products, such as debit and credit cards, but not cover e-money or other forms of innovative payments products.

There may also be overlaps in consumer protection rules applicable to e-money. It is not uncommon to include consumer protection provisions in e-money regulatory regimes (for example, in relation to safeguarding client funds, transparency, and consumer-recourse issues). However, there may also be an overlapping general and/or financial services–specific, consumer protection framework applicable to e-money products. Such overlaps have the potential to create confusion among consumers as to their rights, uncertainties as to the obligations of regulated entities, and also supervisory overlaps and inefficiencies.

b) Regulatory approaches

The key regulatory approach implemented by jurisdictions has been to allow e-money activities to be undertaken only by entities that are licensed or registered by a financial sector regulator. The BIS Basel Committee on Banking Supervision has noted that a requirement for a non-financial firm issuing e-money to be registered or licensed "would facilitate supervision by the prudential supervisor and the implementation of prompt corrective action or sanctions."[800] This is the EU approach, where the EU Directive on Electronic Money Institutions[801] in effect requires member states to prohibit the issuing of e-money other than by authorized entities.[802] There are also many examples of countries that have taken this approach. For example, in Ghana, under the Payment Systems and Services Act, the only entities that can engage in "electronic money business" are (i) entities licensed and authorized under the Banks and Specialised Deposit-Taking Institutions Act and (ii) non-banks licensed under the Act.[803] The Malaysia Financial Services Act provides another example of this approach. Under it, no person can carry on a business providing for the issuance of a "designated payment instrument" unless it is approved by BNM.[804] Malaysia's Financial Services (Designated Payment Instruments) Order prescribes "electronic money" as a "designated payment instrument" for the purposes of these requirements.[805]

Countries taking an activities-based approach to licensing also tend to apply the same approach to FCP requirements more generally. That is, the FCP regulatory framework applies to all types of FSPs, including specific types of providers, such as e-money issuers, that are licensed under payments laws. Australia[806] and Indonesia[807] are examples of countries where FCP requirements are applied on such a basis.

To deal with the risk that e-money may not be covered as a product by FCP provisions, countries may expressly provide for its inclusion or make provision for new products to be included at a later date. For example, Bank Indonesia's Regulation on Consumer Protection in Payments System expressly includes "electronic money activity" within its scope and also "implementation of any other Payment Systems to be specified in Bank Indonesia provisions."[808] Ghana's Payment Systems and Services Act contains various consumer protection provisions applicable to a "payment service" and defines that term as meaning "the provision of service to facilitate transfer of funds from a payer to a payee using various forms of payments instruments or electronic money."[809] The Central Bank of Nigeria's general-purpose Consumer Protection Framework applies to all institutions regulated by the central bank and refers in broad terms to their "products and services," without defining the term.[810]

7.3 FRAUD OR OTHER MISCONDUCT

a) Risks to consumers

Fraud or misconduct by issuers or related parties

A key consumer concern is suffering losses caused by internal fraud or some other form of misconduct by issuers or related parties. Potential perpetrators include e-money issuers' staff and agents and a range of related parties, such as business partners and service providers. These risks are exacerbated in relation to e-money, given its uptake. As the size and diversity of e-money networks continue to grow exponentially, new actors and business models may not be regulated or experienced or resourced enough to control or respond to the risks, and consumers may not have the digital skills to be able to detect or prevent them.

Fraud involving issuers, agents, or related parties may arise under a variety of circumstances. For example, agents may undertake fraudulent transactions after obtaining a consumer's PIN or charge unauthorized fees in over-the-counter transactions in ATM withdrawal frauds.[811] An example of internal fraud involving e-money concerned MTN Uganda, where six employees were charged with defrauding the company of U Sh 10 billion (approximately $3.4 million at the time).[812] Ponzi-type schemes have been identified in countries such as Nigeria, India, and Ghana, where e-money account holders have been attracted into digital investment schemes that later collapse.[813] Systemic fraud is a particular concern, and arguably the risks increase the more interoperable the payments system becomes.

Agents may also engage in misconduct deliberately or inadvertently.[814] The reasons may include poor selection methods for new agents, as well as a lack of training or ongoing monitoring of agents. This risk may be exacerbated where agent networks are shared if training and monitoring responsibilities are diluted. This is an increasingly important issue, given the rise in the use of e-money products and the related increase in the use of agents.

The GSMA's *State of the Industry Report on Mobile Money 2019* notes that the number of agent outlets has tripled in the last five years and that there are now around 7 million agents globally.[815]

Staff or agents may also be influenced to act not in the best interests of e-money users because of perverse incentive arrangements, such as sales-based commissions. Such arrangements may encourage them to recommend one provider over another because of the higher commissions involved, regardless of whether the product is suitable for the consumer's financial needs, objectives, or capacity.

Third-party fraud

A fundamental consumer concern with e-money and fintech products, and with transacting through digital means more generally, is the risk of loss from third-party fraud. Further, perpetrators and data may be located internationally, creating risks of cross-border enforcement and evidence gathering.[816] Consumers may suffer loss of funds as well as other harms, such as loss of personal data and identity theft.[817] These risks have been noted by various international organizations. They were recently highlighted in the 2020 report *Payment Aspects of Financial Inclusion in the Fintech Era* from the WBG and the BIS Committee on Payments and Market Infrastructures.[818] The IMF also highlighted research suggesting that there will be an increased risk of digital fraud if efforts to scale up digital payments during the COVID-19 crisis are not matched by equally paced improvements in cybersecurity.

A recent example of large-scale e-money fraud occurred in Uganda, where hackers reportedly broke into the systems of Pegasus Technologies, which processes mobile money transactions for entities such as MTN Uganda, Airtel Money, and Stanbic Bank. Billions of Uganda shillings were allegedly stolen, and bank-to-mobile-wallet payment services were temporarily suspended (although account balances were reported not to have been affected).[819]

Another example of third-party fraud is authorized push-payment scams, which may involve e-money accounts as well as other types of payments accounts. These scams involve tricking victims into sending money to a fraudster. They have been widely reported as a problem in the United Kingdom, leading to the development of a voluntary code by payment service providers (including e-money institutions, among others). This is the Contingent Reimbursement Model Code for Authorised Push Payment Scams 2019, which was welcomed by the UK Payments System Regulator.[820]

b) Regulatory approaches

Licensing and vetting requirements

The risk of fraud may be reduced by requiring e-money issuers to be licensed or registered and strict vetting standards for any applicant and key senior management members. As noted above, many countries require e-money issuers to be licensed or registered. The assessment of an application for licensing or registration should include (among other things) vetting the ability of the entity and its senior management to assess and mitigate the risk of internal or external fraud and to implement any required risk management controls. For example, under the EU Directive on Electronic Money Institutions and the related provisions of PSD2, an applicant for an e-money institution license is required to provide evidence of the suitability of persons with specified holdings of capital or voting rights, taking into account the need to ensure sound and prudent management of the institution.[821] A key operational principle specified in Malaysia's e-money rules is that there be a board of directors and management with caliber, credibility, and integrity who fulfill mandated fit and proper requirements.[822]

Agent-related approaches

Regulatory frameworks applicable to e-money often include several measures to address risk of agent fraud or misconduct. Approaches to agent regulation differ. Some rules are institution based (such as those applying only to licensed banks), while others are overarching activities-based rules (so they apply to both banks and non-banks using agents).[823] Examples of applicable rules include the following:

- **Requirements for agents to be trained and monitored:** For example, Malawi's Payment Systems (E-Money) Regulations require that an e-money provider be responsible for the training and supervision of agents. Focus is on the use of the e-money system, customer support and education, monitoring of agent liquidity, and handling of customer complaints.[824] In contrast, Kenya's National Payment Systems Regulations simply require that if a payment service provider wishes to enlist an agent, then, at least 14 days before the appointment, they must notify the Central Bank of Kenya and provide the relevant training manual and related materials.[825] Ethiopia's Use of Agents Directive includes broad requirements in relation to training, contains detailed rules as to how agents should be monitored and supervised by the financial institution (which would include an e-money issuer), and also sets out the supervisory powers of the National Bank of Ethiopia in relation to agent networks.[826]

- **Requirements for agent due diligence:** For example, Kenya's National Payment System Regulation requires that a payment service provider exercise due diligence and carry out suitability assessments in identifying, selecting, and contracting agents or cash merchants.[827] Ethiopia's Use of Agents Directive also requires that a financial institution (including e-money issuers) "establish efficient, clear, well documented and comprehensive agent due diligence policies and procedures for initial and ongoing assessment of agents in a way that mitigates risks."[828]
- **Content requirements for agency agreements:** Ghana's Payment Systems and Services Act provides detailed requirements for the content of agency agreements and also for the responsibility of principal and master agents.[829] Ethiopia's Use of Agents Directive also requires extensive minimum provisions to be addressed in an agency agreement.[830]

In addition, to reduce the risk of unauthorized third parties fraudulently posing as agents, regulators frequently require the publication of lists/registers of authorized agents and/or requirements for agents to display evidence of authorization. This evidence could be the unique agent number and photo and/or the registration number issued by the regulatory authority. For example, the Payment Systems (E-Money) Regulations in Malawi require that an e-money provider ensure that its agents display their agent identification number. Afghanistan's Electronic Money Institution's Regulation has a broad requirement that an "electronic money institution" ensure that customers can verify that an enterprise is an authorized agent. Examples of measures that might be taken include a public database of authorized agents, signage that cannot be copied, displaying a unique photo and number, and a general customer-awareness program.[831]

There may also be requirements for agents to have a business permit or some other qualification. For example, Kenya's National Payment System Regulation provides that a person cannot be appointed as an agent or a cash merchant unless the person has a registration, business license, or permit covering their commercial activities.[832] Singapore also requires agents to be licensed. A licensee is prohibited from providing a payment service thorough an agent unless the agent is licensed.[833]

Risk management and governance

Jurisdictions have applied risk management and governance obligations to e-money issuers. This is in addition to the more specific risk management approaches discussed above. Malaysia's Guideline on Electronic Money requires an issuer of e-money to establish effective and transparent governance arrangements to ensure the continued integrity of their e-money scheme, including segregation of duties and internal control arrangements to reduce the chances of mismanagement and fraud.[834] In addition to requiring compliance with technical standards issued from time to time by the Central Bank of Kenya, Kenya's National Payment System Regulations impose an obligation to comply with specified international standards and any risk management guidelines.[835]

Importantly, technology-related and cyber risk management requirements are also essential approaches to address fraud risk that arises from vulnerabilities affecting e-money platforms and systems. These are discussed in the next section in the context of platform and technology unreliability and vulnerability risks.

Transaction authentication and other fraud prevention standards

Regulators apply numerous approaches to dealing with the risk of unauthorized transactions. They may include any of the following:

- **Mandate transaction-authentication standards so as to minimize the risk of fraud.** For example, the European Union's PSD2 requires "strong customer authentication" when a transaction is initiated.[836] The definition of this term in effect contemplates two-factor authentication, requiring the use of two or more independent elements categorized as knowledge (something only the user knows, such as a PIN) and possession and inherence (something the user is).[837] In contrast, the People's Bank of China's Measures for the Administration of Online Payment Business of Non-Bank Payment Institutions allow use of one or more of three specified authentication standards; the specified transaction limits depend on the standard(s) chosen.[838]
- **A consumer's liability for an unauthorized transaction may also be limited under certain circumstances.** There may be exceptions to such limitations, such as in the case of consumer fraud or gross negligence or unreasonable delays in reporting a lost or stolen card or device, or under more specific circumstances, such as disclosure of a PIN or leaving a card at an ATM. For example, under the European Union's PSD2, the basic rule is that the payer can be made liable only for up to €50 for an unauthorized transaction unless there is fraud or gross negligence.[839] However, the provider may not be liable if notice of an unauthorized transaction is not given in a specified period.[840] Australia's ePayments Code has quite complex provisions on unauthorized transactions.[841] They start by setting out the circumstances under which the holder of the account will have no liability for an unauthorized

transaction (such as fraud by the provider's employees or agents), and then set out the circumstances under which the holder may be liable for all or part of the loss. These losses include those that occur before the loss or theft of a device or passcode is reported and those that result from a breach of security requirements. The provider has the burden of proof in these cases, and, in any event, there is no liability for losses that exceed transaction limits. In other cases, there is an A$150 cap on liability (with some exceptions, where it may be lower). Many other countries, such as India and Kenya,[842] have variations on these provisions that, generally speaking, are also oriented in favor of consumers.

- **Require consumers to be advised of the need to report lost or stolen mobile devices or any security credentials (such as a PIN) and any suspected unauthorized use of the e-money account.** The European Union's PSD2 requires that users be advised of their obligation to report such events "without undue delay" and that users have "appropriate means" to make such reports.[843] Afghanistan also requires that payment service providers educate customers on security features and capabilities and the importance of protecting personal information.[844]
- **Some countries also place the burden of proof on the provider if they want to show a consumer is liable for all or part of an unauthorized transaction.** The European Union's PSD2 is explicit in this regard.[845] Ghana's Payment Systems and Services Act takes a slightly different approach, requiring a provider to "ensure" that a transaction against an account is authorized by the account holder.[846]

Liability and responsibility for staff and agents

While providers to some extent may be liable for conduct of persons acting on their behalf under general laws (for example, of employment or agency), regulators commonly consider it necessary to impose responsibility and liability for such matters, especially for agents. The concern of regulators and other commentators is that a provider may seek to disclaim liability for the acts or omissions of their agents, including in relation to such matters as fraud or incorrect advice (among others).[847] Without regulatory intervention, this is likely to occur given the greater bargaining power of the provider. In such cases, affected consumers would need to resort to seeking redress from the relevant agent, who may not be able to deal with the issue and is unlikely to have sufficient resources to compensate consumers. This is a significant issue, given the potential for agents to engage in fraudulent activities. The risks of fraud are increasing with the growth of e-money services and rapid increases in the size of agent networks. As mentioned above, the GSMA's *State of the Industry Report on Mobile Money 2019* states that the number of agent outlets is now around 7 million agents globally.[848] Against this background, regulators have introduced various approaches to deal with this risk.

Providers are usually required to accept responsibility for their agents, including (in some cases) even if actions are not authorized. These provisions are common but vary in approach.[849] Kenya's National Payment System Regulations are narrower, as they impose liability only for the actions of agents that are "within the scope of the agency agreement." However, an agency agreement cannot exclude a payment service provider from liability.[850] Bank Indonesia's Regulation on Consumer Protection in Payments System refers to "losses arising from the mistakes of its management and employees" and so is also quite narrow in scope.[851] In contrast, Ghana's Payment Systems and Services Act expressly makes a principal liable for all acts of an agent "in respect of the agency business" even if the acts are not authorized by the agency agreement.[852] Ethiopia's Use of Agents Directive has a similar approach.[853]

Some regulators also prohibit agents from charging fees. This is designed to prevent such practices as agents charging fees over and above those that may be charged by the provider of the e-money product (for example, fees for cash-in or cash-out transactions or fees for the opening of an account). For example, Malawi's Payment Systems (E-Money) Regulations require an e-money service provider to ensure that its agents "do not charge any additional fees or tariffs to customers above those specified by the e-money service provider."[854] Ghana's Payment Systems and Services Act specifically prohibits agents from charging a fee beyond that charged by the principal.[855]

General conflicts mitigation obligations of the kinds already discussed in chapters 5 and 6 would also be relevant approaches in this context. Some jurisdictions have implemented additional targeted approaches. For example, Ghana's Payment Systems and Services Act prohibits an agent from approving an application for credit, insurance, or an investment product.[856]

Warnings and information for consumers

Some e-money regulatory frameworks require reporting to the regulator of large-scale fraud/security breaches. For example, Ethiopia's Licensing and Authorization of Payment Instrument Issuers Directive requires the prompt reporting to the National Bank of Ethiopia of any suspected or confirmed cases of fraud or major security breaches.[857] The European Union's PSD2 also requires that users be informed of any security incident that may have an impact on their financial interests.[858]

It is also common to require consumers to be educated about security risks with the goal of preventing unauthorized transactions. For example, the requirements may be to provide advice on security features, ways to reduce the risk of fraud, the need to keep PINs confidential, and the liability regime for unauthorized transactions. Australia's ePayments Code requires that users be given guidelines on the security of their devices and passcodes in the T&C or in other publications. These guidelines must be consistent with requirements in the code on security of passcodes and must also clearly distinguish the circumstances under which there is liability for unauthorized transactions.[859] Similar requirements are found, for example in the European Union's PSD2[860] and applicable rules in Malaysia.[861]

7.4 E-MONEY PLATFORM/ TECHNOLOGY VULNERABILITY OR UNRELIABILITY

a) Risks to consumers

If platforms and other technology systems for an e-money product do not operate as expected, or are vulnerable to threats, consumers can be at significant risk of suffering loss, inconvenience, or other harms. This risk was highlighted in the 2016 *G20 High-Level Principles for Digital Financial Inclusion*, which stressed the need for the digital financial services ecosystem (including retail payments systems infrastructure) to be reliable and safe.[862] This point was also made recently by the WBG and the BIS Committee on Payments and Market Infrastructures in the report *Payment Aspects of Financial Inclusion in the Fintech Era*. The report included as a key action for consideration (in summary) the testing of payments infrastructure on an ongoing basis and enhancement as necessary to keep up with emerging threats to holders of transaction accounts as well as payment service providers and operators.[863] Unreliability and vulnerability may arise due to a variety of factors. For example, they may be because of poor system design (for example, the system is slow in operating or is not designed to limit errors in payments processing or does not expeditiously correct them), or they may be affected by external causes (such as a failure affecting a cell phone base station or the entire system or a dropped connection affecting a single transaction).

Although unreliability and vulnerability risks have always existed in the context of e-money systems, the scale of the risks and the potential for loss is rapidly increasing with the rise in e-money accounts and the number and value of transactions. The GSMA's *State of the Industry Report on Mobile Money 2019* highlighted key statistics reflecting these trends, including the milestone of 1 billion registered mobile money accounts.[864] Further, operational failures are a very real risk for consumers. A well-known example is the 2017 M-Pesa system outage, which affected a number of its core processes, reportedly lasted around seven hours, and led to a one-day waiver of fees for sending money on the M-Pesa network.[865] Many other outages have been reported since then, including a major outage in December 2018.[866]

These risks may cause various types of consumer issues. Apart from inconvenience caused by loss of time and general frustration, there may be the additional risk of losses caused by fraud, losses of date integrity, or penalties applied if transactions cannot be completed on time (such as late payment fees and penalty interest). Consumers unable to make payments for essential services, such as utilities, may suffer great inconvenience if these services are not available to them because an e-money system is unable to complete a payment transaction. Against this background, it is no surprise that the inability to transact due to network downtime or system unreliability was the most common risk identified in a 2016 CGAP report.[867] Ultimately, it is likely that poor operational reliability will result in a lack of trust in the e-money system with likely adverse effects on financial-inclusion levels.

b) Regulatory approaches

In addition to more general risk management and governance standards mentioned above, regulators have been imposing more targeted risk management and operational reliability requirements. These include the following:

- **Mandating technology risk- and cybersecurity-management requirements:** Ghana's Payment Systems and Services Act requires an appropriate and tested technology system that is equipped with fraud monitoring and detection tools and a third-party certificate as to compliance with standards specified by the Bank of Ghana and a cybersecurity policy, where applicable. Payment service providers are also prohibited from engaging in acts likely to result in systemic risk or affecting the integrity, effectiveness, or security of the payments system.[868] In the European Union, security rules under PSD2 require that there be a security policy in place, including detailed risk-assessment and related control and mitigation measures, to adequately protect users against risks such as fraud. In contrast, Malawi's Payment Systems (E-Money) Regulations simply require the delivery of "secure" e-money services.[869] These requirements are accompanied by system-audit requirements.[870]

- **Mandating that e-money and related payments systems ensure operational reliability:** A general requirement and/or specific requirements may cover issues such as transaction processing, system capacity, business continuity, disaster recovery, incident responses, and back-ups. For example, the European Union's PSD2[871] requires that payment service providers have appropriate mitigation measures and control mechanisms to manage operational (and security) risks, and that they make reports to the regulator on these risks at least annually.[872] Kenya's National Payment System Regulations require measures to ensure "operational reliability of the service including contingency arrangements."[873] Malaysia's Guideline on Electronic Money has more detailed requirements, including for comprehensive and well-documented operational and technical procedures to ensure operational reliability, and a robust business continuity framework, including a reliable back-up system (ss. 8.2–8.5). Malawi's Payment Systems (E-Money) Regulations provide other example of these type of specific requirements.[874] The Payment Systems and Services Act in Ghana has a specific requirement that an e-money issuer (or a payment service provider) ensure "high quality performance of at least 99.5% service availability and accessibility."[875]
- **Requiring notice to users of anticipated/actual service interruptions:** Afghanistan,[876] China,[877] the European Union, [878] and Ghana provide examples of such requirements. Ghana's Payment Systems and Services Act requires that users of e-money be notified within 24 hours of a service disruption or an anticipated disruption. This notice must be given by SMS or another means approved by the Bank of Ghana.[879] Some countries also require reports to the regulator of major operational or security incidents. Ethiopia's Licensing and Authorization of Payment Instrument Issuers Directive requires that agreements with users provide for announcements about service interruptions and also requires quarterly reports to the National Bank of Ethiopia about the number, duration, and reason for service interruptions and the measures taken to resolve the issue.[880]
- **Making the payer institution liable for transactions not being completed as instructed:** Afghanistan,[881] the European Union, and Ghana[882] all have such requirements. In the case of the European Union's PSD2, the liability extends to an obligation to make a refund to the payer "without undue delay." However, there will be no liability if the payment service provider can prove that the payee's institution received the transaction amount. The payer's payment service provider is also obliged to try to trace an incorrectly executed transaction.[883] There is, however, some protection for the payment service provider, as they will not be liable, in summary, under abnormal or unforeseeable circumstances beyond their control and the consequences of which are unavoidable. [884]
- **Making clear the user has no liability for system/equipment/electronic network malfunction:** Australia has such a provision in the ePayments Code. However, this is subject to the qualification that, if the user should reasonably have been aware that a system that is part of a shared network was malfunctioning, then liability may be limited to correcting errors and refunding fees. [885]

7.5 MISTAKEN TRANSACTIONS

a) Risks to consumers

Mistakes in e-money transactions are a key consumer protection concern, as they may result in an accountholder's funds being misdirected to the incorrect account, and it may be difficult to have the mistake corrected, especially given the need for irrevocability of payments transactions. This risk has been highlighted in various international guidelines and standards.[886] The mistake may be caused by users (for example, because of a confusing user interface) and also by agents or other persons who are assisting them. This is a human-error issue, rather than fraud. It is especially likely to occur with consumers who are new to financial services and not used to using their mobile phones to conduct financial transactions. Of course, mistakes could have arisen with electronic payments transactions even before the advent of e-money, but it is the scale of the risk in this context that is of concern, given the abovementioned rapid growth in the use of e-money and the likely low levels of digital capability in a financial-inclusion context.

b) Regulatory approaches

Various regulatory approaches have been developed to deal with this important issue. They include the following:

- **Requiring a mechanism that enables the consumer to verify the details of a transaction after it has been initiated but before it is finalized**: For example, Eswatini's Mobile Money Service Providers Practice Note requires that there must be a mechanism for the customer to verify the name and number of the proposed recipient before the transaction is finalized.[887] Malawi has a similar requirement, but it applies only "where feasible."[888]
- **Requiring that the provider explain how to stop transfers:** Afghanistan's Electronic Money Institution's Regulation requires that an e-money institution clearly

explain to its customers how to stop a transfer that was initiated in error or without consent.[889]

- **Requiring that the financial institutions concerned assist in resolving any mistake:** Where a user claims that a transaction was not properly executed, the European Union's PSD2 puts an onus on the provider to "prove that the payment transaction was authenticated, accurately recorded entered in the accounts and not affected by a technical background or some other deficiency of the service."[890] The provider also has an obligation to make "reasonable efforts" to recover the funds involved.[891] Australia's ePayments Code has detailed provisions relating to mistaken payments that also put an onus on the provider to assist the user in the case of a mistaken transaction.[892]

There do not yet seem to be examples of regulations that require the user interface for e-money to be designed so that it is simple and easy to use, to assist in minimizing the risk of mistakes. CGAP, for example, proposes 21 principles for user interface/user experience design in the context of mobile money.[893] The suggestions for improvements to user interfaces discussed in chapter 4 in relation to digital microcredit may also assist.

7.6 PROVIDER INSOLVENCY OR ILLIQUIDITY

a) Risks to consumers

A significant risk associated with e-money arrangements is that a provider may become insolvent and funds may be insufficient to meet the demands of e-money holders.[894] The balance in an e-money account may not be considered a "deposit" protected under banking regulations. Examples of protective regulations for such deposits include depositor priority rules in a winding-up.[895] For example, the European Union's Directive on Electronic Money Institutions makes it clear that the issue of e-money is not a regulated deposit-taking activity, given that it is considered to be a surrogate for banknotes and coins to be used as a means of payment, rather than saving.[896] Deposit insurance rules may also not apply to e-money accounts, as discussed further below. The result of this lack of protection is likely to be that e-money holders will rank with other unsecured creditors and will be paid after any deposit holders, any secured creditors, and any other creditors with some other form of statutory priority.

There is also the risk that an e-money provider or their agents may not have enough liquid funds to meet consumer demand on a day-to-day basis, especially for cash-out transactions. Non-bank e-money issuers that are not prudentially regulated are of most concern in this regard, as they would not be subject to the full range of liquidity and capital requirements. A related risk is that agents may not have enough liquidity, in the sense of not having enough cash or "e-float," to satisfy consumer demands, even if the provider has sufficient liquid funds.

b) Regulatory approaches

Segregation of client funds

The most common regulatory approach to covering the risk of providers becoming insolvent is to require an e-money issuer to isolate and ring-fence funds equivalent to the amount of outstanding e-money balances in a trust account or equivalent that is segregated and unencumbered.[897] The funds may be required to be held in separate accounts (usually in the nature of trust accounts) held in one or more prudentially regulated banks, in government securities, or in other investments that are considered to be similarly secure. For a discussion of issues related to a requirement for segregation of client funds, see the 2019 World Bank report *Prudential Regulatory and Supervisory Practices for Fintech: Payments, Credit and Deposits*.[898]

Jurisdictions take various approaches to such segregation requirements.[899] Malawi's Payment Systems (E-Money) Regulations require that an e-money service provider maintain a trust account at a bank that holds an amount equal to no less than 100 percent of outstanding balances, and that no more than 50 percent may be held in any one bank. The funds in the trust account must be unencumbered and must not be intermediated.[900] In contrast, the European Union's PSD2 provides two options for safeguarding funds: (1) to keep funds matching outstanding balances in a separate account in a prudentially regulated credit institution or invested in secure, low-risk assets as defined by a member state, or (2) to cover the outstanding funds with private insurance from an unrelated (e-money) issuer or credit institution that is payable if the payments issuer is unable to meet its financial obligations.[901] Bank Indonesia's E-Money Regulation requires, in summary, 30 percent of the e-money float to be held in a commercial bank and 70 percent to be held in government or Bank Indonesia securities or financial instruments or in an account at Bank Indonesia.[902]

In some cases, the segregated account obligations apply only to non-bank issuers, and banks have lesser obligations (presumably because of the prudential regulations that apply to them). For example, under Tanzania's Payments Systems (Electronic Money) Regulations, banks and other financial institutions that are e-money issuers have to open a "special account" to maintain funds deposited by non-bank customers issued with e-money,

whereas other e-money issuers must maintain these funds in a trust account maintained by a separate trust entity.[903]

Regulatory frameworks may also require multiple banks to hold the trust account or equivalent balances. Some countries require safeguarded funds to be held in more than one bank when the safeguarded funds reach a certain threshold. This is to cover the risks that the bank may become insolvent even if the e-money issuer is solvent. For example, Kenya's National Payment System Regulations provide that if the relevant amount is over K Sh 100 million, then the funds must be held in a minimum of two "strong rated banks" with a maximum of 25 percent in any one bank. [904] Malawi's Payment Systems (E-Money) Regulations state that only 50 percent of trust funds may be maintained with a single bank at any one time.[905]

Limit activities e-money issuers can carry out

This approach is designed to protect against the risk that providers may dissipate their e-money assets through the need to support other businesses. Many countries and regions have such requirements, including the European Union,[906] Ghana,[907] Malawi,[908] Malaysia,[909] and Singapore.[910] For example, under Malawi's Payment Systems (E-Money) Regulations, an e-money issuer is prohibited from carrying out any business other than e-money services, or other than banking business if they are a bank.[911] In some cases, additional activities may be carried out with the approval of the regulator. Under the Indonesia E-Money Regulation, approval may be obtained for "cooperation" activities (for example, with other service providers).[912]

E-money businesses may also be required to be in a separate subsidiary or in a business unit that is separate from other businesses (especially for non-banks). A requirement for non-bank e-money issuers to establish a separate legal entity has also been endorsed by the Bank for International Settlements Basel Committee on Banking Supervision.[913] The E-Money Circular of Bangko Sentral ng Pilipinas' (BSP), the Central Bank of the Philippines, provides that non-bank providers may provide e-money services only through a separate entity incorporated exclusively for that purpose.[914] In contrast, Kenya's National Payment System Regulations provide for a payment service provider to separate its payment services in a separate business unit with a separate management structure and books of account.[915]

Require liquidity to be maintained

In addition to the above safeguards, there may also be a specific requirement to maintain liquidity on an ongoing basis. For example, Malaysia's Guideline on Electronic Money requires issuers to ensure that they have sufficient liquidity for their daily operations.[916] Malawi also requires that e-money service providers ensure that their agents maintain sufficient liquidity to honor cash-out obligations to their customers. [917]

Initial and ongoing capital requirements

Capital requirements may also be imposed on e-money issuers. These requirements may relate to both initial and ongoing capital and may differentiate on the basis of factors such as whether the provider is a bank or non-bank financial institution, the nature of their activities, and the size of the e-money business of the provider. Requirements may also vary from time to time, as determined by the regulator. Many countries and regions have such requirements for e-money issuers. For example, Malaysia's Guideline on Electronic Money is to the effect that issuers of "large e-money schemes" are required to maintain unimpaired shareholders' funds of RM 5 million or 8 percent of the monthly average of their outstanding e-money liabilities over the last six months, whichever is higher. These rules apply only to issuers that are not licensed under Malaysia's Banking and Financial Institutions Act of 1989, the Islamic Banking Act of 1983, or the Development Financial Institutions Act of 2002. A "large e-money scheme" means a scheme with a purse limit exceeding RM 200 and outstanding e-money liabilities for six consecutive months of RM 1 million or more. [918] For further discussion of capital requirements applicable to e-money issuers in a wide range of countries, see the 2019 WBG report *Prudential Regulatory and Supervisory Practices for Fintech: Payments, Credit and Deposits.*[919]

Recovery and resolution planning

Finally, a regulatory approach that might be considered is including specific requirements for large e-money issuers, especially those that are dominant in their markets, on reorganization plans and plans to exit the market in an orderly manner, akin to recovery and resolution plans applicable for the banking sector. This issue is raised for completeness, as it is beyond the scope of this paper to consider it in detail.

7.7 E-MONEY NOT COVERED BY DEPOSIT INSURANCE SCHEMES

a) Risks to consumers

E-money balances may not have the benefit of deposit insurance that applies to traditional accounts. One of the objectives of such insurance is to protect consumers if the institution holding the relevant funds fails. As CGAP noted in a recent paper, there are two general approaches to deposit insurance in relation to e-money accounts: the direct approach, where e-money accounts are consid-

ered to be eligible accounts under the deposit insurance scheme, and the pass-through approach, where cover "passes though" an account (such as a trust account) held at an institution covered by the deposit insurance scheme.[920]There is also the exclusion approach, whereby the products are expressly excluded from the deposit insurance scheme. Arguments for and against each of these options are outside the scope of the current discussion but have been recently canvassed by CGAP[921] and country context will of course always be a key consideration. Regardless of the approach taken, consumers should know whether their e-money balances are protected, and this should be clear from the regulatory framework.

For completeness, it is also noted that, besides deposit insurance, there are other controls designed to mitigate the risks of insolvency of a custodial institution holding an e-money float (such as a bank holding a trust account). For a full discussion of relevant controls (including as to insolvency of the provider as well as the custodial institution) see the 2019 World Bank report *Prudential Regulatory and Supervisory Practices for Fintech: Payments, Credit and Deposits*[922] and the 2020 report *Payment Aspects of Financial Inclusion in the Fintech Era* from the WBG and the BIS Committee on Payments and Market Infrastructures.[923]

b) Regulatory approaches

Some jurisdictions have chosen to make clear in their frameworks that e-money balances are in fact covered by deposit insurance. Ghana's Payment Systems and Services Act provides that an e-money holder is eligible for protection under the Ghana Deposit Protection Act, provided their balance is within the prescribed threshold.[924] Afghanistan's Electronic Money Institution's Regulation requires the "mother" or "pooled account" to be insured with the Afghan Deposit Insurance Corporation. If the corporation does not exist, then the e-money institution must ensure that e-money deposits are "fully insured by a solvent, licensed insurer."[925]

Some jurisdictions have made the decision to clearly exclude e-money balances from deposit insurance and to require consumers to be warned about this being the case. Under the Philippines BSP E-Money Circular, e-money is not considered a deposit when issued by banks and is not insured by the Philippine Deposit Insurance Corporation. Further, customers must be advised of this fact and must agree in writing.[926] A similar position applies in China under the Measures for the Administration of Online Payment Services by Non-Bank Payment Institutions.[927]

In some jurisdictions, deposit insurance may apply to a custodial account holding the e-money float, for the benefit of the individual e-money holders. The United States takes this approach. The Federal Deposit Insurance Corporation has rules to the effect that the deposit insurance scheme covering a pooled account held for the purposes of a prepaid card program will pass through to the individual card holders if the records of the deposit institution acknowledge the agency or custodial relationship; if there are records of the cardholders and the amounts due to them; and if the funds in question are clearly owned by the prepaid cardholders.[928] The existence of such insurance must be noted on the mandatory short-form disclosure document for such products.[929]

7.8 E-MONEY NOT REDEEMABLE FOR FACE VALUE

a) Risks to consumers

Consumers wanting to redeem their e-money balances may face the unexpected risk of providers withholding a portion of those balances. This may be the case if providers seek to apply a discount to the funds redeemed in addition to or instead of market-based fees that apply for a redemption service. For completeness, this is different from the risk that a government may act to limit cash-out services in the event of a cash crisis, as was the case in Zimbabwe in 2019.[930]

b) Regulatory approaches

The common regulatory approach for this risk is mandating that providers allow e-money balances funds to be redeemed at face value, sometimes also referred to as par or equivalent value. This requirement applies in a wide range of jurisdictions, including Afghanistan,[931] the European Union,[932] Ghana,[933] Kenya,[934] Malawi,[935] and the Philippines.[936] For example, Malawi's Payment Systems (E-Money) Regulations provide that e-money must be issued and redeemed in Malawi kwacha as legal tender and redeemed for face or par value.[937] In contrast, Singapore's Payments Act appears to prohibit the exchange of e-money for Singapore currency for users who are resident in Singapore, other than on closure of the account.[938]

7.9 CONSUMERS NOT PROVIDED WITH ADEQUATE INFORMATION

a) Key product information not disclosed upfront

Risks to consumers

As in the case of digital microcredit, discussed in chapter 4, poor disclosure practices are a common concern with respect to e-money.[939] While transparency-related

risks are already a concern in connection with traditional products, they are exacerbated in the digital environment of e-money, given the technological interface through which information is provided (it is often provided on a small mobile phone screen); the fact that it may not be possible to retain the information for future reference (for example, where it is provided on a feature phone with limited internet connectivity); the speed with which the information may be presented to the consumer, which gives them little time to read or understand the information; and that the consumers are likely to have low levels of financial or digital literacy. Another challenge may be that consumers feel that they have little choice about accepting a particular e-money product and hence do not see the point in reading all the T&C. This could occur, for example, where there is limited competition between e-money issuers and where consumers are offered a digital account as a means of receiving wages or cash transfers or other benefits (such as those provided as a result of the COVID-19 crisis).

If the consumer is not provided with key e-money product information, or the information provided is not clear, they may not understand the product features and functions, will not understand how much it will cost or how to use it, and they will be unable to compare offers easily. For example, research by CGAP in Kenya on consumers' awareness of changes in transaction fees for the popular M-Pesa product indicated a failure to take advantage of favorable aspects of these changes even though they were widely publicized. This research also indicated that consumers had limited knowledge of competitors' fees; some mistakenly believed that Airtel Money was more expensive.[940] The end result of such misunderstandings and nondisclosures generally may be that consumers choose products that do not meet their needs and incur costs that could have been avoided. This may lead to low usage levels of the product in question and ultimately low levels of trust in at least e-money products and perhaps more broadly.

Regulatory approaches

Providers have been required to comply with an overarching principle of transparency and/or disclosure. For example, in Malawi, a specific rule states, "An e-money service provider shall adopt market conduct and consumer protection measures that comply with principles of… (b) full disclosure of information."[941] Other examples of general transparency obligations applicable to e-money are provided by the regulatory regimes in Ghana,[942] Indonesia,[943] Malaysia,[944] and Nigeria.[945]

Disclosing contractual T&C to the consumer is one of the most common regulatory requirements. For example, the European Union's PSD2 requires the disclosure of information about framework contracts for payment services; the requirements apply to contracts for e-money services.[946] Other examples are in the regulatory frameworks in countries and regions as varied as Australia,[947] Ethiopia,[948] Indonesia,[949] Kenya,[950] and Nigeria.[951]

Require disclosure of fees and charges to consumer. This is also a common requirement. Eswatini,[952] the European Union,[953] Kenya,[954] Malawi,[955] Malaysia,[956] and Nigeria[957] all provide examples. In some cases, there is a requirement to disclose fees both up front and on a transaction basis. For example, the European Union's PSD2 requires that all charges be disclosed to the consumer before the contract is entered into and before a transaction is initiated. Separately, there are mandatory EU requirements for standardized disclosures of fee information on consumer payments accounts, including information about the standardized terms and definitions to be used to describe common fees and a mandatory fee information disclosure template. The United Kingdom is one example of a country that has introduced such requirements.[958] Kenya provides another example of transaction-specific fee disclosure requirements, as the Competition Authority of Kenya's 2016 rule requires that mobile FSPs present full transaction cost information at the time of the transaction and on the same screen. Research by CGAP has suggested that this requirement has resulted in increased pricing awareness.[959]

Requiring the up-front availability of key information through applicable channels, including on websites, through agents, and in any branches, is an important measure to ensure accessibility. Kenya's National Payment System Regulations require information about charges (and other T&C) to be displayed "prominently at all points of service."[960] Malaysia's Guideline on Electronic Money also requires that information about fees and charges (and other T&C) be made available through "various channels," which include the issuer's website, brochures, and registration form (user's and merchant's copy).[961]

Requiring that a written agreement be provided to each consumer covering the terms of the service and any related fees can be a complementary approach, and it may help consumers retain such information. For example, Kenya requires that a payment system provider complete a customer service agreement with every customer and that it contain specified information, including information about many of the issues detailed above.[962] Other examples of such requirements are in China,[963] Ghana,[964] Malaysia,[965] and the Philippines.[966]

b) Inadequate ongoing information

Consumers also face risks if they are not provided with ongoing information about their use of an e-money account. This may mean they cannot keep track of transactions and account balances for financial management and budgeting purposes, and it may also make it difficult to identify fraudulent activity or mistaken transactions. Given the potential lack of physical touchpoints with providers (such as branch visits that may be usual when operating a traditional account), the importance of providing such information to consumers can be even more significant in this context.

Risk of insufficient notice of changes

Without sufficient notice of changes to their e-money account, consumers may not to be able to deal with such changes adequately—such as by closing or switching products. Any adverse impact of such a change may therefore be increased. For example, a consumer may be unaware that a provider may unilaterally withdraw or suspend a product, and that, if this were to occur without notice, it could cause considerable inconvenience for the consumer and possibly expose them to late payment fees and other penalties if the facility is unavailable when needed. An example of the considerable impact of even a temporary suspension of e-money accounts was provided when the Uganda Communications Commission ordered mobile money operators to disable their platforms during an election. The effects included an inability to pay school fees and for utilities such as electricity and water, and, perhaps more significantly, a loss of trust in the mobile money system, indicated by the emptying of mobile wallets when the platform became operational again.[967]

Regulatory approaches

Regulators now frequently require consumers to be given notice of changes to T&C and fees and charges. Many countries and regions have such requirements, but there are variations in the time period for giving of notice, the nature of changes that must be notified, and how the notice may be provided. For example, in the Australian ePayments Code, at least 20 days' advance notice must be given of changes to fees for transactions, issuing a device or passcode, any increase in liability for transaction losses, and also changes to daily or periodic transaction limits. There are also tailored requirements for low-value facilities (those that can have a balance of no more than A$500 at any time). Otherwise, notice must be given before the change takes effect. These notices may be given electronically.[968] In the European Union, under PSD2, there must be a two months' notice of changes to a wide variety of matters, including to charges (fees) and provisions concerning mistaken and unauthorized transactions.[969] In contrast, Ghana's Payment Systems and Services Act requires seven days' notice of changes to fees and charges, and notice must be made by SMS or any other method approved by the Bank of Ghana.[970] None of the regulatory regimes reviewed appear to negate the effect of the change if the required notice is not given, although breaches may be the subject of complaints and/or penalties.

Some jurisdictions have also specifically required providers to give advance notice of withdrawal or suspension. The European Union adopts this approach, as PSD2 requires giving a minimum of two months' notice of the termination of a framework notice, and only if the right to do so is agreed in the contract.[971]

Risk of inadequate transaction receipts/ confirmations

Receipts for an e-money transaction may not be provided or may be incomplete. This will be a concern for any consumer who wants to keep track of the full details of their transactions and the associated fees (for example, so as to manage records of a small business or a household budget record). Receipts are also an important means of checking for fraudulent and mistaken transactions. All these issues are especially important for e-money transactions that are conducted electronically without a paper trail in situations where there is not necessarily easy access to the provider of the service. The Better Than Cash Alliance provides as an example of enhancing product transparency the client receiving proof of each transaction and also having access to clear and simple transaction and account records.[972]

Regulatory approaches

The most obvious regulatory approach is obliging providers to issue transaction receipts. For example, Kenya's National Payment System Regulations require the payment service provider "without undue delay" to provide the payer with a unique transaction reference and detail of the amount, payee and their account, and the debit. The payee is also required to be given advice about the crediting of the relevant amount.[973] The European Union's PSD2 also has detailed requirements for transaction information to be provided to both the payer and the payee in an individual payment transaction. A payer may also request information about the maximum execution time and any charges before a specific transaction is completed.[974]

Another option is requiring that transaction information be available to the user, without necessarily mandating the provision of receipts. For example, Bank Indonesia's Regulation on Consumer Protection in Payments System, in general terms, requires a provider to provide facilities "to allow Consumers to obtain information." China's Measures for the Administration of Online Payment Business

of Non-Bank Payment Institutions also include an obligation to provide a free enquiry service about transactions for a year.[975] Malawi's Payment Systems (E-Money) Regulations also require extensive transaction information to be maintained and to be available to the user.[976]

Risk of inadequate periodic statements/updates

Consumers may be unable to keep track of their e-money transactions and accounts if they are not provided with periodic statements of account or equivalent information.[977] It may be the case that these statements are not provided or only "mini-statements" are made available for e-money accounts. In either case, consumers will run the risk of not seeing mistaken/unauthorized transactions or misunderstanding account balances and debits and credits. Further, the lack of complete periodic statements may be a problem if the consumer has only a limited time in which to notify the provider of concerns about the transaction. However, there are likely to be challenges in providing periodic statements where e-money services are provided through USSD devices and consumers do not have formal postal addresses. As with other risks, these risks are likely to be exacerbated in the fintech era as the use of e-money grows.

Regulatory approaches

The strongest regulatory approach is to impose a requirement to provide periodic statements, while a potentially less effective approach is making them available on request. The Australian ePayments Code reflects the former approach by requiring periodic statements every six months. However, these requirements do not apply to low-value facilities (with balances of no more than A$500). For such facilities, providers must give users a process to check the balance of the account as well as either a receipt or a mechanism to check transaction history.[978]

Some jurisdictions require enabling the consumer to access details of their transactions or to be given information about how to do so. For example, in Ethiopia at least the last 10 transactions must be online.[979] Eswatini makes provision for statements on previous transactions to be provided on request (without any limit on the number).[980] Afghanistan requires that customers be advised as to how they can learn their current e-money balance and obtain a list of recent transactions.[981]

c) Inability to retain information

Risks to consumers

A consumer may be provided with all/some of the information they need to make informed decisions about an e-money account, but the information may not be provided in a form that can be retained for future reference.[982] Retention of this information is important as a reference for consumer understanding of their rights and obligations, and as evidence in the case of a complaint or dispute. This risk is compounded when information is provided via USSD on feature phones with small screens or is available only on a website that may not retain the version of the information originally given to the consumer.

Regulatory approaches

The most direct approach is to require, in effect, that the information be in a form that the customer can access and keep for future reference. For example, the European Union's PSD2 requires that information be provided on paper or in a "durable medium," which in turn is defined as (in summary) an instrument that allows the user to store information in a way that makes it accessible for future reference.[983] Malaysia's Guideline on Electronic Money also requires that T&C be "easily accessible" (as well as understood).[984]

d) Disclosure format risks in a digital context

Chapter 4 discussed, in the context of digital microcredit, other factors in a digital context that can harm the provision of information or that may require adaptation from a paper environment to ensure its effectiveness. Equivalent issues are relevant to the presentation and delivery of information in connection with e-money.

e) Misleading marketing

Risks to consumers

As is the case in relation to digital microcredit, discussed in chapter 4, misleading marketing practices have been detected in connection with e-money that could have significant impact, particularly on vulnerable users of such products. Providers may fail to disclose or may be misleading about key product features, transaction fees, minimum balances, or monetary limitations on usage.[985] The FCA, for example, expressed concerns about misleading advertisements by e-money issuers and other payment service providers that allege that their services are "free," even though fees are charged by intermediary service providers, and about providers that advertise themselves as offering "bank" accounts or imply that they are a bank.[986] Another FCA concern was that customers were being misled by comparative cost claims; the FCA has noted that, as a result, customers may miss out on services that are better suited to their needs "with better quality, prices or overall value."[987]

These risks are likely to be exacerbated in a digital financial inclusion context. In that environment, consumers are more likely to have low levels of financial or technological capability. They are thus likely to be especially vulnerable if they are presented with a misleading offer of digital e-money services, especially in an environment where there is no opportunity to ask questions, seek advice, or make comparisons.

Regulatory approaches

Some jurisdictions prohibit misleading marketing specifically in relation to e-money accounts. The Payment Systems and Services Act in Ghana requires that marketing by e-money issuers and payment service providers "follows the general principles of honesty and transparency").[988] There are prohibitions against misleading and deceptive conduct also in Kenya's National Payment System Regulations and Malaysia's Financial Services Act.[989] However, such provisions are not commonly included in e-money regulatory frameworks, perhaps because general requirements are in place.[990]

There may also be requirements to disclose the provider's details in advertising or sales materials as well as in T&C, to assist consumers with recourse if they are harmed by these materials. For example, Ghana's Payment Systems and Services Act requires the inclusion of the provider's address, telephone number, and e-mail address in all marketing material. The FCA's Payments and E-Money Standards also require that all communications sent to an e-money customer include the name of the provider. This approach minimizes the risk that a consumer might be unaware of who the provider is, especially where e-money products are marketed under a brand name (for example, "M-Pesa") or that of a third party under a white-labelling arrangement.

Other specific requirements may relate to communications sent to e-money customers. For example, the FCA's Payments and E-Money Standards require that communications be accurate and, in particular, that they not emphasize the potential benefits of a service without a "fair and prominent indication of any relevant risks." There are also requirements that the communications be likely to be understood by the average member of the target group and that they not "disguise, diminish or obscure important information, statements or warnings."[991]

7.10 UNSUITABLE E-MONEY PRODUCTS

a) Risks to consumers

The risk that particular e-money products may not be designed to be suitable for the consumer segments they are marketed to can be heightened in markets where new providers are involved and products are increasingly used by, and aggressively marketed to, previously unserved or underserved consumers. Suitability issues can include the degree of acceptance of e-money by merchants, utility providers, government agencies, and other consumers; the availability of payment points (for example, agents, branches, third parties, and ATMs); transaction fees and limits; the extent to which the product is interoperable; and, importantly, whether the product meets the needs of specific target groups (such as women, youth, farmers, or savings groups). Further, the COVID-19 pandemic may be compounding these risks, as cash transfers, remittances, and other forms of income support (as well as emergency credit) are being made available through digital payments accounts such as e-money. In such cases, consumers may feel that they have no choice but to accept the product, even if it is not entirely suitable for their needs.

Calls have been increasing for some time for digital financial services products (including payments products such as e-money) to be proactively designed to meet consumer needs. For example, the 2016 *G20 High-Level Principles for Digital Financial Inclusion* also describe consumer-centric approaches to product design that focus on customer needs, preferences, and behaviors as examples of action to promote digital financial inclusion.[992]

b) Regulatory approaches

Product design and distribution requirements

As discussed in previous chapters, there is an emerging regulatory trend of requiring FSPs to design and distribute products to meet the needs and capabilities of users in their target market. Common elements of such regimes are discussed in chapter 3. Some jurisdictions have applied, or are in the process of extending, such requirements to payments products.[993]

Product suitability requirements

Some regulatory frameworks also require that there be consideration of the financial objectives, financial situation, or needs (or similar concepts) of a specific consumer before providing a financial service, particularly where personal recommendations or advice are being provided. These requirements are in addition to any product design rules. The statement of advice and general advice rules in Australia's Corporations Act provide an example of such requirements. These requirements apply to a wide range of financial products and services, which could include non-cash payments products such as e-money.[994]

NOTES

789 "Diversification of the Financial Services Ecosystem" in GSMA, *State of the Industry Report on Mobile Money 2018*.
790 World Bank Group, *Global Findex Database 2017*, chapter 2.
791 World Bank Group, *Global Findex Database 2017*, chapter 4.
792 "The Evolution of the Digital Ecosystem" in GSMA, *State of the Industry Report on Mobile Money 2019*.
793 "Regulatory Developments in 2019" in GSMA, *State of the Industry Report on Mobile Money 2019*.
794 GSMA, *State of the Industry Report on Mobile Money 2019*, 29.
795 GPFI, *Report on Advancing Women's Digital Financial Inclusion*, s. 4.1.
796 See, for example, IMF, "Digital Financial Services and the Pandemic." See also Jurd De Girancourt et al., "How the COVID-19 Crisis May Affect Electronic Payments."
797 See, for example, the definitions of *e-money* and *mobile money* in Ehrentraud et al., *Policy Responses to FinTech*, 26, para 43, and 53; Adrian and Mancini-Griffoli, *Rise of Digital Money*, 4; and Financial Action Task Force, *Virtual Currencies* (see the description of *e-money* in the definition of *virtual currency* on page 4). A few examples of the various regulatory frameworks that define *e-money* or *electronic money* are the broad definition in the EU Directive on Electronic Money Institutions 2009, art. 2; Ghana's Payment Systems and Services Act 2019, s. 102, which refers to e-money being redeemable for cash as well as being accepted by a person; Indonesia's E-Money Regulation 2018, art. 1(3), which states that one of the elements of electronic money is that the value deposited by a holder is "not savings as referred to in the law concerning banking"; and Singapore's Payment Services Act 2019, s. 2—this definition unusually refers to the underlying value being "pegged" to a currency.
798 GSMA, "Mobile Money Glossary."
799 World Bank Group, *Good Practices*, annex A, s. A1.
800 Basel Committee on Banking Supervision, "Guidance on Application of Core Principles" (Principle 4).
801 Directive 2009/110 on Electronic Money Institutions 2009 (EU).
802 Directive 2009/110 on Electronic Money Institutions 2009 (EU), art. 10.
803 Payment Systems and Services Act 2019 (Ghana), s. 21 and related definitions in s. 102.
804 Financial Services Act 2013 (Malaysia), s. 8 (1) and Division 1 of Part 1 of Schedule 1.
805 BNM Financial Services (Designated Payment Instruments) Order (2013), s. 2(d).
806 Corporations Act 2001 (Cth), Chapter 7 and the ePayments Code 2016 (Australia).
807 BI Regulation on Consumer Protection in Payments System 2014 (Indonesia).
808 BI Regulation on Consumer Protection in Payments System 2014 (Indonesia), art. 2.
809 Payment Systems and Services Act 2019 (Ghana), s. 102.
810 CBN Consumer Protection Framework 2016 (Nigeria), s. 1.2.
811 Buku and Mazer, "Fraud in Mobile Financial Services," 2. See also ITU-T Focus Group on Digital Financial Services, *Commonly Identified Consumer Protection Themes,* s. 3.3.
812 Morawczynski, "Fraud in Uganda."
813 Buku, "Innovation in Mobile Money."
814 World Bank Group, *Good Practices*, annex A, ss. C4 and C6.
815 "Growing and Globalising" in GSMA, *State of the Industry Report on Mobile Money 2019*.
816 IMF, "Digital Financial Services and the Pandemic."
817 ITU-T Focus Group on Digital Financial Services, *Commonly Identified Consumer Protection Themes*.
818 Committee on Payments and Market Infrastructures and World Bank Group, *Payment Aspects of Financial Inclusion*, s. 4.3.2 and Guideline 3.
819 See, for example, Kyamutetera, "Hackers Break Into Mobile Money System." See also Stanbic Bank Uganda, MTN Uganda, and Airtel Uganda, "System Incident Impacting Bank."
820 The Contingent Reimbursement Model Code for Authorised Push Payments Scams 2019 (UK).
821 EU Directive 2009/110 on Electronic Money Institutions 2009, art. 4. See also PSD2, art. 5.
822 BNM Guideline on E-Money 2016 (Malaysia), s. 7.1.1.
823 Staschen, "Basic Regulatory Enablers," Box 4.
824 Payment Systems (E-Money) Regulations 2019 (Malawi), r. 22.
825 National Payment System Regulations 2014 (Kenya), s. 16(2)(g).
826 Use of Agents Directive 2020 (Ethiopia), art. 17(6) and Part VII.
827 National Payment System Regulations 2014 (Kenya), art. 20.
828 Use of Agents Directive 2020 (Ethiopia), art. 6.
829 Payment Systems and Services Act 2019 (Ghana), ss. 87 and 88.
830 Use of Agents Directive 2020 (Ethiopia), art. 9 and annex II.
831 Electronic Money Institutions Regulation 2016 (Afghanistan), r. 14(f).
832 National Payment System Regulations 2014 (Kenya), r. 17.
833 Payment Services Act 2019 (Singapore), s. 18 (prohibits a licensee providing payment services through an agent unless the agent is licensed).
834 BNM Guideline on E-Money 2016 (Malaysia), s. 7.1.3.
835 National Payment System Regulations 2014 (Kenya), r. 24.
836 PSD2, art. 97.

837 PSD2, art. 4.
838 People's Bank of China Measures for the Administration of Online Payment Business of Non-Bank Payment Institutions 2016 (China), art. 22–24.
839 PSD2, art. 73 and 74.
840 PSD2, art. 71. (The relevant period is 13 months.)
841 ePayments Code 2016 (Australia), clauses 11 and 12.
842 National Payment System Regulations 2014 (Kenya), r. 28(5).
843 PSD2, art. 51(5), 69 and 70.
844 Regulation on Electronic Fund Transfers 2016 (Afghanistan), art. 6(6).
845 PSD2, art. 72(1).
846 Payment Systems and Services Act 2019 (Ghana), art. 20(2).
847 World Bank Group, *Good Practices*, annex A, s. C6(a).
848 "Growing and Globalising" in GSMA, *State of the Industry Report on Mobile Money 2019*.
849 The World Bank Group's G*lobal Financial Inclusion and Consumer Protection Survey* found that more than 75 percent of responding jurisdictions that permitted agent relationships had rules in place to hold a financial institution liable for its agents' actions or omissions. See also Kerse et al., *Technical Note on the Use of Agents*.
850 National Payment System Regulations 2014 (Kenya), rr. 14(4) and (5).
851 BI Regulation on Consumer Protection in Payments System 2014 (Indonesia), s. 10.
852 Payment Systems and Services Act 2019 (Ghana), s. 86(1).
853 Use of Agents Directive 2020 (Ethiopia), art. 6(1).
854 Payment Systems (E-Money) Regulations 2019 (Malawi), s. 21 (3)(f).
855 Payment Systems and Services Act 2019 (Ghana), s. 91 (2)(b).
856 Regulation of Mobile and Agent Banking Services Directives 2012 (Ethiopia), art. 9.2.7.
857 Regulation of Mobile and Agent Banking Services Directives 2012 (Ethiopia), art. 13(1).
858 PSD2, art. 96(1).
859 ePayments Code (Australia), clauses 12 and 13.
860 PSD2, art. 55(5).
861 BNM Guideline on E-Money 2016 (Malaysia), s. 9.2.
862 G20, *G20 High-Level Principles for Digital Financial Inclusion*, Principle 4.
863 Committee on Payments and Market Infrastructures and World Bank Group, *Payment Aspects of Financial Inclusion in the Fintech Era*, Guiding Principle 3.
864 Executive summary and "A Step towards a Digital Future for All" in GSMA, *State of the Industry Report on Mobile Money 2019*. As noted above, other 2019 statistics from the GSMA report include 371 million active accounts (up 13.6 percent), 37.1 billion transaction volume (up 21.8 percent), and $690.1 billion in transaction value (up 26 percent). The GSMA estimates transaction value will be $1 trillion by 2023.
865 Safaricom, "Update on April 24th Network Outage."
866 allAfrica, "Kenya to Investigate Mobile Operator's M-Pesa Outage."
867 Zimmerman and Baur, "Understanding How Consumer Risks."
868 Payment Systems and Services Act 2019 (Ghana), arts. 20 and 15, respectively.
869 Payment Systems (E-Money) Regulations 2019 (Malawi), r. 5(2).
870 Payment Systems (E-Money) Regulations 2019 (Malawi), r. 15.
871 PSD2 applies to e-money institutions, as well as other payment service providers (see Article 1). However, a separate directive, Directive 2009/110 on Electronic Money Institutions 2009, covers the "taking up, pursuit and prudential supervision of the business of electronic money institutions."
872 PSD2, art. 95.
873 National Payment System Regulations 2014 (Kenya), r. 27(2).
874 E-Money Regulations 9 (Malawi), rr. 14–17 .
875 Payment Systems and Services Act 2019 (Ghana), s. 45(1) (i).
876 Regulation on Electronic Fund Transfers (Afghanistan), art. 14(2) and (3).
877 Measures for the Administration of Online Payment Services 2016 (China), art. 31.
878 PSD2, art. 96.
879 Payment Systems and Services Act 2019 (Ghana), s. 45(2).
880 Licensing and Authorization of Payment Instrument Issuers Directive No. ONPS/01/2020 (Ethiopia), art. 12(2) and 13.2.
881 Regulation on Electronic Fund Transfers (Afghanistan), art. 14 (1).
882 Payment Systems and Services Act 2019 (Ghana), ss. 57–62.
883 PSD2, art. 89(1).
884 PSD2, art. 84, 89, and 93.
885 ePayments Code 2016 (Australia), clauses 14.
886 See, for example, G20, *G20 High-Level Principles for Digital Financial Inclusion*, Principles 2 and 5; Better Than Cash Alliance, *Responsible Digital Payments Guidelines*, Guideline 2.
887 Mobile Money Service Providers Practice Note 2019 (Eswatini), art. 22.4.
888 Payment Systems (E-Money) Regulations 2019 (Malawi), r. 17(3).
889 DAB Electronic Money Institutions Regulation 2016 (Afghanistan), r. 14(e)(2).
890 PSD2, art. 72.
891 PSD2, art. 88.

892 ePayments Code 2016 (Australia), Chapter E.
893 Chen, Fiorillo, and Hanouch, "Smartphones & Mobile Money."
894 Committee on Payments and Market Infrastructures and World Bank Group, *Payment Aspects of Financial Inclusion*, s. 3.1.2.3; Committee on Payments and Market Infrastructures and World Bank Group, *Payment Aspects of Financial Inclusion in the Fintech Era*, s. 4.2.4.
895 Adrian and Mancini-Griffoli, *Rise of Digital Money*, 4 and following.
896 EU Directive 2009/110 on Electronic Money Institutions 2009, Recital para 13 and art. 6(3).
897 GSMA, *Safeguarding Mobile Money*, 5.
898 World Bank Group, *Prudential Regulatory and Supervisory Practices* (see "Approaches to Supervision").
899 See Kerse and Staschen, *Safeguarding Rules for Customer Funds*.
900 Payment Systems (E-Money) Regulations 2019 (Malawi), Part IV.
901 PSD2, art. 10, and see also EU Directive 2009/110 on Electronic Money Institutions 2009, art. 7.
902 BI Regulation on E-Money 2018 (Indonesia), art. 48.
903 Payments Systems (Electronic Money) Regulations, 2015 (Tanzania), Part V.
904 National Payment System Regulations 2014 (Kenya), r. 25(3) and Fourth Schedule.
905 Payment Systems (E-Money) Regulations 2019 (Malawi), r. 7(7). More generally, for examples of spreading e-float funds across multiple banks and other fund safeguarding measures see Kerse and Staschen, *Safeguarding Rules for Customer Funds* and GSMA, *Safeguarding Mobile Money*.
906 Directive 2009/110 on Electronic Money Institutions 2009 (EU).
907 Payment Systems and Services Act 2019 (Ghana), s. 31.
908 Payment Systems (E-Money) Regulations 2019 (Malawi), r. 5(4).
909 Financial Services Act (Malaysia), s. 14(2).
910 Payment Services Act 2019 (Singapore), s. 20.
911 Payment Systems (E-Money) Regulations 2019 (Malawi),r. 5(5).
912 BI Regulation on E-Money, 2018 (Indonesia), art. 17(2).
913 Basel Committee on Banking Supervision, "Guidance on Application of Core Principles" (Principles 1 and 4).
914 BSP E-Money Circular 2009 (Philippines), s. 5(B).
915 National Payment System Regulations 2014 (Kenya), r. 25(2).
916 BNM Guideline on E-Money 2016 (Malaysia), s. 10.1.
917 Payment Systems (E-Money) Regulations 2019 (Malawi), r. 21(3).
918 BNM Guideline on Electronic Money (Malaysia), ss. 4, 5, and 14.2.
919 World Bank Group, *Prudential Regulatory and Supervisory Practices* (see especially table 4).
920 Izaguirre et al., *Deposit Insurance Treatment of Money*.
921 Izaguirre et al., *Deposit Insurance Treatment of Money*.
922 World Bank Group, *Prudential Regulatory and Supervisory Practices* (see "Approaches to Safety Nets").
923 Committee on Payments and Market Infrastructures and World Bank Group, *Payment Aspects of Financial Inclusion*, s. 4.2.4 and Guideline 2.
924 Payment Systems and Services Act 2019 (Ghana), s. 46.
925 DAB Electronic Money Institutions Regulation 2016 (Afghanistan), r. 14.
926 BSP E-Money Circular 2009 (Philippines), ss. 2(2), 4(C), and 4(G).
927 Measures for the Administration of Online Payment Services by Non-Bank Payment Institutions 2016 (China), art. 7.
928 See Consumer Financial Protection Bureau. 2016. Final Rule on Prepaid Accounts under the Electronic Fund Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z) (USA).
929 Electronic Fund Transfer (Regulation E) 12 CFR Part 1005 (USA), para. 1005.18(b)(2)(xi).
930 Reserve Bank of Zimbabwe, "Cash-In, Cash-Out and Cash-Back Facilities."
931 Electronic Money Institution's Regulation 2016 (Afghanistan), art. 14(b).
932 Directive 2009/110 on Electronic Money Institutions 2009 (EU), art. 11.
933 Payment Systems and Services Act 2019 (Ghana), s. 29.
934 National Payment System Regulations 2014 (Kenya), r. 44(1).
935 Payment Systems (E-Money) Regulations 2019 (Malawi), r. 5(10).
936 BSP E-Money Circular 2009 (Philippines), s. 4C.
937 Payment Systems (E-Money) Regulations 2019 (Malawi), r. 5(5).
938 Payment Services Act 2019 (Singapore), s. 19.
939 Numerous international standards highlight this risk. See, for example, World Bank Group, *Good Practices*, annex A, ss. B3, B4, and B7; Committee on Payments and Market Infrastructures and World Bank Group, *Payment Aspects of Financial Inclusion in the Fintech Era*, Principle 5 ("Establish Responsible Digital Financial Practices to Protect Consumers"); Better Than Cash Alliance, *Responsible Digital Payments Guidelines,* Principle 3. See also Staschen, "Basic Regulatory Enablers."
940 Mazer and Rowan, "Competition in Mobile Financial Services."
941 Payment Systems (E-Money) Regulations 2019 (Malawi), r. 24(1).
942 Payment Systems and Services Act 2019 (Ghana), s. 44(b), and see also s. 45(6) regarding marketing materials.
943 BI Regulation on E-Money 2018 (Indonesia), art. 43, and BI Consumer Protection in Payment Service Regulation 2014 (Indonesia), art 3 and 11.
944 Financial Services Act 2013 (Malaysia), s. 124 (1) and Schedule 7, and Malaysia E Money Guideline 2008 (Malaysia), ss. 9.2(i) and 9.3.

945 Consumer Protection Framework 2016 (Nigeria), s. 2.3.
946 PSD2, art. 52.
947 ePayments Code.
948 Licensing and Authorization of Payment Instrument Issuers Directive No. ONPS/01/2020 (Ethiopia), art. 12(2).
949 BI Consumer Protection in Payment Service Regulation 2014 (Indonesia), art. 11.
950 National Payment System Regulations 2014 (Kenya), r. 35(1).
951 Consumer Protection Framework 2016 (Nigeria), s. 2.3.1.
952 Mobile Money Service Providers Practice Note 2019 (Eswatini), s. 22.1.
953 PSD2, arts. 51 and 52.
954 National Payment System Regulations 2014 (Kenya), r. 35 (1).
955 Payment Systems (E-Money) Regulations 2019 (Malawi), r. 24(2).
956 BNM Guideline on Electronic Money 2008 (Malaysia), s. 9.3.
957 Consumer Protection Framework 2016 (Nigeria), s. 2.3.1.
958 United Kingdom Payment Account Regulations: Final Linked Services List 2018, and EBA, *Final Report on Standardized Terminology*.
959 Mazer, "Kenya's Rules on Mobile Money Price Transparency Awareness."
960 National Payment System Regulations 2014 (Kenya), r. 35(1)(b).
961 BNM Guideline on Electronic Money 2016 (Malaysia), s. 9(3)(i).
962 National Payment System Regulations 2014 (Kenya), rr. 41(1)(a) and (2).
963 People's Bank of China Measures for the Administration of Online Payment Business of Non-Bank Payment Institutions 2016 (China), art. 7.
964 Payment Systems and Services Act 2019 (Ghana), ss. 453) and (4).
965 BI Regulation Concerning E-Money 2018 (Indonesia), art. 9.3.
966 BSP E-Money Circular 2009 (Philippines), s. 4(G).
967 Bold and Pillai, "The Impact of Shutting Down Mobile Money in Uganda."
968 ePayments Code 2016 (Australia), clauses 4 .11–4.17 and 21.
969 PSD2, art. 52.
970 Payment Systems and Services Act 2019 (Ghana), s. 45(9).
971 PSD2, art. 55(3).
972 Better Than Cash Alliance, *Responsible Digital Payments Guidelines*, Guideline 3.
973 National Payment System Regulations 2014 (Kenya), r. 35.
974 PSD2, art. 57 and 58.
975 People's Bank of China Measures for the Administration of Online Payment Business of Non-Bank Payment Institutions 2016 (China), art. 28.
976 Payment Systems (E-Money) Regulations 2019 (Malawi), r. 17(4).
977 World Bank Group, *Good Practices*, annex A, s. B6.
978 ePayments Code 2016 (Australia), clauses 5.8 and 7.1–7.7
979 Regulation of Mobile and Agent Banking Services Directives 2012 (Ethiopia), art. 12.8.
980 Mobile Money Service Providers Practice Note 2019 (Eswatini), s. 22.4(g).
981 Electronic Money Institution's Regulation 2016 (Afghanistan), r. 14(e)(2).
982 World Bank Group, *Good Practices*, annex A, B1(c), and Better Than Cash Alliance, *Responsible Digital Payments Guidelines*, Principle 3.
983 PSD2, art. 51, and, in art. 4, the definition of a *durable medium*.
984 BNM Guideline on E-Money 2016 (Malaysia), s. 9.1.
985 World Bank Group, *Good Practices*, annex A, s. B2.
986 FCA, *General Standards and Communication Rules*, para 3.34–3.39.
987 FCA, *General Standards and Communication Rules*, para 3.18–3.24.
988 Payment Systems and Services Act 2019 (Ghana), s. 45(6)(a).
989 National Payment System Regulations 2014 (Kenya), r. 37, requires that advertisements be precise and clearly understood, not misleading, and comprehensive enough to inform customers properly of the main features and conditions. Further, the Financial Services Act (Malaysia) prohibits engaging in misleading and deceptive conduct in relation to the "nature, features, terms or price" of financial products and services.
990 For example, the commentary on the PSD2 notes that consumers should continue to be protected against unfair and misleading practices by other specified directives (such as 2005/29/EC, relating to unfair business to consumer practices, and 2011/83/EU, relating to consumer rights).
991 FCA, *General Standards and Communication Rules*, s. 2.3.1A of Annex C—Amendments to the Banking: Conduct of Business Sourcebook.
992 G20, *G20 High-Level Principles for Digital Financial Inclusion*, Principle 1.
993 See Boeddu and Grady, *Product Design and Distribution*.
994 Corporations Act 2001 (Cth) (Australia), Part 7.7.

REFERENCES

Legislation, Binding Rules, and Regulatory Guidance

Afghanistan. Electronic Money Institutions Regulation. 2016.

Afghanistan. Regulation on Electronic Fund Transfers. 2016.

Australia. ASIC Corporations (Product Intervention Order – Short Term Credit) Instrument 2019/917. 2019.

Australia. Corporations Act (Cth). 2001.

Australia. Corporations Amendment (Crowd-sourced Funding) Act (Cth). 2017.

Australia. Corporations Amendment (Design and Distribution Obligations) Regulations (Cth). 2019.

Australia. Corporations Regulations (Cth). 2001.

Australia. ePayments Code. 2016.

Australia. Explanatory Memoranda, A Corporations Amendment (Crowd-sourced Funding for Proprietary Companies) Bill 2017.

Australia. National Consumer Credit Protection Act (Cth). 2009.

Belgium. Consumer Credit Act. 1991.

Brazil. National Monetary Council Resolution Number 4,656. April 26, 2018.

Brazil. Securities and Exchange Commission Instruction No. 588, of July 13, 2017.

California (United States of America). Consumer Privacy Act. 2018.

China. Guide to the Administration of Recordation and Registration of Peer-to-Peer Lending Information Intermediaries. China Banking Regulatory Commission and other authorities, October 28, 2016.

China. Guide to the Disclosure of Information on Business Activities of Peer-to-Peer Lending Information Intermediaries. China Banking Regulatory Commission, August 23, 2016.

China. Guidelines for Online Lending Fund Depository Business. China Banking Regulatory Commission, February 22, 2017.

China. Guiding Opinions on Promoting the Healthy Development of Internet Finance. 2015.

China. Interim Measures for the Administration of the Business Activities of Online Lending Intermediary Institutions. China Banking Regulatory Commission and other authorities, August 17, 2016.

China. Peer-to-Peer Lending Information Intermediaries of Guangdong Province—Detailed Implementation Rules for Recordation and Registration (Exposure Draft). February 14, 2017.

China. People's Bank of China Measures for the Administration of Online Payment Business of Non-Bank Payment Institutions. 2016.

Dubai. Dubai Financial Services Authority Rulebook—April 2020.

Dubai. Regulatory Law No. 1 of 2004.

Eswatini. Mobile Money Service Providers Practice Note. 2019.

Ethiopia. Licensing and Authorization of Payment Issuers Directive No. ONPS/01/2020.

Ethiopia. Use of Agents Directive No. FIS/02/2020.

EU (European Union). Directive 2002/65/EC on Distance Marketing of Consumer Financial Services. 2002.

EU. Directive 2008/48 on Consumer Credit Agreements. 2008.

EU. Directive 2009/110 on Electronic Money Institutions. 2009.

EU. Directive 2011/83 on Consumer Rights. 2011.

EU. Directive 2014/65/EU on Markets in Financial Instruments. 2014.

EU. Directive 2015/2366 on Payments Services. 2015.

EU. Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). 2016.

EU. Regulation 2020/1503 on European crowdfunding service providers for business. 2020.

France. Official order No. 2014-559 of 30 May 2014 on crowdfunding. 2014.

Ghana. Payment Systems and Services Act. 2019.

Hong Kong. Hong Kong Monetary Authority Guiding Principles on Consumer Protection in Respect of Use of Big Data Analytics and Artificial Intelligence by Authorized Institutions. 2019.

India. NBFC (Non-Banking Financial Company)—Peer to Peer Lending Platform (Reserve Bank) Directions. 2017.

Indonesia. Bank Indonesia Regulation on Consumer Protection in Payments System. 2014.

Indonesia. Bank Indonesia Regulation on E-Money. 2018.

Indonesia. Financial Services Authority Circular Number 18/SEOJK.02/2017 Regarding Information Technology Risk Management and Management in Information Technology-Based Lending.

Indonesia. Regulation of the Financial Services Authority Number 77/POJK.01/2016 Concerning Information Technology-Based Loan Services.

Italy. Resolution no. 18592 of 26 June 2013.

Japan. Financial Instruments and Exchange Act No. 25. 1948.

Japan. Money Lending Business Act No. 32. May 13, 1983.

Kenya. National Payment System Regulations. 2014.

Korea (Republic of). Online Investment-Linked Finance and Protection of Users Act. 2019.

Latvia. Consumer Rights Protection Law. 1999.

Lithuania. Guidelines on Advertising Financial Services, Bank of Lithuania, 2012.

Malawi. Payment Systems (E-Money) Regulations. 2019.

Malaysia. Bank Negara Malaysia Financial Services (Designated Payment Instruments) Order. 2013.

Malaysia. Bank Negara Malaysia Guideline on Electronic Money. 2016.

Malaysia. Bank Negara Malaysia Guidelines on Recognized Markets SC-GL/6-2015 (R4-2020).

Malaysia. Financial Services Act. 2013.

Mexico. Banking and Securities Commission—General Provisions Applicable to Financial Technology Institutions. September 10, 2018, amended March 25, 2019.

Mexico. Banking and Securities Commission—General Provisions of CONDUSEF on Transparency and Sound Practices Applicable to Financial Technology Institutions. July 9, 2019.

Mexico. Financial Technology Institutions Law. 2018.

Mexico. Law on Transparency for Financial Services. 2007.

Netherlands. Consumer Credit Act. 2011.

Nigeria. Central Bank of Nigeria Consumer Protection Framework. 2016.

Paraguay. Circular SB. SG. No. 00065/2015.

Peru. Emergency Decree No. 013-2020-JUS/DGTAIPD. 2020.

Philippines. Bangko Sentral ng Pilipinas E-Money Circular. 2009.

Philippines. National Privacy Commission Circular No. 20-01 on Guidelines on the Processing of Personal Data for Loan-Related Transactions. 2020.

Portugal. Banco de Portugal Circular Letter No. CC/2020/00000044 on Best Practices Applicable to the Selling of Retail Banking Products and Services through Digital Channels.

Portugal. Notice of Banco de Portugal No. 4/2017.

Singapore. Payment Services Act. 2019.

South Africa. Department of Trade and Industry Regulations on Review of Limitations on Fees and Interest Rates. 2015.

South Africa. National Credit Act. 2005.

Tanzania. Payments Systems (Electronic Money) Regulations. 2015.

UK. The Contingent Reimbursement Model Code for Authorised Push Payments Scams. 2019.

UK. Financial Conduct Authority Client Assets Sourcebook—October 2020.

UK. Financial Conduct Authority Conduct of Business Sourcebook—October 2020.

UK. Financial Conduct Authority Consumer Credit Sourcebook—October 2020.

UK. Financial Conduct Authority Principles for Businesses—October 2020.

UK. Financial Conduct Authority Senior Management Arrangements, Systems and Controls Sourcebook—October 2020.

UK. Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (SI 2001/544).

USA. Consumer Financial Protection Bureau's Final Rule on Prepaid Accounts under the Electronic Fund Transfer Act. 2016.

USA. Electronic Fund Transfer (Regulation E) 12 CFR Part 1005.

USA. Regulation Crowdfunding, General Rules and Regulations 17 CFR Part 227.

USA. Securities Act. 1933.

USA. Truth in Lending (Regulation Z).

USA. Truth in Lending Act. 1968.

Other Sources

Adrian, T., and T. Mancini-Griffoli. *The Rise of Digital Money* (Fintech Note No. 19/001). International Monetary Fund, 2019. https://www.imf.org/en/Publications/fintech-notes/Issues/2019/07/12/The-Rise-of-Digital-Money-47097#:~:text=FinTech%20Notes&text=The%20series%20will%20carry%20work,banks%20and%20credit%20card%20companies.

AFI (Alliance for Financial Inclusion). "Digitally Delivered Credit: Consumer Protection Issues and Policy Responses to New Models of Digital Lending." AFI Global, 2017. https://www.afi-global.org/sites/default/files/publications/2017-11/AFI_CEMC_digital%20survey_AW2_digital.pdf.

AFI. "Digitally Delivered Credit: Policy Guidance Note and Results from Regulator Survey." AFI Global, 2015. https://www.afi-global.org/sites/default/files/publications/guidelinenote-17_cemc_digitally_delivered.pdf.

AFI. "Policy Framework for Responsible Digital Credit." AFI Global, 2020. https://www.afi-global.org/publications/3216/Policy-Framework-for-Responsible-Digital-Credit.

AFI. "Policy Model for E-Money." AFI Global, 2019. https://issuu.com/afi-global/docs/afi_dfs_emoney_aw_digital.

AI Now Institute. "Algorithmic Accountability Policy Toolkit." New York University, 2018.

allAfrica. "Kenya to Investigate Mobile Operator's M-Pesa Outage." allAfrica InFocus. https://allafrica.com/view/group/main/main/id/00065353.html.

ASBA (Association of Supervisors of Banks of the Americas) and IDB (Inter-American Development Bank). *Consumer Protection in the New Environment of Financial Technological Innovation: Regulatory and Supervisory Considerations*. ASBA and IDB, 2020. http://www.asbasupervision.com/en/bibl/publications-of-asba/working-groups/2378-consumer-protection-1/file.

ASBA and IDB. *Global Fintech Regulation and Supervision Practices*. ASBA and IDB, 2020. http://www.asbasupervision.com/en/bibl/publications-of-asba/working-groups/2205-global-fintech-regulation-and-supervision-practices/file.

ASIC (Australian Securities and Investments Commission). *Crowd-Sourced Funding: Guide for Companies* (Regulatory Guide 261). ASIC, June 2020. https://download.asic.gov.au/media/5702668/rg261-published-19-june-2020-20200727.pdf.

ASIC. *Facilitating Digital Financial Services Disclosures* (ASIC Regulatory Guide 221), March 2016. https://download.asic.gov.au/media/3798806/rg221-published-24-march-2016.pdf.

ASIC. *Marketplace Lending (Peer-to-Peer Lending) Products* (Information Sheet 213). ASIC, 2016. https://asic.gov.au/regulatory-resources/financial-services/marketplace-lending/marketplace-lending-peer-to-peer-lending-products/.

ASIC. *Survey of Marketplace Lending Providers* (Report 526). ASIC, 2017, para 17–18. https://download.asic.gov.au/media/4276660/rep-526-published-1-june-2017.pdf.

ASIC. *Survey of Marketplace Lending Providers: 2016–2017* (Report 559). ASIC, 2017, para 45–46. https://download.asic.gov.au/media/4573524/rep559-published-14-december-2017.pdf.

ASIC. *Survey of Marketplace Lending Providers: 2017–2018* (Report 617). ASIC, 2019. https://download.asic.gov.au/media/5074452/rep617-published-12-april-2019.pdf.

Australian Competition and Consumer Commission. *Guidelines for Developing Effective Voluntary Industry Codes of Conduct*. 2011. https://www.accc.gov.au/system/files/Guidelines%20for%20developing%20effective%20voluntary%20industry%20codes%20of%20conduct.pdf.

Bae. H. "S. Korea to Place Investment Cap on Peer-to-Peer Lending" *The Korea Herald*, March 30, 2020. http://www.koreaherald.com/view.php?ud=20200330000800#.

Balyuk, T. "Financial Innovation and Borrowers: Evidence from Peer-to-Peer Lending" (Rotman School of Management Working Paper No. 2802220). 2019. https://ssrn.com/abstract=2802220.

Basel Committee on Banking Supervision. "Guidance on the Application of the Core Principles for Effective Banking Supervision to the Regulation and Supervision of Institutions Relevant to Financial Inclusion." Bank for International Settlements, 2016. https://www.bis.org/bcbs/publ/d383.pdf.

Berg, T., V. Burg, A. Gombovi, and M. Puri. "On the Rise of FinTechs—Credit Scoring Using Digital Footprints." *The Review of Financial Studies* 33, no. 7 (July 2020), 2845–97.

Better Than Cash Alliance. *Responsible Digital Payments Guidelines*. Better Than Cash Alliance, 2016. https://btca-prod.s3.amazonaws.com/documents/212/english_attachments/DigitalGuidelines-withMemo-MECH-Update1d.pdf?1504714863.

BFA Global. "Dipstick Surveys: The Financial Impact of Covid-19 on Low-Income Populations." BFA Global, 2020. https://bfaglobal.com/our-work/covid-19-impact/.

Blechman, J. "Mobile Credit in Kenya and Tanzania: Emerging Regulatory Challenges in Consumer Protection, Credit Reporting and Use of Customer Transactional Data." *African Journal of Information and Communication*, no. 17, 2016. http://www.macmillankeck.pro/media/pdf/AJIC_Issue_17_2016_Blechman.pdf.

Boeddu, G., and R. Grady. *Product Design and Distribution: Emerging Regulatory Approaches for Retail Banking Products* (Discussion Note). World Bank Group, 2019. http://documents1.worldbank.org/curated/en/993431567620025068/pdf/Product-Design-and-Distribution-Emerging-Regulatory-Approaches-for-Retail-Banking-Products-Discussion-Note.pdf.

Bold, C., and R. Pillai. 2016. "The Impact of Shutting Down Mobile Money in Uganda." *CGAP Blog*, March 7, 2016. https://www.cgap.org/blog/impact-shutting-down-mobile-money-uganda.

Buku, M. "Innovation in Mobile Money: What Are the Risks?" *CGAP Blog*, May 25, 2017.

Buku, M., and R. Mazer. "Fraud in Mobile Financial Services: Protecting Consumers, Providers, and the System." *CGAP Brief*, April 2017. https://www.cgap.org/sites/default/files/Brief-Fraud-in-Mobile-Financial-Services-April-2017.pdf.

Busara Center for Behavioral Economics. *Pricing Transparency, Switching Costs, and Accountability. Final Report: Experimental Results and Analysis*. 2017.

Caplan, R., J. Donovan, L. Hanson, and J. Matthews. *Algorithmic Accountability: A Primer*. Data & Society, 2018. https://datasociety.net/library/algorithmic-accountability-a-primer/.

CCAF (Cambridge Centre for Alternative Finance). *The Global Alternative Finance Market Benchmarking Report*. CCAF, 2020. https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/the-global-alternative-finance-market-benchmarking-report/.

CCAF. *The Third Asia Pacific Region Alternative Finance Industry Report*. CCAF, 2018. https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-3rd-asia-pacific-alternative-finance-industry-report.pdf.

Central Bank of Ireland. *Consumer Notice on Crowdfunding, Including Peer-to-Peer Lending*. Information Notice, June 2014.

Central Bank of Kenya. *The 2016 FinAccess Household Survey on Financial Inclusion*. Kenya National Bureau of Statistics and FSD Kenya, 2016. https://s3-eu-central-1.amazonaws.com/fsd-circle/wp-content/uploads/2016/02/30093031/The-2016-FinAccess-household-survey-report4.pdf.

CGTN Africa. "Google Fails to Stamp Out Short-Term Payday Lending Apps." CGTN Africa, January 24, 2020. https://africa.cgtn.com/2020/01/24/google-fails-to-stamp-out-short-term-payday-lending-apps/.

Chen, G., A. Fiorillo, and M. Hanouch. "Smartphones & Mobile Money: Principles for UI/UX Design (1.0)" (slide deck). Consultative Group to Assist the Poor, October 2016. https://www.cgap.org/sites/default/files/publications/slidedeck/principlesofsmartphonedesign05oct16-161005230428.pdf.

Committee of Advertising Practice (UK). "Trivialisation in Short-Term High-Cost Credit Advertisements" (Advertising Guidance). June 2015. https://www.asa.org.uk/asset/3EE84177-B1BE-4E77-9292EA4F7CD5091E.FFBC27CC-F120-4877-BD230015141DE7CE/.

Committee on the Global Financial System and Financial Stability Board Working Group. *FinTech Credit: Market Structure, Business Models and Financial Stability Implications*. Financial Stability Board and Committee on the Global Financial System, May 22, 2017. https://www.bis.org/publ/cgfs_fsb1.pdf.

Committee on Payments and Market Infrastructures and World Bank Group. *Payment Aspects of Financial Inclusion*. Bank for International Settlements, 2016. https://www.bis.org/cpmi/publ/d144.htm.

Committee on Payments and Market Infrastructures and World Bank Group. *Payment Aspects of Financial Inclusion in the Fintech Era*. Bank for International Settlements, 2020. https://www.bis.org/cpmi/publ/d191.htm.

Cornelli, G., J. Frost, L. Gambacorta, R. Rau, R. Wardrop, and T. Ziegler. *Fintech and Big Tech Credit: A New Database* (Working Paper No. 887). Bank for International Settlements, 2020. https://www.bis.org/publ/work887.htm.

Davis, K., and J. Murphy. "Peer-to-Peer Lending: Structures, Risks and Regulation." *JASSA The Finsia Journal of Applied Finance*, no. 3 (2016), 37–44. https://www.finsia.com/docs/default-source/jassa-new/JASSA-2016-/jassa-2016-issue-3/jassa-2016-iss-3-complete-issue.pdf.

Deng, C., and X. Yu. "China's Once-Hot Peer-to-Peer Lending Business Is Withering." *Wall Street Journal*, February 2, 2020. https://www.wsj.com/articles/chinas-once-hot-peer-to-peer-lending-business-is-withering-11580644804.

Dentons. "SEC Adopts Final Rules for Securities Crowdfunding under Title III of the JOBS Act." Dentons, December 2015. https://www.dentons.com/en/~/media/7ee86097b5ad4e47a7469ea3cb554e87.ashx.

Duoguang, B. "Growing with Pain: Digital Financial Inclusion in China." Chinese Academy of Financial Inclusion, 2018. http://www.cafi.org.cn/upload/file/20190121/1548034976707794.pdf.

EBA (European Banking Authority). *Final Report on Guidelines on Loan Origination and Monitoring* (EBA/GL/2020/06). EBA, 2020. https://eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/Guidelines%20on%20loan%20origination%20and%20monitoring/884283/EBA%20GL%202020%2006%20Final%20Report%20on%20GL%20on%20loan%20origination%20and%20monitoring.pdf.

EBA. *Final Report on Standardized Terminology, Fee Information Documents and Statement of Fees for Common Services Linked to Payments Accounts.* EBA, 2017.

EBA. "Opinion of the European Banking Authority on Lending-Based Crowdfunding" (EBA/Op/2015/03). EBA, February 26, 2015. https://eba.europa.eu/documents/10180/983359/EBA-Op-2015-03+%28EBA+Opinion+on+lending+based+Crowdfunding%29.pdf.

EBA. *Second EBA Report on the Application of the Guidelines on Product Oversight and Governance (POG) Arrangements (EBA/GL/2015/18)* (EBA/REP/2020/28). EBA, 2020. https://eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2020/935640/Second%20EBA%20report%20on%20the%20application%20of%20the%20POG%20guidelines%20arrangements.pdf.

EC (European Commission). *Behavioral Study on the Digitalisation of the Marketing and Distance Selling of Retail Financial Services.* EC, April 2019. https://ec.europa.eu/info/sites/info/files/live_work_travel_in_the_eu/consumers/digitalisation_of_financial_services_-_main_report.pdf.

EC. *Crowdfunding Explained.* EC, 2015. https://ec.europa.eu/docsroom/documents/10229/attachments/1/translations/en/renditions/pdf.

EC. *Crowdfunding in the EU Capital Markets Union.* EC, 2016. https://ec.europa.eu/info/system/files/crowdfunding-report-03052016_en.pdf.

EC. "Inception Impact Assessment: Legislative Proposal for an EU Framework on Crowd and Peer to Peer Finance." EC, 2017. https://ec.europa.eu/info/law/better-regulation/initiative/1166/publication/124034/attachment/090166e5b61525a3_fr.

EC. "Proposal for a Directive of the European Parliament and of the Council amending Directive 2014/65/EU on markets in financial instruments." EC, 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018PC0099

EC. "Proposal for a Regulation of the European Parliament and of the Council on European Crowdfunding Service Providers (ECSP) for Business." EC, 2018. https://eur-lex.europa.eu/resource.html?uri=cellar:0ea638be-22cb-11e8-ac73-01aa75ed71a1.0003.02/DOC_1&format=PDF.

The Economist. "Created to Democratise Credit, P2P Lenders Are Going After Big Money." *The Economist,* December 5, 2019. https://www.economist.com/finance-and-economics/2019/12/05/created-to-democratise-credit-p2p-lenders-are-going-after-big-money.

EFIN (European Financial Inclusion Network) Working Group on Over-Indebtedness. *Indicators to Monitor Over-Indebtedness.* EFIN, 2016. http://mfc.org.pl/wp-content/uploads/2017/03/EFIN-WG-Over-Indebtedness-Indicators-VF6Dec.pdf.pdf.

Ehrentraud, J., D. Garcia Ocampo, L. Garzoni, and M. Piccolo. *Policy Responses to Fintech: A Cross-Country Overview* (FSI Insights on Policy Implementation No. 23). Bank for International Settlements, 2020. https://www.bis.org/fsi/publ/insights23.pdf.

European Central Bank. *Guide to Assessments of Fintech Credit Institution License Applications.* 2018.

European Parliamentary Research Service. *A Governance Framework for Algorithmic Accountability and Transparency.* April 2019.

Faridi, O. "P2P Fintech Lending Sector in Indonesia May Struggle Due to Risky Loans, as Lenders Rejected Over 50% of Restructuring Requests." *Crowdfund Insider*, June 11, 2020. crowdfundinsider.com/2020/06/162599-p2p-fintech-lending-sector-in-indonesia-may-struggle-due-torisky-loans-as-lenders-rejected-over-50-of-restructuring-requests/.

Financial Action Task Force. *Virtual Currencies: Key Definitions and Potential AML/CFT Risks.* Financial Action Task Force, 2014. https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

FCA (Financial Conduct Authority). *Detailed Rules for the Price Cap on High-Cost Short-Term Credit Including Feedback on CP14/10 and Final Rules* (PS14/16). FCA, 2014.

FCA. *The FCA's Regulatory Approach to Crowdfunding (and Similar Activities)* (CP13/13). FCA, October 2013. https://www.fca.org.uk/publication/consultation/cp13-13.pdf.

FCA. *The FCA's Regulatory Approach to Crowdfunding over the Internet, and the Promotion of Non-Readily Realisable Securities by Other Media: Feedback to CP13/13 and Final Rules* (PS14/04). FCA, 2014. https://www.fca.org.uk/publication/policy/ps14-04.pdf.

FCA. *Feedback Statement FS16/10 on Smarter Consumer Communications.* FCA, October 2016. https://www.fca.org.uk/publication/feedback/fs16-10.pdf.

FCA. *Financial Lives Survey*. FCA, 2020. https://www.fca.org.uk/publications/research/understanding-financial-lives-uk-adults.

FCA. *General Standards and Communication Rules for the Payment Services and E-money Sectors* (PS19/3). FCA, 2019. https://www.fca.org.uk/publication/policy/ps19-03.pdf.

FCA. *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms: Feedback on Our Post-Implementation Review and Proposed Changes to the Regulatory Framework* (CP18/20). FCA, 2018. https://www.fca.org.uk/publication/consultation/cp18-20.pdf.

FCA. *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms: Feedback to CP18/20 and Final Rules* (CP19/14). FCA, 2019. https://www.fca.org.uk/publication/policy/ps19-14.pdf.

FCA. *Message Received? The Impact of Annual Summaries, Text Alerts, and Mobile Apps on Consumer Banking Behavior* (FCA Occasional Paper No. 10). FCA, March 2015. https://www.fca.org.uk/publication/occasional-papers/occasional-paper-10.pdf.

FCA. "A Review of the Regulatory Regime for Crowdfunding and the Promotion of Non-Readily Realisable Securities by Other Media." FCA, February 2015. https://www.fca.org.uk/publication/thematic-reviews/crowdfunding-review.pdf.

FCA. "Temporary Intervention on the Marketing of Speculative Mini-Bonds to Retail Investors." FCA, November 2019. https://www.fca.org.uk/publication/tpi/temporary-intervention-marketing-speculative-mini-bonds-retail-investors.pdf.

Financial Markets Authority of New Zealand. *Fair Dealing in Advertising and Communications—Crowdfunding and Peer-to-Peer Lending*. Financial Markets Authority, 2018. https://www.fma.govt.nz/compliance/guidance-library/advertising-and-comms-in-crowdfunding-and-p2p/.

Financial Services Agency (Japan). Amendment of Financial Instruments and Exchange Act, and so on (Act No.44 of 2014) [Briefing Materials], May 2014.

Financial Times. "Ant Posed Threat to China's Centralised Control." *Financial Times*, November 9, 2020. https://www.ft.com/content/e703082a-2007-4bd3-aebc-f3e26f6085ae.

FinCoNet (International Financial Consumer Protection Organisation). "FinCoNet Annual General Meeting 2020," press release, November 2020. http://www.finconet.org/Press-release-FinCoNet_AGM-Nov-2020.pdf.

FinCoNet. *FinCoNet Report on Responsible Lending*. FinCoNet, 2014. http://www.finconet.org/FinCoNet-Responsible-Lending-2014.pdf.

FinCoNet. *Guidance to Supervisors on Digitalisation of Short-Term, High-Cost Consumer Credit*. FinCoNet, February 2019. http://www.finconet.org/Guidance_Supervisors_Digitalisation_STHCCC.pdf.

FinCoNet. *Guidance to Supervisors on the Setting of Standards in the Field of Sales Incentives and Responsible Lending*. FinCoNet, 2016.

FinCoNet. *Report on the Digitalisation of Short-Term, High-Cost Consumer Credit*. FinCoNet, November 2017. http://www.finconet.org/Digtalisation-Short-term-High-cost-Consumer-Credit.pdf.

FinCoNet. *SupTech Tools for Market Conduct Supervisors*. FinCoNet, November 2020. http://www.finconet.org/FinCoNet-Report-SupTech-Tools_Final.pdf.

FSD Kenya (Financial Sector Deepening Kenya). *Digital Credit Audit Report*. FSD Kenya, 2019. https://s3-eu-central-1.amazonaws.com/fsd-circle/wp-content/uploads/2019/11/13160713/Digital-Credit-audit-report.pdf.

FSD Kenya. "Tech-Enabled Lending in Africa," presentation, August 28, 2018. https://s3-eu-central-1.amazonaws.com/fsd-circle/wp-content/uploads/2018/10/02095806/FSD-Kenya-CIS-Digital-Credit.pdf.

FTC (USA Federal Trade Commission). *Mobile Privacy Disclosures: Building Trust through Transparency* (FTC Staff Report). FTC, February 2013. https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

G20 (Group of Twenty). *G20 High-Level Principles for Digital Financial Inclusion*. Global Partnership for Financial Inclusion, 2016. https://www.gpfi.org/publications/g20-high-level-principles-digital-financial-inclusion.

G20/OECD (Organisation for Economic Co-operation and Development) Task Force on Financial Consumer Protection. *Considerations for the Application of the G20/OECD High-Level Principles on Financial Consumer Protection to Digital and Alternative Financial Services*. OECD, 2018.

G20/OECD Task Force on Financial Consumer Protection. *Effective Approaches for Financial Consumer Protection in the Digital Age: FCP Principles 1, 2, 3, 4, 6 and 9*. OECD, 2019. http://www.oecd.org/finance/financial-education/Effective-Approaches-FCP-Principles_Digital_Environment.pdf.

G20/OECD Task Force on Financial Consumer Protection. *Effective Approaches to Support the Implementations of the G20 High-Level Principles on Financial Consumer Protection*. OECD, 2014. https://www.oecd.org/g20/topics/financial-sector-reform/financialconsumerprotection.htm.

G20/OECD Task Force on Financial Consumer Protection. *Financial Consumer Protection Policy Approaches in the Digital Age*. OECD, 2018. https://www.oecd.org/finance/G20-OECD-Policy-Guidance-Financial-Consumer-Protection-Digital-Age-2018.pdf.

Gibbens, E. "Helping Small Businesses Navigate through COVID-19." IFC Insights, IFC, March 20, 2020. https://www.ifc.org/wps/wcm/connect/news_ext_content/ifc_external_corporate_site/news+and+events/news/insights/smes-covid-19.

GPFI (Global Partnership for Financial Inclusion). *Data Protection and Privacy for Alternative Data* (GPFI-FCPL Sub-Group Discussion Paper). GPFI, May 2018. https://www.gpfi.org/sites/gpfi/files/documents/Data_Protection_and_Privacy_for_Alternative_Data_WBG.pdf.

GPFI. *Report on Advancing Women's Digital Financial Inclusion.* GPFI, 2020. https://www.gpfi.org/sites/gpfi/files/sites/default/files/saudig20_women.pdf.

Grady, R., et al. *Financial Consumer Protection and New Forms of Data Processing Beyond Credit Reporting* (Discussion Note). World Bank Group, 2018. http://documents.worldbank.org/curated/en/677281542207403561/pdf/132035-WP-FCP-New-Forms-of-Data-Processing.pdf.

GSMA (GSM Association). "Mobile Money Glossary," https://www.gsma.com/mobilefordevelopment/mobile-money/glossary/.

GSMA. *Safeguarding Mobile Money: How Providers and Regulators Can Ensure That Customer Funds Are Protected*. GSMA, 2016. https://www.gsma.com/mobilefordevelopment/resources/safeguarding-mobile-money-how-providers-and-regulators-can-ensure-that-customer-funds-are-protected/.

GSMA. *State of the Industry Report on Mobile Money 2018*. GSMA, 2018. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/2018-State-of-the-Industry-Report-on-Mobile-Money.pdf.

GSMA. *State of the Industry Report on Mobile Money 2019*. GSMA, 2019. https://www.gsma.com/sotir/wp-content/uploads/2020/03/GSMA-State-of-the-Industry-Report-on-Mobile-Money-2019-Full-Report.pdf.

Guzman, L. "SEC to Shut Down Eight More Online Lending Apps." CNN Philippines, September 27, 2019. https://www.cnnphilippines.com/business/2019/9/27/sec-illegal-online-lending-issuances.html.

Havrylchyk, O. *Regulatory Framework for Loan-Based Crowdfunding Platforms* (Economics Department Working Papers No. 1513). OECD, 2018. http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=ECO/WKP(2018)61&docLanguage=En.

High-Level Expert Group on Artificial Intelligence. *Ethics Guidelines for Trustworthy AI*. EC, 2018. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419.

Hornby, L., and A. Zhang. "China's Middle Class Hit by Shadow Banking Defaults." *Financial Times*, December 26, 2018. https://www.ft.com/content/c55901f0-ff7d-11e8-aebf-99e208d3e521.

Huang, R. H. "Online P2P Lending and Regulatory Responses in China: Opportunities and Challenges." *European Business Organization Law Review* 19, no. 1 (2018): 63–92. https://doi.org/10.1007/s40804-018-0100-z.

ICCR (International Committee on Credit Reporting). *Use of Alternative Data to Enhance Credit Reporting to Enable Access to Digital Financial Services by Individuals and SMEs Operating in the Informal Economy* (Guidance Note). ICCR, 2018. https://www.gpfi.org/sites/gpfi/files/documents/Use_of_Alternative_Data_to_Enhance_Credit_Reporting_to_Enable_Access_to_Digital_Financial_Services_ICCR.pdf.

IMF (International Monetary Fund). "Digital Financial Services and the Pandemic: Opportunities and Risks for Emerging and Developing Economies" (IMF Special Series on COVID-19). IMF, July 1, 2020. https://www.imf.org/en/Publications/SPROLLs/covid19-special-notes.

IMF. *The Promise of Fintech: Financial Inclusion in the Post COVID-19 Era*. IMF, 2020. https://www.imf.org/en/Publications/Departmental-Papers-Policy-Papers/Issues/2020/06/29/The-Promise-of-Fintech-Financial-Inclusion-in-the-Post-COVID-19-Era-48623.

Intergovernmental Fintech Working Group (South Africa). *IFWG Fintech Workshop 19–20 April 2018*. Financial Intelligence Centre, National Treasury, Financial Sector Conduct Authority, and South African Reserve Bank, 2018. https://www.fic.gov.za/Documents/Final%20IFWG%20Report_April%202018(lower%20res%20email%20version).pdf.

IOSCO (International Organization of Securities Commissions). *IOSCO Research Report on Financial Technologies (Fintech)* (FR02/2017). IOSCO, 2017. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf.

ITU-T (International Telecommunications Union) Focus Group on Digital Financial Services. *Commonly Identified Consumer Protection Themes for Digital Financial Services* (05/2016). International Telecommunications Union, 2016. https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/09_2016/ConsumerProtectionThemesForBestPractices.pdf.

ITU-T Focus Group on Digital Financial Services. *ITU Focus Group Digital Financial Services: Main Recommendations* (03/2017). International Telecommunications Union, 2017. https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/201703/ITU_FGDFS_Main-Recommendations.pdf.

Izaguirre, J. C., and R. Mazer. "How Regulators Can Foster More Responsible Digital Credit." *CGAP Blog*, November 5, 2018. https://www.cgap.org/blog/how-regulators-can-foster-more-responsible-digital-credit.

Izaguirre, J. C., M. Kaffenberger, and R. Mazer. "It's Time to Slow Digital Credit's Growth in East Africa." *CGAP Blog*, 2018. https://www.cgap.org/blog/its-time-slow-digital-credits-growth-east-africa.

Izaguirre, J. C., R. Mazer, and L. Graham. "Digital Credit Market Monitoring in Tanzania" (slide deck). Consultative Group to Assist the Poor, September 2018. https://www.cgap.org/sites/default/files/publications/slidedeck/Digital-Credit-Market-Monitoring-in-Tanzania-Slide-Deck-9-25-18.pdf.

Izaguirre, J. C., et al. "Deposit Insurance and Digital Financial Inclusion." *CGAP Brief*, October 2016. https://www.cgap.org/sites/default/files/Brief_Deposit_Insurance_and_Digital_Financial_Inclusion.pdf.

Izaguirre, J. C., et al. *Deposit Insurance Treatment of E-Money: An Analysis of Policy Choices* (CGAP Technical Note). Consultative Group to Assist the Poor, 2019. https://www.cgap.org/sites/default/files/publications/2019_10_Technical_Note_Deposit_Insurance_Treatment_EMoney_0.pdf.

Jurd De Girancourt, F., M. Kuyoro, N. Ofosu-Amaah, E. Seshie, and F. Twum. "How the COVID-19 Crisis May Affect Electronic Payments in Africa." McKinsey & Company Financial Services, June 4, 2020. https://www.mckinsey.com/industries/financial-services/our-insights/how-the-covid-19-crisis-may-affect-electronic-payments-in-africa.

Kaffenberger, M., and P. Chege. "Digital Credit in Kenya: Time for Celebration or Concern?" *CGAP Blog*, October 2016. https://www.cgap.org/blog/digital-credit-kenya-time-celebration-or-concern.

Kaffenberger, M., and E. Totolo. *A Digital Credit Revolution: Insights from Borrowers in Kenya and Tanzania* (Working Paper). Consultative Group to Assist the Poor, 2018. https://www.cgap.org/sites/default/files/publications/Working-Paper-A-Digital-Credit-Revolution-Oct-2018.pdf.

Karakas, C., and C. Stamegna. "Defining an EU-Framework for Financial Technology (Fintech): Economic Perspectives and Regulatory Challenges." *Law and Economics Yearly Review* 7, no. 1 (2018): 106–29. http://www.laweconomicsyearlyreview.org.uk/Law_and_Economics_Yearly_Review_LEYR_Journal_vol_7_part_1_2018.pdf.

Kerse, M., and S. Staschen. *Safeguarding Rules for Customer Funds Held by EMI and GSMA* (CGAP Technical Note). Consultative Group to Assist the Poor, 2018. https://www.cgap.org/sites/default/files/publications/Technical-Note-Safeguarding-Funds-Dec-2018.pdf.

Kerse, M., et al. *Technical Note on the Use of Agents by Digital Financial Services Providers* (Technical Note). Consultative Group to Assist the Poor, 2020. https://www.cgap.org/sites/default/files/publications/2020_02_Technical_Note_Use_Agents_Dig_Fin_Serv_Providers.pdf.

Kyamutetera, M. "Hackers Break Into Mobile Money System, Make Off with Unspecified Billions Belonging to Airtel, MTN, Stanbic, and Other Financial Institutions." *The CEO East Africa,* October 5, 2020. https://www.ceo.co.ug/hackers-break-into-mobile-money-system-make-off-with-unspecified-billions-belonging-to-airtel-mtn-stanbic-and-other-financial-institutions/.

Lee, N., et al. "Algorithmic Bias Detection and Mitigation: Best Practices and Policies to Reduce Consumer Harms." Brookings, May 22, 2019. https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/.

Lenz, R. "Peer-to-Peer Lending—Opportunities and Risks." *European Journal of Risk Regulation* 7, no. 4 (2016): 688–700. https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/peertopeer-lending-opportunities-and-risks/9B9E21667A148330DDA491775A23AF5E.

Liu, J. "The Dramatic Rise and Fall of Online P2P Lending in China." *Tech Crunch,* August 2, 2018. https://techcrunch.com/2018/08/01/the-dramatic-rise-and-fall-of-online-p2p-lending-in-china/.

Lo, B. "If It Ain't Broke: The Case for Continued SEC Regulation of P2P Lending." *Harvard Business Law Review Online* 6 (2016): 87–110. https://www.hblr.org/hblr-online-volume-6-2016/.

Makortoff, K. "Peer-to-Peer Lender Funding Secure Goes into Administration." *The Guardian*, October 24, 2019. https://www.theguardian.com/money/2019/oct/23/peer-to-peer-lender-funding-secure-administration-pawnbroker.

Mazer, R. "Does Transparency Matter: Assessing the Impact of Improved Disclosure in Digital Financial Services in Kenya" (slide deck). Consultative Group to Assist the Poor, 2018. https://www.cgap.org/sites/default/files/publications/slidedeck/2018_03-Slidedeck-Does_Transparency_Matter.pdf.

Mazer, R. "Kenya's Rules on Mobile Money Price Transparency Awareness Are Paying Off." *CGAP Blog,* April 4, 2018.

Mazer, R., and K. McKee. "Consumer Protection in Digital Credit" (Focus Note 108). Consultative Group to Assist the Poor, 2017. https://www.cgap.org/sites/default/files/Focus-Note-Consumer-Protection-in-digital-Credit-Aug-2017.pdf.

Mazer, R., and P. Rowan. "Competition in Mobile Financial Services: Lessons from Kenya and Tanzania" (Working Paper). Consultative Group to Assist the Poor, 2016. https://www.cgap.org/sites/default/files/Working-Paper-Competition-in-MFS-Kenya-Tanzania-Jan-2016.pdf.

Mazer, R., J. Vancel, and A. Keyman. "Finding 'Win-Win' in Digitally-Delivered Consumer Credit." *CGAP Blog*, January 13, 2016. https://www.cgap.org/blog/finding-win-win-digitally-delivered-consumer-credit.

McKee, K., et al. "Doing Digital Finance Right: The Case for Stronger Mitigation on Customer Risks" (Focus Note 103). Consultative Group to Assist the Poor, 2015. https://www.cgap.org/sites/default/files/Focus-Note-Doing-Digital-Finance-Right-Jun-2015.pdf.

Megaw, N. "Peer-to-Peer Groups Battle to Survive More Hostile Market." *Financial Times,* June 9, 2019. https://www.ft.com/content/275c7d6a-8880-11e9-97ea-05ac2431f453.

MicroSave. "Making Digital Credit Truly Responsible." Center for Financial Inclusion, September 2019. https://content.centerforfinancialinclusion.org/wp-content/uploads/sites/2/2019/09/Digital-Credit-Kenya-Final-report.pdf.

MicroSave. "Where Credit Is Due: Customer Experience of Digital Credit in Kenya." Center for Financial Inclusion, March 2017. https://www.microsave.net/wp-content/uploads/2018/10/Where_Credit_Is_Due_Customer_Experience_of_Digital_Credit_In_Kenya.pdf.

Morawczynski, O. "Fraud in Uganda: How Millions Were Lost to Internal Collusion." *CGAP Blog*, March 11, 2015. https://www.cgap.org/blog/fraud-uganda-how-millions-were-lost-internal-collusion.

Morita, H. 2016. "Crowdfunding in Japan: Current Regulation and the Future of Business." SSRN, March 21, 2016. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2752312.

New, J., and D. Castro. "How Policymakers Can Foster Algorithmic Accountability." Center for Data Innovation, 2018. http://www2.datainnovation.org/2018-algorithmic-accountability.pdf.

OECD (Organisation for Economic Co-operation and Development). *Financial Consumer Protection Policy Approaches in the Digital Age—Protecting Consumers' Assets, Data and Privacy*. OECD, 2020. https://www.oecd.org/daf/fin/financial-education/Financial-Consumer-Protection-Policy-Approaches-in-the-Digital-Age.pdf.

OECD. *G20 High-Level Principles on Financial Consumer Protection*. OECD, 2011. https://www.oecd.org/daf/fin/financial-markets/48892010.pdf.

OECD. *Recommendation of the Council on Artificial Intelligence* (OECD/LEGAL/0449). OECD, 2019. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

OECD. *Recommendation of the Council on Consumer Protection in the field of Consumer Credit* (OECD/LEGAL/0453). OECD, 2019. https://www.oecd.org/finance/financial-education/Recommendation-FCP-Consumer_Credit.pdf.

OECD. *Short-Term Consumer Credit: Provision, Regulatory Coverage and Policy Responses*. OECD, 2019. http://www.oecd.org/daf/fin/financial-education/Short-term-consumer-credit-report.pdf.

OJK (Otoritas Jasa Keuangan). "OJK Issues Regulation on IT-Based Lending Services," press release SP 01/DKNS/OJK/I/2017, January 10, 2107. https://www.ojk.go.id/en/berita-dan-kegiatan/siaran-pers/Documents/Pages/Press-Release-OJK-Issues-Regulation-on-It-Based-Lending-Services/SIARAN%20PERS%20POJK%20%20%20%20FIntech-ENGLISH.pdf.

Owens, J. "Responsible Digital Credit." Center for Financial Inclusion, 2018. https://content.centerforfinancialinclusion.org/wp-content/uploads/sites/2/1970/01/Responsible_Digital_Credit_FINAL_2018.07.18.pdf.

Oxera. *Crowdfunding from an Investor Perspective*. Oxera, 2015. https://ec.europa.eu/info/sites/info/files/file_import/160503-study-crowdfunding-investor-perspective_en_0.pdf.

Rahman, R. "'They Terrorized Me Every Day': Fintech Debtors Tell of Abuse." *The Jakarta Post*, November 6, 2018. https://www.thejakartapost.com/news/2018/11/06/they-terrorized-me-every-day-fintech-debtors-tell-of-abuse.html.

Reserve Bank of India. *Report of the Working Group on FinTech and Digital Banking*. Reserve Bank of India Central Office, 2017. https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/WGFR68AA1890D7334D8F8F72CC2399A27F4A.PDF.

Reserve Bank of Zimbabwe. "Cash-In, Cash-Out and Cash-Back Facilities," press statement, October 2, 2019. https://www.rbz.co.zw/documents/press/Press-Statement---02-October-2019.pdf.

Reuters. "Regulatory Problems Have Choked China's P2P Lending Industry." *The Japan Times,* September 6, 2019. https://www.japantimes.co.jp/news/2019/09/06/business/regulatory-problems-choked-chinas-p2p-lending-industry/.

Reynolds, T., M. Klawitter, C. L. Anderson, P. Biscaye, K. Callaway, M. Greenaway, D. Lunchick-Seymour, M. McDonald, and A. Hayes. "Review of Digital Credit Products in India, Kenya, Nigeria, Tanzania, and Uganda." Evans School of Policy Analysis and Research, April 2017. https://evans.uw.edu/wp-content/uploads/files//EPAR_UW_351a_Review%20of%20Digital%20Credit%20Products_4.12.17.pdf.

Safaricom. "Update on April 24th Network Outage," press release, April 25, 2017. https://www.safaricom.co.ke/about/media-center/publications/press-releases/release/355.

Samitsu, A. "Structure of P2P Lending and Investor Protection: Analyses Based on an International Comparison of Legal Arrangements" (Bank of Japan Research LAB No17-E-6). Bank of Japan, October 23, 2107. https://www.boj.or.jp/en/research/wps_rev/lab/lab17e06.htm/.

SEC (USA Securities and Exchange Commission). "Facilitating Capital Formation and Expanding Investment Opportunities by Improving Access to Capital in Private Markets: A Proposed Rule by the Securities and Exchange Commission on 03/31/2020." *Federal Register*, March 31, 2020. https://www.federalregister.gov/documents/2020/03/31/2020-04799/facilitating-capital-formation-and-expanding-investment-opportunities-by-improving-access-to-capital.

SEC. "Final Rule: Crowdfunding", Release Nos. 33-9974; 34-76324; File No. S7-09-13, RIN 3235-AL37, March 25, 2015. https://www.sec.gov/rules/final/2015/33-9974.pdf.

SEC. "Investor Bulletin: Be Cautious of SAFEs in Crowdfunding." US Securities and Exchange Commission, May 9, 2017. https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_safes.

SEC. "SEC Proposes Rule Changes to Harmonize, Simplify and Improve the Exempt Offering Framework," press release 2020-55, March 4, 2020. https://www.sec.gov/news/press-release/2020-55.

SEC. "Updated Investor Bulletin: Crowdfunding for Investors." US Securities and Exchange Commission, May 10, 2017. https://www.sec.gov/oiea/investor-alerts-bulletins/ib_crowdfunding-.html.

Securities and Exchange Commission (Brazil). *Public Hearing Notice SDM No. 02/2020*.

Shin & Kim. "National Assembly Passes New Law for P2P Lenders, Becoming the First of Its Kind to Provide Legal Basis for Marketplace Lending." Lexology, November 7, 2019. https://www.lexology.com/library/detail.aspx?g=dd7ef79a-5c8d-4462-963f-229db56435fd.

The Smart Campaign. "Tiny Loans, Big Questions: Client Protection in Mobile Consumer Credit." Center for Financial Inclusion, 2017. https://www.centerforfinancialinclusion.org/smart-brief-tiny-loans-big-questions.

The Smart Campaign. "Standards of Protection for Digital Credit." Center for Financial Inclusion, June 2019. https://www.smartcampaign.org/storage/documents/Digital_Credit_Standards_June_2019.pdf.

Stanbic Bank Uganda, MTN Uganda, and Airtel Uganda. "System Incident Impacting Bank to Mobile Money Transactions," press statement, October, 5, 2020. https://www.mtn.co.ug/press-statement/.

Staschen, S. "Basic Regulatory Enablers for Digital Financial Services" (CGAP Focus Note). Consultative Group to Assist the Poor, May 2018. https://www.cgap.org/research/publication/basic-regulatory-enablers-digital-financial-services.

World Bank Group. *Capital Markets and SMEs in Emerging Markets and Developing Economies: Can They Go the Distance?* World Bank Group, 2020. https://openknowledge.worldbank.org/handle/10986/33373.

World Bank Group. *Global Experiences from Regulatory Sandboxes*. World Bank Group, 2020. https://openknowledge.worldbank.org/handle/10986/34789.

World Bank Group. *Global Financial Inclusion and Consumer Protection Survey: 2017 Report*. World Bank Group, 2017. https://openknowledge.worldbank.org/handle/10986/28998?locale-attribute=en.

World Bank Group. *Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Agenda*. World Bank Group, 2017. https://openknowledge.worldbank.org/handle/10986/29510.

World Bank Group. *Good Practices for Financial Consumer Protection*: *2017 Edition*. World Bank Group, 2017. https://openknowledge.worldbank.org/handle/10986/28996.

World Bank Group. *The Next Wave of Suptech Innovation: Suptech Solutions for Market Conduct Supervision*. World Bank Group, 2021. http://documents.worldbank.org/curated/en/735871616428497205/The-Next-Wave-of-Suptech-Innovation-Suptech-Solutions-for-Market-Conduct-Supervision

World Bank Group. *Prudential Regulatory and Supervisory Practices for Fintech: Payments, Credit and Deposits*. World Bank Group. 2019. https://openknowledge.worldbank.org/handle/10986/33221.

World Bank Group and CCAF (Cambridge Centre for Alternative Finance). *Regulating Alternative Finance: Results from a Global Regulator Survey*. World Bank Group, 2019. https://openknowledge.worldbank.org/bitstream/handle/10986/32592/142764.pdf.

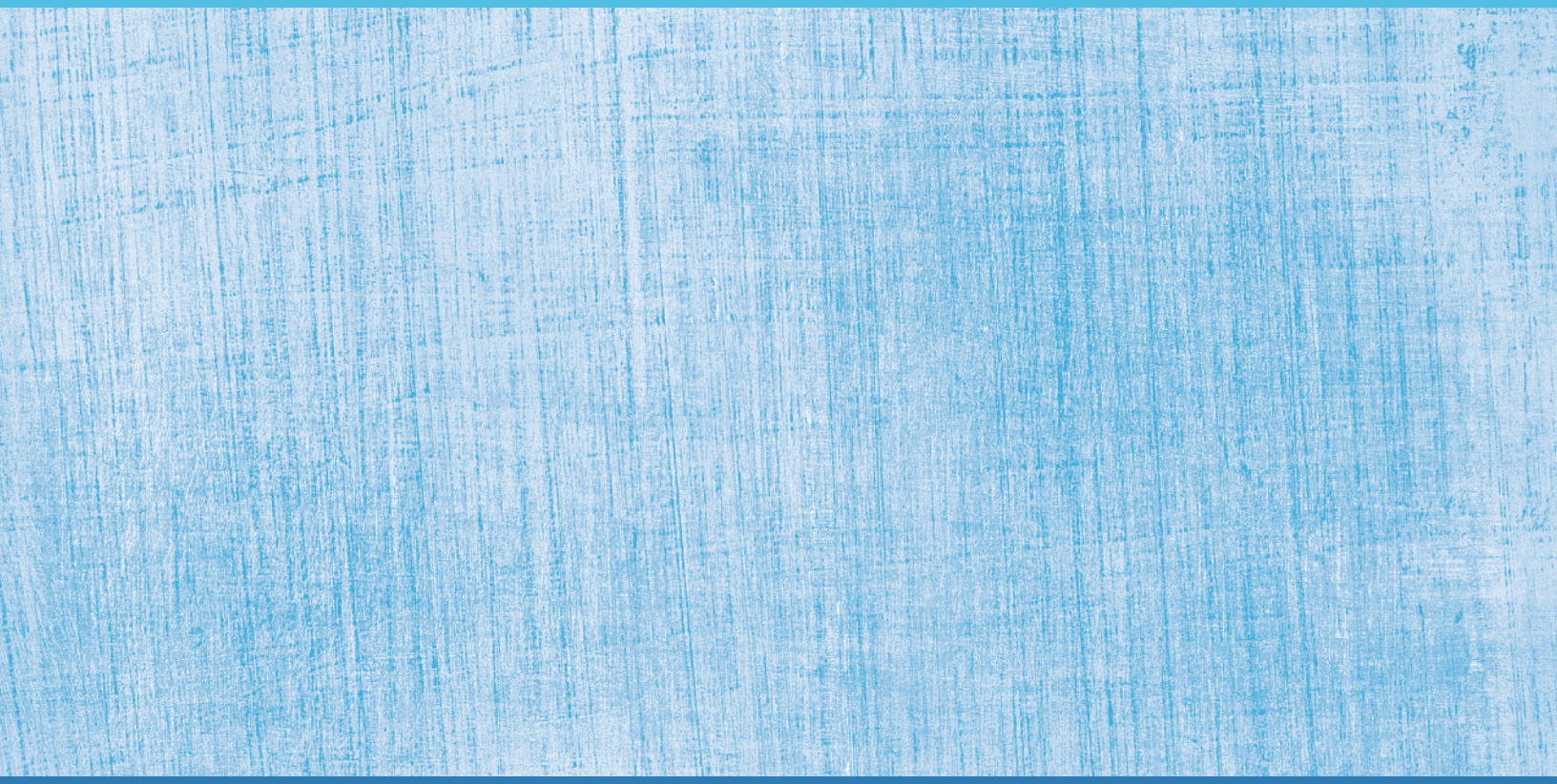
World Bank Group and International Committee on Credit Reporting. *Credit Scoring Approaches Guidelines*. World Bank Group, 2019. http://pubdocs.worldbank.org/en/935891585869698451/CREDIT-SCORING-APPROACHES-GUIDELINES-FINAL-WEB.pdf.

World Bank Group and International Monetary Fund. *The Bali Fintech Agenda—Background Paper*. International Monetary Fund, 2018. https://www.imf.org/~/media/Files/Publications/PP/2018/pp101118-bali-fintech-agenda.ashx.

Xiao, L. "Improving China's P2P Lending Regulatory System: An Examination of International Regulatory Experience." *US-China Law Review* 13 (2016): 460–73. https://pdfs.semanticscholar.org/11a2/06c0dbd2f55e49803c475ba0e178bfd79604.pdf.

Ziegler, T., et al. *Shifting Paradigms: The 4th European Alternative Finance Benchmarking Report*. University of Cambridge, 2019. https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2019-04-4th-european-alternative-finance-benchmarking-industry-report-shifting-paradigms.pdf.

Zimmerman, J., and S. Baur. "Understanding How Consumer Risks in Digital Social Payments Can Erode Their Financial Inclusion Potential." *CGAP Brief*, March 2016. https://www.cgap.org/sites/default/files/researches/documents/Brief-Understanding-How-Consumer-Risks-in-Digital-Social-Payments-March-2016.pdf.



WORLD BANK GROUP