INTERNATIONAL MONETARY FUND

MONETARY AND CAPITAL MARKETS
AND LEGAL DEPARTMENTS

E-Money

Prudential Supervision, Oversight, and User Protection

Prepared by Marc Dobler, José Garrido, Dirk Jan Grolleman,
Tanai Khiaonarong, and Jan Nolte

DP/2021/027

2021
DEC

DEPARTMENTAL PAPER

INTERNATIONAL MONETARY FUND

MONETARY AND CAPITAL MARKETS AND LEGAL DEPARTMENTS

DEPARTMENTAL PAPERS

E-Money

Prudential Supervision, Oversight, and User Protection

Prepared by Marc Dobler, José Garrido, Dirk Jan Grolleman, Tanai Khiaonarong, and Jan Nolte

Cataloging-in-Publication Data
IMF Library

Names: Dobler, Marc, author. | Garrido, José María, 1965-, author. | Grolleman, Dirk Jan,author. | Tanai Khiaonarong, author. | Nolte, Jan Philipp, author. | International Monetary Fund, publisher.
Title: E-money : prudential supervision, oversight, and user protection / prepared by Marc Dobler, José Garrido, Dirk Jan Grolleman, Tanai Khiaonarong, and Jan Nolte.
Other titles: International Monetary Fund. Monetary and Capital Markets Department (Series). | International Monetary Fund. Legal Department (Series).
Description: Washington, DC : International Monetary Fund, 2021. | 2021 December. | Departmental Paper Series. | Includes bibliographical references.
Identifiers: ISBN 9781513593401 (paper)
Subjects: LCSH: Electronic funds transfers—Law and legislation. | Deposit insurance. | Financial institutions—Law and legislation.
Classification: LCC K1081 .D6 2021

Prepared by a joint team from the IMF Monetary and Capital Markets and Legal Departments, led by Marc Dobler and José Garrido and comprising Dirk Jan Grolleman, Tanai Khiaonarong, and Jan Nolte (coordinator), with contributions from Ender Emre, Cristina Muller, Ryan Rizaldy, Arthur Rossi, Hironori Suganuma, and Mario Tamez. We would like to thank Tobias Adrian, Alessandro Gullo, Dong He, Yan Liu, Aditya Narain, and Miguel A. Savastano (all IMF) for their guidance, as well as Jonathan Greenacre (Boston University), Danilo Palermo (World Bank), and Bert van Roosebeke (IADI) for their review comments. Charmane Ahmed and Israel Guerrero supported the production of the paper.

JEL Classification Numbers:	G18, G23, G28, G33, K30, O30
Keywords:	E-money, Financial regulation, Payment systems, Deposit insurance, Digital currency, Debit cards, Deposit banking
Authors' E-Mail Addresses:	mdobler@imf.org; jgarrido@imf.org; dgrolleman@imf.org; tkhiaonarong@imf.org; jnolte@imf.org

Publication orders may be placed online or through the mail:
International Monetary Fund, Publication Services
P.O. Box 92780, Washington, DC 20090, USA
T. +(1) 202.623.7430
publications@imf.org
IMFbookstore.org
elibrary.IMF.org

Contents

1. Introduction

This departmental paper discusses the evolving prudential frameworks for nonbank[1] issuers of electronic money. Some jurisdictions take a relatively light-touch approach to regulating electronic money issuers (EMIs). Others have sought to apply more stringent requirements to protect electronic money (e-money) users, as the sector has grown in importance. The paper aims to build on previous IMF staff contributions to the literature and to draw policy conclusions for strengthening e-money regulatory regimes; in particular in jurisdictions where issuers, individually or collectively, have grown to a size to which they are of macro-financial importance (see below). Chapter 2 provides background on the development of e-money, its economic benefits, and potential risks. Chapter 3 discusses prudential supervision of EMIs, followed in Chapter 4 by their oversight from a payments system perspective. Chapter 5 discusses potential additional measures for user protection and contingency arrangements for EMI failure. The last chapter presents policy recommendations for policymakers, especially in those emerging market economies and developing countries wherein EMIs have reached a scale at which they could have a significant economic impact if they were to fail.

[1] Any entity involved in the provision of retail payment services whose main business is not related to taking deposits from the public and using these deposits to make loans (CPMI 2014), which range from unlicensed fintech companies to e-money issuers with a narrow license for payment services.

2. Background

Definitions for e-money differ across jurisdictions (Box 1). E-money can be defined as a stored monetary value or prepaid product in which a record of the funds or value available to the consumer for multipurpose use is stored on a prepaid card or electronic device (for example, a computer or mobile phone), and which is accepted as a payment instrument by other than the issuer (multipurpose use). The stored value represents a claim enforceable against the e-money provider to repay the balance on demand and in full. This redeemability distinguishes e-money from retail gift cards and other payment instruments that can only be spent with one retail group (single purpose).[2] E-money can also be distinguished from "mobile banking," the term applied to provision of payment and other services by banks through, for example, mobile phones or the internet.

Box 1. Legal Nature of E-Money

Definition of e-Money

Different approaches have been adopted regarding the definition of e-money, for example:

- **EU Directive**: Electronically, including magnetically, stored monetary value as represented by a claim on the issuer, which is issued on receipt of funds for the purpose of making payment transactions and which is accepted by a natural or legal person other than the EMI.
- **Kenya**: Monetary value as represented by a claim on its issuer, which is (1) electronically or magnetically stored, (2) issued against receipt of currency of Kenya or any other currency authorized by the Central Bank of Kenya, and (3) accepted as a means of payment by persons other than the issuer.
- **Singapore**: Any electronically stored monetary value that (1) is denominated in any currency or pegged by its issuer to any currency; (2) has been paid for in advance to enable the making of payment transactions through the use of a payment account; (3) is accepted by a person other than its issuer; and (4) represents a claim on its issuer, but does not include any deposit accepted in Singapore, from any person in Singapore.

The following common elements can be discerned from the above: (1) electronic store of monetary value, (2) expressed in an existing official monetary unit, (3) representing a claim enforceable against the EMI, and (4) accepted as means of payment by undertakings other than the EMI.

Legal Relationship between the EMI and the User

From a legal perspective, typically the EMI holds money on the user's behalf, with the obligation of redeeming such funds when demanded. The user has a claim against the issuer, and the issuer is keeping the money on behalf of the user and is executing the users' instructions regarding payments with such funds. Thus, even when the physical cash has been transferred to the EMI, the funds should remain fully available for the user to make payments. In general, e-money legal frameworks, in consideration of the different policy objectives (for example, user protection) and the purpose of the operation (making payments), provide that users' funds should be segregated from other assets and liabilities of the EMI, and the EMIs are allowed to invest the funds only in "safe and liquid" assets. In this context, it is relevant to consider legal protection under two distinct scenarios:

- *Insolvency of the EMI:* If the amounts received from users, in line with the governing legal provision, are adequately invested and recorded in the EMI's balance sheet in a way that they can be indisputably identified, such funds should be treated as users' assets and segregated from other assets and liabilities, without exposure to losses.

[2] Existing crypto-assets (for example, Bitcoin, Litecoin, Ethereum, etc.) do not fall within the definition of e-money. Most stable coins also do not meet the definition (for example, claim on the issuer and the right to redeem at par). Stable coins that are designed as, and fall within the definition of, e-money should be regulated according to the same requirements. For the categorization of digital currencies, see Mancini-Griffoli (2019).

Box 1. Legal Nature of E-Money *(continued)*

- *Materialization of operational, business, and investment risks*: EMIs will be exposed to several operational risks, including fraud and cybersecurity incidents and to business and investment risks, for example, failure of the EMI's bank or banks. These risks may still expose users to loss despite segregation safeguards.

While e-money operations and bank deposits share similar features (for example, they both involve transfer of funds to a financial institution and the provision of payment services), in bank deposits the bank can use the deposited funds without any restrictions, particularly to make loans.

Legal Form of EMIs

E-money can be issued by different types of firms. The key difference between e-money and mobile/e-banking stems from the legal and regulatory status of EMIs (not being legally classified or regulated as banks). These firms take the form of subsidiaries of phone companies, payment providers, or so-called "fintech" (financial technology) firms.

E-money services have evolved in conjunction with a rapid growth in mobile networks and access to the internet. Many people in Africa and other developing regions do not have access to bank accounts. The "unbanked" typically have to rely on cash or cash-based (such as money order) payment services, which are often slow, unreliable, and costly. However, access to mobile phone networks has grown rapidly across developing countries, enabling EMIs to provide financial services to large numbers of customers who were previously without access. Digital financial services are faster, more efficient, and typically cheaper than traditional financial services (Sahay and others 2021) and can deliver significant benefits in terms of financial inclusion. In a growing number of developing countries, mobile money (a specific form of e-money) is used for a significant portion of payments in the economy (Box 2).

E-money has grown rapidly in some countries and is making EMIs potentially systemic in some cases. In several East African countries, the e-money system is important from a macro-financial perspective, given the percentage of the population using e-money and the lack of substitutability—the unavailability of other payment instruments and service providers of scale. For instance, Safaricom's M-Pesa in Kenya accounts for about 90 percent of mobile money transactions.[3] It is estimated that two-thirds of the combined adult population of Kenya, Rwanda, Tanzania, and Uganda use e-money regularly. Of those, many do not have a bank account or other access to the formal financial system. As such, the rapid adoption of e-money and its market concentration in some jurisdictions may make EMIs potentially systemic from a macro-financial perspective—the impact on the real economy, given the importance of the payments services they provide in day-to-day transactions, if they were to fail and if e-money users were to lose a significant share of their disposable funds.

The growing importance of EMIs and their evolving business models make their regulatory framework and arrangements for protecting e-money users increasingly pressing. Regulatory practices are evolving on a country-by-country basis, and international standards[4] may not be fully tailored to the specific risks posed by some EMIs. Measures to strengthen regulatory frameworks may, in particular, be needed where:

- An EMI or the whole sector has become systemic because of the size (transaction volume, value of stored funds) as well as the number and types of users and where the failure could have a macro-financial impact, as other sectors, for example, banking and government, could be negatively impacted by a failure of large EMIs, through large exposures to e-money balances (concentration risk) and interdependencies (for example, tax collection) ("potentially systemic" argument; see some suggested criteria in Table 1).
- E-money accounts have become "deposit-like" (for example, users hold high proportions of their disposable funds for extended periods) and are being used for savings as well as transactional purposes ("functional" argument).
- A large portion of society has no access to conventional banking and is using EMIs as substitutes ("financial inclusion" argument).

[3] At the same time, the number of Kenyans using two or more types of financial services has increased from 9 percent in 2006 to 74 percent in 2019.
[4] The Basel Core Principles, the Principles for Financial Market Infrastructures, the IADI Core Principles for Effective Deposit Insurance Systems, and the FSB Key Attributes of Effective Resolution Regimes for Financial Institutions.

- EMIs' products are used by many unsophisticated, low-income households and small businesses, particularly vulnerable to financial losses if an EMI were to fail ("consumer protection" argument).

Box 2. E-Money Systems

In e-money schemes, users have access to payment functions similar to those in bank-based deposit systems. Users can (1) store cash in an account indefinitely, (2) transfer some or all of their balance to other mobile money users or receive payments, and/or (3) convert some or all of their balance back into cash. Customers can be persons, merchants/corporates, banks, utilities, and governments. In cash-based e-money services, EMIs may operate with a closed-loop system wherein all e-money transactions are settled in the EMI's own platform, and interbank payment and settlement systems are only used for the distribution of trust balances among banks. E-money payments in advanced economies, with wide access to bank services, are often linked with preexisting bank accounts or credit cards; while in developing countries, the systems may be linked to a SIM-card and cash-based. Here, e-money users deposit and withdraw funds through a network of local agents. The activities of "mobile money" issuers typically include:

- **Issuance of e-money (mobile money)**: Customers receive one unit of e-money for each unit of cash they provide to agents. E-money is stored in their transaction accounts, linked to their mobile phone and accessible through a SIM card.
- **Operating a platform**: The platform consists of hardware and software allowing the e-money issuer to keep records of transaction accounts of customers and their balances and settle payments between e-wallets. Payment and other financial service messages are communicated through the telecommunication network also used for voice and data services.
- **Fund management**: The cash received from customers is invested and managed according to regulation (for example, held in a trust or in escrow in pooled bank accounts). Issuers have a treasury function to invest customers' funds. EMIs are not allowed to use the funds to provide credit directly to the public.
- **Management of an agent distribution network**: Issuers maintain a network of agents and authorized retail outlets, to provide face-to-face contact with users, an entry point for them to register for an e-wallet, and a convenient location to cash in and cash out e-money.

Some EMIs' business models have developed from pure payment services to providing broader mobile financial services. These include access to credit, savings products, insurance products, and other financial services as part of a strategic alliance with licensed financial institutions. The EMI is only executing instructions of the financial institution and not extending loans or savings products on its own account.

Table 1. Potential Systemic Risk Criteria and Indicators for EMIs

Criteria[1]	Indicator
Size: The importance of an EMI for the welfare of the population, which generally increases with the volume of payments and other services that it provides (including across border).	Number of customers measured by (active) accounts. Types of customers such as individuals, merchants, utilities, insurance companies, and governments. Number and value of transactions; market share controlled. Breadth of services provided.
Substitutability: The importance of an EMI increases where it is difficult for other entities to provide the same or similar services (including in size).	Availability of cash-out points that do not need the use of the EMIs, that is, agents and ATMs linked to other EMIs and banks, and bank branches. Availability of other payment options such as debit/credit cards, checks, postal money orders, and bank transfers.
Interconnectedness: Systemic risk can arise through macro-financial linkages between EMIs and national sectors and/or markets so that the EMI's failure negatively impacts the functioning of the other sectors, or public confidence in any of the sectors.	Float balances of EMIs expose banks to concentration risk through exposures to large deposits. EMIs growth affects the profitability of banks by competing for clients, funds, and services. The use of e-money services for paying government taxes and utility bills exposes governments and utilities to potential loss of income if the EMI fails. The failure of an EMI may undermine public confidence in other EMIs, banks, utility firms, etc.

Source: IMF staff.
[1]See also IMF-BIS-FSB (2009).

3. Prudential Regulation and Supervision of EMIs

International prudential standards are well established for banks, insurers, and securities intermediaries, but not yet for EMIs.[5] The ultimate objective of prudential supervision is to protect savers and investors, and to preserve financial stability. To achieve these objectives, prudential regulation and supervision pursue safe and sound financial groups, financial systems, and markets. This is distinct from payment oversight, which concentrates on the sound and safe functioning of the payment systems, including critical service providers (CPMI 2005). International prudential standards generally require financial institutions and groups to control and manage their risks and hold adequate capital and liquidity to ensure their financial soundness. They provide a framework for risk management and corporate governance to ensure the integrity of the institution and the financial system. While there are no international standards for the regulation and supervision of EMIs, many countries have put in place well-developed legal frameworks for e-money and require a license and compliance with prudential standards to operate as an EMI (IMF 2021).

Prudential supervision should be proportionate to the risks to e-money users and to the financial system. The speed of technological innovation in products, services, and delivery channels require supervisors to fully understand the risks involved (Annex 1) and to tailor their prudential requirements accordingly. Recognizing financial inclusion benefits, policymakers need to consider novel approaches to ensure high-quality supervision and regulation and support the safe use of innovative technologies while ensuring that regulation remains proportionate to the risks (Sahay and others 2021). The remainder of this section discusses the approaches taken in sample jurisdictions[6] and concludes with policy recommendations on key aspects of licensing and supervising EMIs.

A. Legal Structure

Authorities generally apply prudential requirements on the legal, managerial, operational, and ownership structures of EMIs. As a practical consequence of this principle, EMIs in most countries are required to conduct their activities as a legal entity separate, for example, from a mobile network operator that may be the parent. A separate legal entity facilitates (1) the segregation of the activities from other activities and financial flows (potentially limiting the risk of the EMI failing owing to losses in other business activities) and (2) the regulation and prudential supervision of the EMI on a standalone basis.

B. Fund Safekeeping

EMIs need to limit the risk to which client funds are exposed and therefore should not be allowed to intermediate customer funds. The intermediation of retail client funds is an activity that should require—in line with international standards and best practices—a credit institution license, for example, as bank, credit union, microfinance institution, etc. As a result of not being allowed to intermediate client funds, EMIs should have limited (or potentially no) exposure to credit, maturity transformation, and leverage risks. Accordingly, regulatory requirements related to credit institutions' intermediation (for example, risk-weighted capital and related-party lending) may not be applicable or are generally simplified. Instead, EMIs are typically required to maintain a pool of liquid funds (e-float), at least equivalent to the aggregate balance of their clients' e-wallets.

This one-on-one matching requirement should ensure that EMIs always have sufficient funds to pay out their customers. Generally, jurisdictions require that investments should be in instruments with minimal credit, market, and liquidity risks, and available on demand. A widely used practice is to require EMIs to hold liquid assets in demand deposits at domestic commercial banks. This minimizes liquidity risks, as these types of deposits provide the EMI with prompt access for cash

[5] International prudential standards for banks, insurers and securities intermediaries, and financial market infrastructures are set, respectively, by the Basel Committee for Banking Supervision, International Association of Insurance Supervisors, International Organization of Securities Commissions, and the Committee on Payments and Market Infrastructures.
[6] Colombia, European Union, India, Kenya, Nigeria, the Philippines, Singapore, and the United States.

withdrawals. It also minimizes credit risks, by placing the funds in supervised entities of sound credit, as well as potentially credit concentration risks if diversified across several banks.

EMIs may also be authorized to invest a portion of client funds in tradable, high-quality, and short-term securities. Treasuries and short-term, tradeable government debt could be allowed, in the presence of liquid secondary markets, as these would limit (but not eliminate) liquidity risks. In addition, this approach adds some market risk, as the value of these securities will fluctuate with market interest rates, although, given the short maturities, the fluctuation should be limited. In light of these risks, EMIs that are allowed to invest in securities should be subject to more sophisticated risk management requirements (including a prohibition on the re-use or pledge of these securities), as well as prudential requirements that take into account market risk and/or limits. Allowing EMIs to invest in short-term government securities could, to some extent, limit credit risks, as they generally have lower credit risk than commercial banks. Another advantage could be potentially higher returns compared to placing the EMIs in demand deposits at banks. However, these potential advantages should be carefully weighed against the additionally introduced liquidity and market risks.

Alternatively, requiring or allowing EMIs to deposit the client funds in a reserve account at the central bank would remove investment risks. Requiring e-money users' funds to be held in a reserve account eliminates credit and investment risks, but does not protect against others, for example, operational risks. From an EMI business model perspective, depositing at the central bank may be less attractive because the return may be lower than a commercial deposit or short-term government debt. It may also contribute to some extent, to the disintermediation of user funds.[7] Allowing EMIs to diversify their funds over commercial bank deposits, high-quality liquid short-term securities, and central bank reserves may provide diversification benefits.

Country-specific elements need be carefully considered when designing fund safekeeping requirements. Elements that should be considered in designing safekeeping (including diversification) requirements include: the size and soundness of the banking system, the availability of high-quality liquid short-term securities, the size and the relevance of the EMI sector, EMIs' risk management capacity, as well as EMIs' ability to comply with operational and risk management requirements for accessing central bank facilities.

C. Fund Segregation

Segregation of user funds is a critical element of the e-money regulatory regime. Segregation addresses the risk that general creditors of an EMI seize e-money users' funds in the event of its insolvency. Segregation is essential, regardless of other safekeeping strategies, and should be required in all e-money regulatory regimes. If e-money users' funds were commingled with the EMI's own funds, or otherwise considered part of the EMI estate, they would be distributed to general creditors in its insolvency. This could result in substantial losses for users and damage public confidence in e-money. Various legal approaches have been taken to protect users from commingling (Box 3).[8] The authorities should aim to achieve a high level of protection whichever legal approach is used. However, in the absence of specific insolvency rules, segregation does not ensure that the e-money users get quick access to their funds in the event of the EMI's failure, and this discontinuity may create problems if the EMI is potentially systemic.

D. Risk Management

EMIs should have a strong internal control framework for fund safekeeping and segregation. EMI boards should approve the risk management framework and policies for credit, market, operational, liquidity, and general business risks. The risk management function (and the audit and risk committees, if any) should monitor the compliance with and performance of these frameworks. EMIs should have written policies, operational procedures, and assigned staff responsibilities regarding internal controls to assure fund segregation and safekeeping. The internal control framework should be subject to minimum standards. Specific internal and external audit requirements regarding the reconciliation of the e-float with the liquid assets

[7] However, under Basel III, EMI deposits will be treated as "short-term unsecured wholesale funding provided by other legal entities" required to be covered 100 percent by high-quality liquid assets.
[8] Fund segregation is also relevant when funds are deposited in a central bank reserve account.

Box 3. Mechanisms for Segregating E-Money Users' Funds

There are several techniques to achieving segregation or ring-fencing of users' funds against claims from EMI creditors. These recognize the users' proprietary interest, so that users are entitled to restitution of their funds, instead of just holding unsecured claims on the EMI's assets. Mechanisms include:

- **Trusts**: EMIs may be required to establish a trust under which legal title in the property is transferred to a trustee (the person who administers the trust), who holds the assets on behalf of the beneficiaries (the e-money users). Considering that (1) beneficiaries and their balances are continuously varying and (2) the trustee has very limited discretion in managing the assets, the trustee's role is limited to maintaining the ring-fencing of the funds, rather than the typical functions of a trustee, who manages the trust assets for the benefit of the beneficiaries. The main element of the trust that EMIs use is the separation of ownership of user's funds from the settlor and trustee's assets, avoiding that those funds are seized by EMI creditors. The trust would not protect per se against misuse of customer funds as the trustee (if separate from the EMI) would not perform any oversight over the EMI and its management and accounting of user funds. The trust mechanism is used in numerous common law jurisdictions, but it can also be used in civil law countries: Afghanistan, Bangladesh, Jamaica, Kenya, Lesotho, Liberia, Malawi, Myanmar, Namibia, Rwanda, Tanzania, the United States (where EMIs are regulated at the state level), and Zambia are among the countries in which trusts are used in this way.
- **Fiduciary contracts**: In certain civil law jurisdictions, fiduciary contracts can be used to achieve similar results as trusts. Through fiduciary contracts, the EMI sets aside the users' funds with the legally authorized fiduciary, which commits to give them a specific purpose, such as returning the funds to the e-money users in case of the EMI's insolvency. This legal technique has been enshrined within the e-money framework of Latin-American countries, and to a lesser extent in francophone sub-Saharan Africa. The extent to which customer funds will be protected in the event of the insolvency of the fiduciary varies significantly and will depend on the scope that fiduciary contracts have in each jurisdiction.
- **Escrow accounts**: Escrow accounts are frequently used in business practice and some regulated activities to protect funds that are earmarked for a particular purpose (for example, a real estate payment). A specially designated account for users' funds will help distinguish the provider's own funds from those delivered by users and can protect the rights of users in the event of providers' insolvency. In India, for instance, nonbank prepaid payment instrument providers must back 100 percent of their obligations with a noninterest-bearing escrow account maintained with a licensed commercial bank, on behalf of their customers. Under the Indian legislation, the float deposited in the escrow account is immune from the powers of the liquidator, or from creditor action, in the event of the insolvency of the prepaid payment instrument provider or the payment bank.
- **Legal provisions**: Some countries (Brazil, Chad, and the Philippines) have introduced specific provisions in legislation to protect users' funds. The risk posed in the event of an EMI's insolvency in countries that lack legal instruments similar to trusts, or just want to provide more protection, has led them to apply specific legislative provisions. A direct provision in the law stating that the funds delivered by the users to an EMI are deemed separate from the EMI's assets, and therefore cannot be seized by the EMI's creditors, may fulfill that purpose. To operate effectively, the legal provision needs to be accompanied by a clear identification of the users' account.

should be required. The effectiveness or measures to protect user funds relies on the reconciliation of the e-float with the pool of liquid assets. EMIs must have constantly updated data on the identity of users and their e-wallet balances. EMIs need to be able to reconcile the total e-float with the segregated pool of liquid assets. There appears to be wide variation in reconciliation procedures across EMIs (CGAP 2018b). Ideally the reconciliation should be done in real time. However, practices vary greatly, ranging from highly manual (for example, an EMI staff calls the bank at the end of each day

to increase/reduce the balance in the account in which customer funds are deposited) to entirely automated (for example, the float account is adjusted automatically once or several times daily, that is, batch, or even in real-time).[9]

Operational risks may trigger the unavailability or loss of client balances. Internal and external fraud and business continuity risks—as a result of cyber risk, physical damage to buildings and equipment, and IT problems—are significant risks that could result in the (temporary or permanent) loss of client funds and/or failure of the EMI. Given the similarity of issues—and working from the principle of same activity, same risk, same regulation—operational risk management requirements should, in principle, be similar to those of banks (BCBS 2011) and payment systems (PFMI Principle 17). Minimum requirements should cover operational risk governance and management frameworks, outsourcing, fraud prevention, data and cybersecurity, business continuity, and disaster recovery. Where relevant, EMIs should have an adequate control framework for agent network management and monitoring, including for anti-money laundering and countering the financing of terrorism (AML/CFT) and consumer protection issues. Agents need to be properly screened, trained, and monitored to avoid the misuse of financial services (including fraud) and ensure protection (for example, disclosure of fees, no offline transactions, etc.), and liability rules need to be in place to make the EMI legally responsible for the agent's actions.

EMIs should be subject to regulatory requirements that promote the integrity of the financial system. They should be proportionate to the type and risk of activities and cover, among other aspects:

- Fit-and-proper requirements for direct and indirect beneficial shareholders, the board and senior management of an EMI (and, if applicable, the trustees)
- Market conduct and consumer protection regulation (Box 4). Clear disclosure requirements regarding the fee structure and the mechanisms for handling complaints should be incorporated in e-money regulation. A key disclosure that may need more emphasis and be consistently communicated to market participants, is the extent to which the customer funds are covered (or not) by deposit insurance. A few recent examples of EMI failures have indicated that customers may be unaware that their funds may not be covered (Chapter 5). To limit customers' exposure to EMIs, some jurisdictions impose limits on balances and the size of transactions users can make. While they may help to delineate e-money from bank deposits and limit the absolute losses users can incur, if it still represents a substantial portion of users' disposal funds, or if a large portion of the population depends on the services, they may not prevent an adverse macro-financial impact in the failure of an EMI.[10]

E. Minimum Capital Requirements

Most jurisdictions apply nominal statutory capital requirements. All EMIs in the sample of jurisdictions reviewed must meet statutory minimum requirements for licensing (on an ongoing basis) that are significantly lower than those for banks. Capital requirements should be seen as a barrier to entry to less serious investors, and so far have not played a role in limiting e-money development. The minimum statutory capital should ensure that investors have initial capital to undertake the proposed activities, as a new firm will have significant initial costs, and experience has shown that it may take a while for the business to break even. Thus, the EMI should be able to absorb startup losses and meet the cost of nonproductive assets. Depending on the business model and potential systemic significance of EMIs, complementary risk-based capital requirements may be considered. Even in case of effective segregation (and assuming that reconciliation takes place in real-time), customer funds are still subject to credit (for example, if deposited in a bank), market (if invested in securities), and operational risks (including internal and external fraud). The Basel framework and resulting risk-based capital requirements could be a model, but it would need to be simplified and made consistent with the business model of EMIs (in particular, in the absence of lending). More work is needed in this regard, in particular in the context of developing a comprehensive regulatory and supervisory framework for potentially systemic EMIs.

[9] Generally, jurisdictions require that the reconciliation between the e-float and users' aggregate balances takes place at least once a day, before the bank closes (24/7 processing is not yet possible in many jurisdictions).
[10] Limits might also be relevant for a risk-based approach to AML/CFT.

Box 4. Consumer Protection and e-Money Services

E-money services have become increasingly complex, increasing consumer protection risks. Consequently, financial consumer protection plays an increasingly salient role. Mobile money issuers have grown from offering prepaid e-money transfers to low numbers to providing increasingly sophisticated services to millions of active users. Legislators of 102 different countries were reported to have enacted laws to cater to specific risks faced by consumers using e-money, and 73 jurisdictions have enacted regulatory frameworks for nonbank EMIs. Guidance for the protection of e-money users can be found in documents by the World Bank/BIS (joint guiding principles and key actions), the G20/OECD (high-level principles of 2011 and 2015 and their associated policy guidance), the Global System for Mobile Communications (principles), the Better than Cash Alliance (guidelines), and the Consultative Group to Assist the Poor (regulatory enablers). Apart from the protection of user funds (covered in Chapter 5), the following high-level principles can be identified:

- **Disclosure and transparency**: E-money users may need special forms of disclosure that require more clarity than other banking services, especially given that individuals using e-money may be inexperienced with financial services. Examples include the duty to disclose transfers to and from the e-money account; simple language in contract documentation; and more clarity on fees, including those applicable to the redemption of e-money.
- **Business conduct rules for authorized agents**: This principle is extremely relevant for those e-money operators that have achieved market penetration thanks to their extensive network of agents. Guaranteeing appropriate behavior of agents and compliance with all obligations represents a challenge, as the network of agents can be complex. Best practices include publishing the list of authorized agents and establishing the liability of the EMIs by agents' actions, including for unlawful actions.
- **Protection of consumer data and privacy**: The data used for e-money transactions may reveal sensitive information, such as spending patterns or types of services or products acquired by users and should be adequately protected. Users should be aware and agree to data dissemination, for example, within a larger Big Tech group, and best practice would include liability accruing to the EMI for data breaches and improper use of information.
- **Complaints handling and redress**: In many developing countries, e-money users represent more vulnerable members of society, and it is critical that mechanisms for complaints handling and redress are accessible and affordable. These mechanisms should not impose unreasonable cost, delays, or burdens on consumers. Best practices include requiring out-of-court mechanisms for redress.
- **Competition**: In the case of EMIs, the existence of powerful network effects may result in de facto monopolies that, in turn, could create situations of abuse of dominant market power. To avoid the exploitation of such network effects, several jurisdictions have imposed interoperability requirements, as well as prohibited exclusivity clauses in agent contracts. Requirements for interoperability of networks and allowing agents to operate on a nonexclusive basis increase competition and benefit users. Providing other market participants access to customer data (on a consent basis) by applying open banking data sharing principles to EMIs could also be relevant to stimulate competition.
- **Service provision**: EMIs should provide reliable and convenient access to their services. Convenient access requires technological capacity and an extensive network of agents that operate at convenient hours. Some regulators have required minimum working hours, and there should be back-up mechanisms to ensure quick recovery of access to funds and services in case of IT problems.

F. Supervisory Approach

The effective implementation of the regulations should be supervised through a mix of off- and on-site work. The supervisory approach and the intensity of supervision should be risk-based, that is, proportionate to the risk profile of the institution/group and its systemic importance. Large EMIs should be expected to have more advanced risk management and internal control standards and systems in place. EMI's risk management and reconciliation policies and procedures are key elements to be understood and reviewed by the supervisor. To allow for effective offsite supervision, key metrics should be periodically reported. Some regulators have required EMIs to provide offsite access to the system (viewing rights) to be able to monitor on a daily basis the e-float balance and the daily reconciliation with the pool of liquid assets. More intensive and real-time monitoring would be particularly important when the EMI sector or individual EMIs are relevant from a financial stability or financial inclusion perspective. EMIs that are part of financial or mixed conglomerates should be brought within the scope of consolidated and cross-border supervision following the same principles as laid out in the Joint Forum's principles.[11]

[11] BCBS Joint Forum (2012).

4. Payments System Oversight for E-Money

The Principles for Financial Market Infrastructures (PFMI)[12] provide a benchmark for oversight of e-money as a payment system. These standards aim to enhance safety and efficiency in financial market infrastructures and, more broadly, to limit systemic risk and foster transparency and financial stability. The application of the PFMI to e-money within the broader oversight of payment systems is at an early stage. However, as EMIs and their inter-connections with other parts of the financial system grow, the application of the PFMI to EMIs is likely to become more relevant and should be integrated into a regulatory framework for EMIs and the oversight framework for payment systems.[13] The prudential approaches outlined in Chapter 2 are broadly compatible with the PFMI and could be built on to develop a proportional oversight approach to EMIs. The governance body of e-money payment schemes should take measures to maintain confidence and mitigate risks associated with the exposure to legal, business, operational (including security and cyber), interdependencies, and financial risks. Some jurisdictions have already started the effort to integrate the regulation and supervision of EMIs into an overall payment system oversight framework. For example, the Eurosystem's single oversight framework for electronic payment instruments, schemes, and arrangements (PISA framework) proposed the application of 16 principles from the PFMI for schemes that handle electronic payment instruments such as e-money (ECB 2020), although the payment schemes/arrangements are not designated as systematically important payment systems (Annex 3).

Access to regulated payment systems and central bank facilities could be considered for potentially systemic EMIs. There are potential benefits to broadening access to regulated payments systems and central bank accounts to allow EMIs to settle in central bank money, increasing the safety and efficiency of settlement. This could help reduce the operational risks arising from tiering of access, foster financial innovation and competition, and ensure interoperability (CPMI and World Bank 2020). It would remove the risk of insolvency of a settlement agent and mitigate disruption risks, in the case of EMIs settling bilaterally, through private settlement services (Khiaonarong and Goh 2020). It could also enhance payment system oversight by ensuring appropriate and consistent rules for clearing and settlement of e-money, as well as potentially reducing transaction fees, increasing transparency, and user convenience (Khiaonarong and Goh 2020). While some central banks allow nonbank payment service providers access to a settlement account, most require EMIs to be licensed banks or payment banks (Table 2). This includes jurisdictions that introduce special purpose payment bank licenses (for example, India,[14] Nigeria). In jurisdictions where access is granted, services are restricted to settlement accounts without credit facilities (including intraday).

[12] Issued by the Committee on Payment and Settlement Systems and the Technical Committee of the International Organization of Securities Commissions.

[13] Annex 2 provides payment statistics of e-money/mobile money payments relative to other types of retail payment instruments in selected jurisdictions.

[14] For India, e-money is issued not only by payment banks but also by authorized nonbank payment system providers.

Table 2. Nonbank EMI Access to Central Bank Account Arrangements

	Direct Access to Settlement Account	Direct Access to Credit Facilities[1]
AFRICA		
Ghana	×	×
Nigeria	×	×
LATIN AMERICA		
Colombia	√	N/A
Mexico	×	×
ASIA		
India	√	×
China	√	×
Philippines	×	×
Malaysia	×	×
EUROPE		
European Union	×	×
United Kingdom	√	×
Switzerland	√	×
NORTH AMERICA		
Canada	×	×
United States	×	×

Source: Central bank websites; and IMF staff.
[1]Including intraday lending.

5. User Protection and Contingency Planning

Authorities should consider additional arrangements to protect users in the event of a potentially systemic EMI and/or its custodian bank failing. EMIs can fail and put customer funds at risk (for example, Celpay in Zambia in 2014). The loss of user funds can be triggered by the failure of the EMI and/or the commercial bank(s) in which user funds are deposited. As discussed above, segregation offers protection to users against certain risks, but it would not protect against the temporary loss of funds until the liquidator (and trustees, if pertinent) made them available again, or the loss of the e-money services if the services of the failed EMI were non-substitutable. It would also not protect against losses if the commercial bank, in which the funds were deposited, were to fail. These funds would be treated as part of the insolvency estate of the failed bank and users could incur losses and with any potential recoveries only accruing after significant delay). Depending on the importance of the EMI from a macro-financial perspective, additional user protection measures may be warranted. This section considers the pros and cons of different approaches, including with respect to deposit insurance and contingency planning.

A. User Protection

Advanced economies typically do not use deposit insurance to protect e-money users. Given ample opportunities to use the formal financial sector, including mobile banking and credit cards, users in these countries mainly use e-money for specific payment transactions and maintain relatively small balances (as a portion of their disposable funds). In well-banked economies, there is less incentive for the authorities to extend deposit insurance, as consumers can use insured deposits at supervised banks to store savings, and the macro-financial risks of the loss of e-money services are relatively low, given the ready substitutability of alternative service providers. In addition, the restrictions on use of the e-money funds (Chapter 3) means that users' balances are less exposed to credit risks than bank deposits.

For developing countries and emerging market economies wherein e-money plays a significant role, authorities have sought to extend deposit insurance through:

- **The indirect approach:** This approach is sometimes called "pass-through" protection and seeks to prevent users from the failure of the bank holding their funds. It does not protect users from losses caused by failure of the EMI (for example, fraud) or a loss of funds invested in other assets.[15] As such, it would not be relevant in regimes where the e-float is held at the central bank for example. Under the indirect approach, EMIs' user funds are held in pooled trust or custodial accounts at banks that are insured by the deposit insurance system (DIS). The beneficiaries of the trust accounts (the e-money users) receive deposit insurance protection for the funds held on their behalf by the EMI at a bank if the accounts fulfill special eligibility conditions for coverage (Box 5). Among others, the DIS must recognize custodial or trust accounts—wherein the custodian holds the deposit for a beneficiary—and apply the insurance coverage to the individual beneficiaries (so-called pass-through coverage). The trustee must be able to disclose the identity of, and the amounts owed to, each beneficiary—to the bank and ultimately the DIS. Banks are levied on the deposits in the float account according to DIS rules.

- **The direct approach:** Some authorities (Box 6) have included e-money in the definition of insured deposits and licensed EMIs (in the form of so-called payment banks or niche banks) as members of the DIS.[16] This approach seeks to protect e-money users from the failure of the EMI. This could, for example, be triggered by the loss of user funds due to fraud or due to the failure of a bank in which the e-float was deposited. As DIS members, these institutions are subject to DIS regulations and pay deposit insurance levies. Requiring legally independent entities to act as licensed and supervised EMIs may have additional advantages for user protection:

    - It helps to segregate user funds, for example, only a subsidiary would be permitted to hold user funds to which the parent/mobile network operator (MNO) would not have direct access.

[15] Countries that apply the indirect approach include, among others, Jamaica, Kenya, Malaysia, Nigeria, Rwanda, WAEMU (consisting of eight countries), and Zimbabwe.
[16] Countries that apply the direct approach include Bangladesh and Colombia. India has direct coverage for eligible deposits mobilized by payment banks, while prepaid payment instruments are not covered under deposit insurance.

- The firm would be supervised by the financial regulator instead of, for example, a telecommunication regulator in case of an MNO, which has no special capacity or knowledge of supervising financial service providers.
- EMIs would become directly subject to DIS membership obligations, such as paying levies and recordkeeping requirements (with on-site verification).

Recordkeeping requirements are of critical importance under both approaches but may create additional challenges under the indirect approach. EMIs must be able to deliver the relevant data for the identification of users and their individual balances within a short timeframe (for example, 24 hours) to enable rapid verification prior to reimbursement by the DIA. For pass-through coverage to be workable in practice, three-way sharing of information among the account holding bank, the EMI, and the DIA is required. Customer records and IT systems need to be in place that allow the firm to identify which customer funds it holds without delay. These records should enable the DIA and/or the liquidator to distinguish customer funds from the firm's own funds, and funds held for one user from the others. Such identification would need to be verified and tested regularly by the regulator and DIA. In addition, it should be subject to annual audits. The recordkeeping arrangements, and the oversight needed by the deposit insurer and/or supervisor to ensure that are in place, if done properly could entail significant costs.[17] However, under the indirect approach EMIs may not be subject to the recordkeeping requirements (such as single customer view) of the DIS (Table 3). Consequently, it appears that, in practice, customer information usually remains solely with the EMI and is not shared on a regular basis with the bank or the DIA for verification. In its absence, the DIA would be unable to verify users and quickly reimburse insured deposits or would need to consider making payment for the full e-float balance held at the failed bank, exposing the DIS to the risk of reimbursing uninsured e-money users.

Challenges also pertain to operationalizing deposit insurance if the EMI were to fail. The premise of indirect deposit insurance is that in the event of bank failure, funds are quickly reimbursed to the EMI before it fails because of illiquidity. This process puts significant pressure on the DIA to have the operational capacity to fulfill this task in a matter of hours or days or the EMI may fail. Under direct deposit insurance the trigger for payout is the failure of the EMI after which its systems may no longer be operable and available to be used to reimburse users. In such circumstances, conventional methods for deposit insurance payouts may not work for e-money reimbursements, especially in developing countries. DISs usually rely on a payout of deposits via balance transfers to other banks (so-called "paying agents"), to directly reimburse depositors. Users of e-money in developing countries may be unbanked and reside in areas with little-or-no bank branch network that could be used to effect reimbursement. Low transaction balances may be cumbersome to reimburse and raise cost and efficiency challenges. If a substitutable service provider exists, the DIS could use the e-money system to compensate users by transferring funds to an e-wallet, which users may have (or could open) with another EMI. As part of resolution planning, the authorities could develop strategies for substitutability and require interoperability. In a scenario where the EMI were to fail and its services were not substitutable, the authorities might need powers to keep the systems of the failed EMI operational and gain control to allow for compensation to be paid via the failed EMI's platform.

Table 3. Comparison of the Direct and Indirect Approaches

	Direct approach	Indirect approach
DIS membership of the EMI	*Yes*	*No*
EMI subject to DIS rules on recordkeeping	*Yes*	*No*
Obligation of the EMI to pay levies to the DIF	*Yes*	*No*
E-money defined as eligible deposits	*Yes*	*No*
Need for IT systems able to track e-money balances	*Yes*	*Yes*
Pooled funds or float held in trust/custodial accounts	*Not required, but recommended*	*Required for pass-through coverage*
Protects against	*Loss caused by failure of the EMI*	*Loss caused by failure of the bank(s) holding the EMI's e-float*
Source: IMF staff.		

[17] While several DIS recognized custodial or trust accounts before e-money, these are often used for a small number of beneficiaries with relatively stable balances (for example, notary accounts), which can be easily identified through the bank's IT system. EMIs use trust or custodial accounts as pooled or omnibus accounts for many users whose fund balances fluctuate regularly, making it much harder and more costly to track in real time.

Box 5. Legal Changes to Implement the Indirect Approach Effectively

An e-float account with a bank would typically not be materially covered by deposit insurance without legal changes to allow for it. It is a deposit by a commercial entity, for example, an MNO, while DIS protection may apply only to individuals and some corporates (for example, small- and medium-sized enterprises). Or it may be considered as a deposit by a financial firm (if EMIs would qualify as financial firms), which are typically ineligible for DIS protection. Where eligible, the deposit insurance limit applying to the float account would not be material, as it would only apply to the aggregate balance. Some jurisdictions (for example, Jamaica, Kenya, Nigeria, Rwanda) allow insurance coverage to "pass through" the nominal account holder and reach the ultimate beneficiary, that is, individual e-money users' balances held in the e-float if certain country-specific requirements are fulfilled.

The following specific requirements concerning the pass-through approach can be observed:

- The DIS law must recognize the existence of custodial or trust accounts and apply the coverage level to the individual beneficiaries and not to the account holder.
- A custodial/trust agreement needs to be in place between the party placing the funds and the beneficiaries (that is, the e-money users) to formalize the relationship.
- The float account must be clearly identifiable as an account created for the funds delivered by e-money users. To do this, the custodial/trust relationship must be disclosed to the bank and recorded in the depositor records of the insured institution (for the DIA to identify the accounts in the case of failure). If a trustee fails to disclose the beneficiary information, or the bank has not identified the account as a trust, it would be treated as a normal deposit and the coverage limit applied to the aggregate amount, effectively voiding the deposit insurance for individual users.
- The identities and individual interests of the users (beneficiaries) should be disclosed in the records of the institution or in the records maintained by the custodian or third party, such as the EMI or a service provider. If this information is unavailable in the bank's records, it must be made available to the DIA upon the bank's failure.
- If the EMI uses more than one bank to deposit the float, a rule should exist to determine how user balances relate to individual bank accounts ex ante of any failure. For example, by assuming that when a customer's funds are commingled in the float account with other customers' funds, and a portion of the overall float is deposited in one or more banks, the customer's insured funds in any of the banks would represent the same fractional share as their share of the total float.
- E-money user funds should not be subject to aggregation with deposits held by the same person in the same bank, as the user would typically be unaware about location of the placement by the EMI.
- Legal changes would be required, and operational capacity developed, to enable the DIA to make users' funds available to the EMI on behalf of its customers (the insured depositors) in a custodial account in another bank within a short timeframe to maintain the matching requirement of liquid assets and the e-money issued. After the users' funds have been made available, the customers should have no claim against the DIS.

Box 6. The Arrangements for Direct Protection in Colombia

In 2012 Colombia created a new deposit category of "electronic deposits" eligible for deposit insurance through the national DIS (FOGAFIN), originally limited to credit institutions (banks, financial cooperatives). In 2014 Colombia created a new type of regulated, specialized financial institution offering electronic deposits and payments (SEDPEs). SEDPEs are allowed to carry out a subset of the activities permitted to banks. They can (1) accept electronic deposits, (2) make payments and money transfers on behalf of clients, (3) borrow domestically or internationally to finance their operations, and (4) issue or cash money orders. They are not allowed to offer intermediate funds or offer credit. Balances of individual customers are subject to transaction limits (about US$780). Deposit accounts offered by SEDPEs can offer interest.

Electronic deposits enjoy the same coverage per person and per SEDPE as bank deposits (currently Col$50 million or US$13,300). However, since the individual balances of eligible depositors are limited by law, all eligible deposits held by SEDPEs should be fully covered in practice. SEDPEs are required to place customer funds either at the central bank or with commercial banks, with funds equivalent to their e-money liabilities. When placed with commercial banks, customer funds are eligible for pass-through deposit insurance, which is particular to the Colombian regime. SEDEPEs are required to register as members with the DIS, but since their business model is less risky than that of commercial banks, due to their limited activities (no intermediation of funds), SEDEPEs pay a lower premium. SEDEPEs are required to make depositor information available to FOGAFIN in a format and timeframe prescribed by the deposit insurance agency (DIA). In case of a liquidation, the liquidator must hand over these data to FOGAFIN within five days. The DIA would directly reimburse electronic deposits that qualify as insured deposits if a SEDPE fails and indirectly cover mobile deposits deposited by the SEDPE with a commercial bank if it were to fail.

B. Contingency Planning

Contingency planning should be prepared for the failure of a potentially systemic EMI and/or the failure of the bank holding the e-float. While non-systemic EMIs could be liquidated under applicable procedures, contingency plans for potentially systemic EMIs should address both risks and aim to ensure the continuity of critical e-money services. Significant service interruptions could have a critical impact on the e-money system, with macro-financial spillovers. In a bankruptcy of the EMI, if segregation requirements have been observed these funds should be separated from the estate of the failed company and returned by the trustee in cooperation with the liquidator to users.[18] However, there may be a significant delay in the recovery of funds due to verification and operational reasons, if both liquidator and trustee are not operating under an objective to return these funds quickly to safeguard financial stability concerns and may not have the operational capacity to refund individual customers. In a bank's failure and without deposit insurance for the e-float in place, the speed of recovery of customer funds will depend on the liquidator's ability to identify the funds and its beneficiaries and realize asset recoveries (which can take years). Without quick access to the funds, the EMI would fail when users cash out their balances.

One way to ensure continuity of systemic EMI services could be to transfer the contracts and user funds from a failing EMI to an alternative service provider. This would, however, require a special legal regime for EMI failure, assigning transfer powers to a public authority or a special administrator, as otherwise its accounts would be frozen in bankruptcy and its IT systems would not be maintained.[19] EMIs are currently not usually subject to such regimes; instead, ordinary corporate insolvency proceedings typically apply. In addition, this would require that EMIs have IT platforms interoperable with other payment providers and mechanisms to allow for the transfer of accounts in bulk and integration of a large number of new users. Authorities would need to assess whether the failure of a large EMI, dominating a market in which its competitors are much smaller, could pose technical challenges for the absorbing entity due to limitations in scaling up the number of customers and accounts. Should a role for the DIS be foreseen to fund this transfer (comparable to a paybox plus mandate) this would require a number of safeguards, including that the costs for the DIS would be no higher than in a payout (least-cost rule). In

[18] The risk that the provider may misuse customer funds, for example, through fraud or by pledging them as collateral to obtain loans from third parties or comingling them with its own funds still exists. If the funds are insufficient, the users should share the loss proportionately.
[19] See UK Payment and Electronic Money Institution Insolvency Regulations 2021.

the absence of other options, temporary public support may need to be considered for a potentially systemic EMI as part of contingency planning for a worst-case scenario.

Requiring EMIs to undertake stress tests and establish wind-down plans would strengthen contingency planning. The United Kingdom requires EMIs to carry out stress testing and prepare wind-down plans proportional to the nature, size and complexity of the firm's business and the risks it bears to analyze their exposure to a range of severe business disruptions and to assess their impact on the firm. Supervisors could use such tests to improve resilience, in particular, to strengthen liquidity and capital resources as well as business systems and controls. Contingency plans that identify critical IT systems, people, data, financials, and necessary funding to cover operational expenses would inform the firm and the regulator on how to preserve critical functions in a failure. Wind-down plans should include solvent and insolvent scenarios and contain triggers and information for the liquidator to enable quick identification and return of customer funds as a priority.

6. Recommendations

All EMIs should be subject to proportionate prudential regulatory requirements. Supervision should be proportionate to risks and forward looking to ensure evolving business models are covered. E-money regulatory regimes should cover the following[20]:

- The legal, governance, operational, and ownership structure;
- Rules for safekeeping and segregation of user funds;
- A prohibition on retail lending;
- Minimum capital requirements;
- Minimum requirements for operational risk governance and management, outsourcing, fraud prevention, data and cybersecurity, business continuity, and disaster recovery;
- Fit-and-proper requirements for direct and indirect beneficial shareholders, the board, senior management, and trustees;
- Market conduct and consumer protection rules;
- A framework for controlling AML/CFT risks and managing and monitoring the agent network (where pertinent); and
- Standards for payments system oversight that ensure safety and efficiency.

Depending on the business model of EMIs particularly if they become potentially systemic, authorities should enhance prudential oversight and user protection arrangements (Figure 1). Supervisory arrangements—intensity of supervision and supervisory expectations regarding governance, risk management and internal control standards and systems—should be strengthened for potentially systemic EMIs. In addition, a systemic EMI warrants enhanced oversight to ensure the safety and efficiency of payment services and protects users. This should be akin to the degree of oversight applied to other systemically important retail payment systems, such as automatic clearing houses used for interbank transactions. Where responsibilities for prudential supervision, market conduct supervision, and payment oversight of EMIs reside in different authorities, licensing and supervision should be careful coordinated to limit overlaps and minimize the regulatory burden and arbitrage. Interagency coordination with the telecom regulator may also be relevant in the case of mobile money. Like other financial institutions, EMIs that are part of financial conglomerates (for example, that include banking, insurance, and/or securities activities) or mixed conglomerates, for example, that include different financial as well as nonfinancial activities should be included in the scope of consolidated and cross-border supervision. The supervisory approach should be risk-based, that is, proportionate to the risk profile of the institution and its systemic importance, and entail a mix of off- and on-site supervision. An EMI's risk management and reconciliation policies and procedures are key elements to be understood and reviewed by the supervisor. To allow for effective offsite supervision, key metrics should be reported periodically. Some regulators have required potentially systemic EMIs to provide off-site access to the system (viewing rights) for daily monitoring of the e-float balance and daily reconciliation with liquid assets. However, authorities will need to carefully assess the potential cost impact and ensure that the measures support the safe use of innovative technologies and are proportionate to the risks.

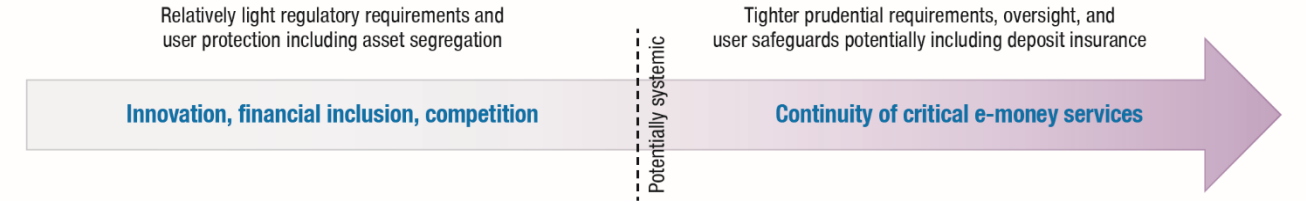
Arrangements for user protection should also be strengthened if EMIs have become potentially systemic. Jurisdictions that rely mainly on conventional banks and/or credit cards for payments may decide, with good reason, to not extend further protection. In countries where an EMI or the e-money sector has become potentially systemic, additional arrangements for user protection should be considered. The user protection mechanisms should seek to preserve users' funds and ensure continuity of critical payments services, with user access and services restored quickly (preferably within hours, or at most a couple of days). Before e-money is added to the scope of an already-established DIS for banks, the impact on the adequacy of DIS funding should be assessed. While in theory EMIs could establish separate insurance schemes, there may be insufficient EMIs to mutualize the risk and, to date, no such schemes have been established. While e-money accounts could be subject to the same coverage level as bank deposits, a lower coverage for e-money balances could help distinguish

[20] Consideration could also be given to transaction limits to delineate e-money from bank deposits.

transactional balances in an EMI from saving in bank deposit accounts. For example, the DIS in the West African Economic and Monetary Union (WAEMU) applies a lower coverage level (IADI 2020).

Figure 1. Regulatory Requirements Should Be Strengthened as EMIs Grow in Importance

As policy objectives (text in blue) change in line with the importance of EMI to the economy, regulatory oversight should be strengthened.



Source: IMF staff.

Operationalization of deposit insurance for e-money remains challenging in practice and untested thus far. Under both approaches, authorities should assess the DIS's capacity to deal efficiently with such institutions for payout purposes and cost implications for EMIs to comply with record-keeping requirements. DIAs should regularly test EMIs' and banks' capacity to provide the necessary data in the prescribed timeframe and verify its accuracy. To support the DIA's information-gathering needs, trustees, EMIs, and their agents should be obliged to cooperate with the DIA. The DIA[21] or the supervisor of the EMI should have the power to issue binding record-keeping requirements. Additionally, third parties should be required to include in their contractual arrangements (for example, the trust deed, fiduciary contract, and service-level agreements) provisions on timely and accurate data provision to the authorities. If the DIA is unable to perform onsite visits at EMIs, it should use its member banks to indirectly test EMI compliance. During an onsite visit of the supervisor or DIA, the bank could be requested to provide the data from the EMI needed to identify insured deposits for data quality and compliance checks. In addition, the compliance of the EMIs' IT systems with customer data requirements should be subject to annual audits. These requirements may have an adverse impact on EMI's low-cost business models.

Direct deposit insurance offers greater protection for e-money users at a cost, and indirect deposit insurance may raise consumer protection issues. Before extending direct deposit insurance, EMIs should be subject to regulation and supervision and should be established as a separate legal entity dedicated to the payment function. Under this approach, EMIs become directly subject to the DIS membership rules and obligations and would pay deposit insurance levies which may impact on financial inclusion benefits. Direct coverage would protect e-money users from losses caused by failures of the EMI (including if this were due to loss of its bank deposits) and may help to prevent runs on the EMI.[22] Indirect coverage only protects against the failure of the bank holding the float, but not if user funds are misused. This critical distinction may be unclear to e-money users, raising significant consumer protection and reputational issues for the DIS in such circumstances. Accordingly, public awareness issues need to be prominently addressed. Clear rules should specify EMI obligations to inform their users about the benefits and limitations of deposit insurance, including the coverage level and types of losses covered (and as applicable differences from bank deposit insurance coverage). Regulators should ensure that users are made fully aware that deposit insurance under the indirect approach only protects against the risk of the failure of the bank holding the float, but not in the case of losses caused by failure of the EMI, for example, due to fraud at the EMI or a loss or breach of the e-wallet.

EMIs should not purport to be covered by deposit insurance without adequate operational arrangements to ensure that the reimbursements can be effected quickly. It is unclear whether these arrangements are currently in place in many regimes that purport to offer deposit insurance. If the DIA were to be unable to reimburse e-money users quickly, this could risk undermining confidence in the payment system and, potentially, lead to a loss of confidence in the DIS more widely. Oversight should be put in place to ensure compliance with data requirements and payout mechanisms. Should concerns exist that the DIS is unable to efficiently protect EMI users' funds, a requirement to keep these funds with the central bank,

[21] IADI Core Principle 15.

[22] Even in cases where user funds have been properly segregated, the DIS may play a crucial role in the failure of the EMI, as it may compensate users before the segregated funds could be released and a way found to return them to individual e-money users.

instead of with commercial banks, may make sense. This approach could also be considered in countries without a DIS. Conventional methods for reimbursing depositors may not work effectively for e-money users in developing countries, given their unbanked customer base, in the event of the failure of the EMI. Additional powers in liquidation may be needed to enable the transfer of the users' e-money balances, and the underlying custodial/trust account, from the failing EMI to another EMI or to allow for the continuation or rapid restoration of the failed EMI's platforms in cases where the services were not substitutable, and the EMI were of macro-financial importance to facilitate the return of customer funds.

Annex 1. E-Money Issuance—Specific Risks

General business risk: any potential impairment of the financial condition (as a business concern) of an EMI owing to declines in its revenue or growth in its expenses, resulting in expenses exceeding revenues and a loss that must be charged against capital. These risks arise from an EMI's administration and operation as a business enterprise.

Legal risks: the risk of losses, following legal uncertainty. For example, when the liability toward customers in case of transaction failure is subject to uncertainty. It may include claims against the EMI for failing to comply with laws, as well as providing legal protection of customer funds that are pooled in trust accounts. Legal risk may also arise if multiple laws and authorities are involved, creating potential inconsistencies and legal uncertainty (Khiaonarong 2014).

Governance risks: the risk of losses following a lack of good governance and internal controls, for example, the lack of a trust board, the absence of good oversight by the trust board, inadequate governance of the risk management and treasury functions, or general absence of proper oversight by the board.

Operational risks: deficiencies in information communication and technology systems or internal processes and policies, or external events, cause disruptions to the e-money platform of the EMI, the connections to banks and agents, or the telecom network, which result in a reduction or unavailability of the EMI's services. Disruptions can occur in the EMI's own systems, as well as systems from third-party providers. The main types of operational risk are business continuity risk, cyber risk, internal and external fraud, and agent risk.

Financial risks: the risk that EMI customers lose access to the funds entrusted to the e-wallets because of (1) bankruptcy of the bank holding the customers' funds; (2) insufficient protection against the failure of an EMI, for example, because the funds have not been adequately isolated; and (3) EMIs' failure to manage the entrusted funds prudently, for example, the funds are invested in relatively illiquid assets. Risks can be subdivided as follows:

a. Liquidity risk: risk that clients' funds are not available for payout.

b. Credit risk: risk that clients' funds are invested in assets of issuers that fail.

c. Interest rate risk: risk of mismatch in interest rates between assets and liabilities.

d. Market risk: risk of loss on investments due to a fall in the value of the assets.

Money laundering/terrorism financing risks: e-money accounts and transactions may be used to launder criminals' money and/or to finance terrorist activities. Hence, compared to cash, mobile money may be considered a good tool for reducing reliance on anonymous cash, as mobile money is generally more traceable and can be subjected to requirements limiting this risk (monitoring and limits).

Consumer risk: loss of customers, or customer confidence, due to ineffective or no disclosure of key information, unfair contractual terms and conditions, product and service failures, unfair sales practices, and a lack of redress mechanisms. Data privacy risks fall under this category as well, which is the risk of potential loss of control over personal information, such as when information about a customer is used without his or her knowledge or permission, and the risk that customer information is not treated in a fair and responsible manner.

Annex 2. Basic Payment Statistics

Annex Table 2.1. Use of Payment Services/Instruments: Volume of Cashless Payments per Inhabitant[1]

				Card and e-money payments					
2019	Credit transfers	Direct debits	Checks	Total volume	By card with a debit function	By card with a delayed debit function	By card with a credit function	E-money payments	Other payment instruments
	(units)								
Argentina	8	2	2	49	24	nap	23	2	0
Australia	86	37	2	409	292	nap	118	nap	16.1
Belgium	148	46	0	210	179	16	9	6	0.1
Brazil	57	29	3	109	52	nap	48	10	nap
Canada	39	25	12	322	167	nap	154	nap	0
China	6	0	0	217	nap	nap	nap	nap	0
France	66	67	25	226	156	38	32	1	0.2
Germany	80	131	0	76	57	17	2	0	nap
Hong Kong SAR	nap	nap	nap	nap	22	nap	110	833	nap
India	14	1	1	9	4	0	2	4	nap
Indonesia	21	0	0	23	3	nap	1	20	0.1
Italy	25	16	2	77	41	nap	20	16	4.2
Japan	13	nap	0	nav	3	nap	nav	56	nap
Korea	114	33	2	458	171	nap	286	1	0
Mexico	13	1	2	31	23	nap	9	nap	nap
The Netherlands	164	85	0	294	281	13	nap	0	0
Russia	16	1	0	284	248	nap	19	17	12
Saudi Arabia	5	0	0	46	42	nap	4	nap	7.9
Singapore	26	11	8	804	101	nap	104	599	nap
South Africa	17	15	0	64	nap	nap	nap	nap	nap
Spain	31	51	1	119	83	37	nap	0	5.6
Sweden	145	39	0	360	299	6	56	0	0.1
Switzerland	124	8	nav	192	124	nap	62	7	nap
Turkey	9	nap	0	79	26	nap	52	1	nap
United Kingdom	76	67	4	337	278	6	54	nap	nap
United States	39	54	38	392	237	nap	134	21	nap

Source: BIS.
[1]Please refer to the individual country tables for a detailed explanation

Annex Table 2.2. Use of Payment Services/Instruments: Average Value of Cashless Payments per Inhabitant[1]

				Card and e-money payments					
2019	Credit transfers	Direct debits	Checks	Total value	By card with a debit function	By card with a delayed debit function	By card with a credit function	E-money payments	Other payment instruments
	(USD)								
Argentina	21,830	248	2,688	1,497	496	nap	940	62	41
Australia	205,974	88,643	14,874	18,343	9,215	nap	9,127	nap	12,789
Belgium	800,735	13,692	508	10,460	8,106	1,443	660	251	205
Brazil	63,448	6,249	1,836	2,200	807	nap	1,355	38	nap
Canada	65,740	17,390	54,642	16,890	5,154	nap	11,736	nap	9
China	279,674	5,197	13,829	80,802	nap	nap	nap	nap	289
France	434,043	29,510	14,049	10,510	6,804	2,194	1,503	10	8,077
Germany	757,156	51,340	976	4,730	3,121	1,479	119	12	nap
Hong Kong SAR	nap	nap	nap	nap	5,765	nap	12,950	3,421	nap
India	3,006	83	847	180	77	4	75	23	nap
Indonesia	9,107	–	35	214	88	nap	88	38	165
Italy	135,623	8,577	6,961	4,759	2,447	nap	1,632	679	10,696
Japan	213,190	nap	13,381	5,973	133	nap	5,341	500	nap
Korea	357,685	3,224	70,361	15,159	3,237	nap	11,906	15	358
Mexico	132,542	237	2,922	1,044	591	nap	453	nap	nap
The Netherlands	1,252,223	17,809	38	9,573	8,386	1,186	nap	1	–
Russia	85,536	241	–	6,862	6,378	nap	332	151	1,192
Saudi Arabia	375,714	6	3,049	2,211	1,909	nap	302	nap	3,467
Singapore	62,539	14,493	73,305	13,539	4,543	nap	8,611	385	nap
South Africa	35,446	2,009	164	1,570	nap	nap	nap	nap	nap
Spain	237,196	16,092	8,088	5,037	3,107	1,930	nap	–	9,283
Sweden	189,424	6,396	–	11,584	8,475	454	2,656	–	20
Switzerland	544,402	10,336	nav	12,113	6,287	nap	5,475	352	nap
Turkey	40,941	nap	1,940	2,070	276	nap	1,786	8	nap
United Kingdom	1,708,119	25,333	8,113	15,871	11,895	578	3,398	nap	nap
United States	134,550	77,725	78,479	21,905	9,193	nap	12,042	670	nap

Source: BIS.
[1]Please refer to the individual country tables for a detailed explanation

Annex Table 2.3. Number of Mobile Money Transactions per 1,000 Adults

Country	2011	2012	2013	2014	2015	2016	2017	2018	2019
Cambodia	340	354	1,369	3,832	5,815	3,332	9,137	12,945	16,884
Cameroon	11	111	81	697	1,438	6,168	21,953	39,734	nav
Chad	nav	nav	nav	2	0	1	1	nav	nav
Colombia	nav	nav	nav	nav	nav	nav	nav	3	107
Fiji	423	629	1,116	172	760	1,066	1,926	3,912	3,780
Ghana		1,135	2,503	6,751	15,468	31,170	54,207	78,299	nav
India	NA	NA	36	117	272	633	1,679	3,067	4,130
Kenya	17,655	22,700	27,944	33,607	39,741	52,647	51,513	56,210	57,528
Mozambique	nav	nav	nav	358	916	9,819	16,011	12,145	31,809
Myanmar	nav	nav	nav	0	0	1	533	954	1,653
Namibia	51	69	64	102	3,840	7,285	1,685	1,896	5,057
Nigeria		25	166	282	434	453	447	nav	nav
Pakistan	426	1,023	1,582	2,236	2,932	3,654	4,828	6,952	9,309
Philippines	2,495	2,902	3,087	4,019	4,732	5,188	5,413	5,507	8,350
Qatar	0	1	5	225	425	1,335	194	319	356
Rwanda	116	3,579	8,958	15,960	24,964	29,538	35,046	40,619	49,811
Samoa	nav	nav	808	1,324	1,579	1,585	1,608	1,219	1,404
Senegal	nav	nav	1,324	2,349	3,438	8,560	17,186	33,093	49,510
Togo	nav	nav	30	160	2,309	4,657	8,487	13,567	19,493
Tonga	5	105	167	245	808	1,450	1,508	2,005	nav
Uganda	5,117	13,644	21,733	25,983	34,884	46,985	50,089	82,865	119,950
Zambia	88	505	1,192	146	332	678	1,234	28,750	52,195
Zimbabwe	306	1,796	15,449	22,822	28,755	37,118	92,355	200,849	228,876

Source: IMF, Financial Access Survey.

Annex Table 2.4. Total Amount of Outstanding Balances on Mobile Money Accounts (In Millions of National Currency)

Country	2015	2016	2017	2018	2019
Afghanistan	200	435	707	559	696
Albania	23	36	nav	44	64
Armenia	124	302	678	1,158	1,281
Bangladesh	10,695	17,861	27,285	27,812	32,009
Botswana	44	48	81	108	142
Cameroon	4,656	22,354	53,129	90,887	nav
Fiji	1	5	2	4	1
Ghana	548	1,257	2,321	2,634	nav
Guinea	33,153	9,270	251,500	468,370	691,157
Guyana	4	14	24	19	21
India	576	3,884	14,054	26,957	31,847
Indonesia	737,786	982,360	2,421,094	4,033,008	6,142,712
Madagascar	78,068	112,514	161,483	85,241	nav
Myanmar	369	603	4,797	5,735	56,267
Namibia	5	667	15	18	28
Pakistan	8,827	11,717	21,139	23,678	28,770
Philippines	14,372	13,831	14,629	17,343	22,420
Romania	1	2	0	1	4
Rwanda	17,023	19,865	17,446	19,960	28,532
Thailand	345	596	941	1,435	2,076
Uganda	325,293	353,733	468,437	338,207	417,594
Zambia	46	96	267	874	1,218
Zimbabwe	89	130	325	542	1,830

Source: IMF, Financial Access Survey

Annex 3. Application of the PFMI to E-Money Under the PISA

As the retail payments ecosystem is constantly evolving due to innovation, as well as technological and regulatory change, the PISA framework aims to address these developments and builds on past experience in the oversight of payment schemes and payment instruments. Accordingly, its scope includes digital payment tokens (for example, stable coins), alongside "traditional" payment instruments and schemes. Another new feature is the inclusion of payment arrangements in the framework. Importantly, the PISA framework follows the principle of proportionality and aims in particular to set requirements for those entities that play a more significant role in the euro area.

The PISA framework is aimed at the governance bodies of payment schemes or arrangements, which are expected to adhere to the oversight principles. It defines criteria to identify the payment schemes or arrangements to be overseen taking into account their relevance for the overall payment system and those which are exempt. These criteria consider the size, market penetration and geographical relevance of a payment scheme/arrangement within the euro area.

The PISA assessment methodology complements the oversight principles of the framework by specifying key considerations and assessment questions. Following are the 16 applicable principles:

- **Principle 1: Legal basis.** A payment scheme/arrangement should have a well-founded, clear, transparent, and enforceable legal basis for each material aspect of its activities in all relevant jurisdiction.
- **Principle 2: Governance.** A payment scheme/arrangement should have governance that is clear and transparent, promotes the safety and efficiency of the payment scheme/arrangement, and supports the objectives of relevant stakeholder.
- **Principle 3: Framework for the comprehensive management of risks.** A governance body should have a sound risk management framework for comprehensively managing a payment scheme/arrangement's legal, credit, liquidity, operational and other risk.
- **Principle 4: Credit risk.** A payment scheme should effectively measure, monitor, and manage its credit exposures to payment service providers (PSPs) and/or end users as well as those arising from its payment, clearing and settlement processes. A payment scheme/arrangement should maintain sufficient financial resources to fully cover its credit exposure to each PSP with a high degree of confidence.
- **Principle 5: Collateral.** A payment scheme that requires collateral to manage its or its payment service providers' credit exposures should accept collateral with low credit, liquidity, and market risk.
- **Principle 7: Liquidity risk.** A payment scheme should measure, monitor, and manage its liquidity risk effectively. A payment scheme should maintain sufficient liquid resources in all relevant currencies to meet its payment obligations in a timely manner with a high degree of confidence. This should be under a wide range of potential stress scenarios that should include, but not be limited to, the default of the PSP and its affiliates that would generate the largest aggregate liquidity obligation for the payment scheme under extreme, but plausible, market conditions.
- **Principle 8: Settlement finality and crediting end users.** A payment scheme should define clear rules for final settlement.
- **Principle 9: Money settlement.** If central bank money is not used for the money settlement of the obligations of the end users or the PSPs of a payment scheme, the governance body should minimize and strictly control the credit and liquidity risk arising from the use of commercial bank money.
- **Principle 13: PSP default rules and procedures.** A payment scheme should have effective and clearly defined rules and procedures for managing the default of a PSP. These rules and procedures should be designed to ensure that a payment scheme can take timely action to contain losses and liquidity pressures and, thereby, continue to meet its obligation.

- **Principle 15: General business risk.** A payment scheme/arrangement should identify, monitor, and manage its general business risk and it should hold sufficient liquid net assets funded by equity to cover potential general business losses. This would allow it to continue operations and provide services as a going concern if such losses were to materialize.
- **Principle 16: Custody and investment risk.** A payment scheme should safeguard its end-users' assets and minimize the risk of losses on these assets or delayed access to them. A payment scheme should invest in instruments that carry minimal credit, market, and liquidity risk.
- **Principle 17: Operational risk.** Payment schemes/arrangements, PSPs and technical service providers should identify the plausible sources of operational risk, whether internal or external, and mitigate impact by implementing appropriate systems, policies, procedures, and controls. Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and the fulfilment of the obligations of the payment scheme/arrangement, the PSPs or the technical service providers, including in the event of a widescale or major disruption.
- **Principle 18: Access and participation requirements.** A payment scheme/arrangement should have objective, risk-based and publicly disclosed criteria for participation, which permit fair and open access.
- **Principle 21: Efficiency and effectiveness.** A payment scheme/arrangement should be efficient and effective in meeting the requirements of the PSPs, end users and the markets it serves.
- **Principle 22: Communication procedures and standards.** A payment scheme/arrangement should use, or at least accommodate, relevant internationally accepted communication procedures and standards to facilitate the efficient transfer of value between end users.
- **Principle 23: Disclosure of rules, key procedures, and market data.** A payment scheme/arrangement should have clear and comprehensive rules and procedures and it should provide sufficient information to enable PSPs, technical service providers and end users to reach an accurate understanding of the risks, fees, and other material costs they incur by participating in/making use of the payment scheme/arrangement. All relevant rules and key procedures should be publicly disclosed, bearing in mind those rules and procedures which, if disclosed, could pose a threat to the security of a scheme or arrangement. The latter should only be disclosed to scheme or arrangement stakeholders on a "need to know" basis.

Notes: Principles 6, 10–12, 14, 19–20, and 23 are nonapplicable for the purpose of assessing payment schemes/arrangements under the PISA framework.

Source: ECB (2020).

References

Adrian, Tobias, and Tommaso Mancini-Griffoli. 2019. “The Rise of Digital Money.” FinTech Note, International Monetary Fund, Washington, DC.

Bank for International Settlements (BIS). 2019. “Big Tech in Finance: Opportunities and Risks.” BIS Annual Economic Report. Basel.

Bank of England. 2019. Bank of England Settlement Accounts. London.

Basel Committee on Banking Supervision (BCBS). 2011. “Principles for the Sound Management of Operational Risk.” Basel.

Basel Committee on Banking Supervision (BCBS) Joint Forum. 2012. “Principles for the Supervision of Financial Conglomerates.” Basel.

Consultative Group to Assist the Poor (CGAP). 2018a. “Safeguarding Rules for Customer Funds Held by EMIs.” Technical Note, Washington, DC.

Consultative Group to Assist the Poor (CGAP). 2018b. “A Guide to Supervising E-Money Issuers.” Technical Guide. Washington, DC.

Consultative Group to Assist the Poor (CGAP). 2019. “Deposit Insurance Treatment of E-Money: An Analysis of Policy Choices.” Technical Note. Washington, DC

Committee on Payments and Market Infrastructures (CPMI). 2005. “Central Bank Oversight of Payments and Settlement Systems.” Basel.

Committee on Payments and Market Infrastructures (CPMI). 2014. “Non-Banks in Retail Payments.” Basel.

Committee on Payments and Market Infrastructures (CPMI), and World Bank. 2020. “Payment Aspects of Financial Inclusion in the Fintech Era.” Basel.

Committee on Payment and Settlement Systems (CPSS). 2001. “Core Principles for Systemically Important Payment System.”, Basel.

Committee on Payment and Settlement Systems (CPSS). 2003. “The Role of Central Bank Money in Payment Systems.” Basel.

Committee on Payment and Settlement Systems (CPSS). 2005. “Central Bank Oversight of Payment and Settlement Systems.” Basel.

Committee on Payment and Settlement Systems, and the International Organization of Securities Commissions (CPSS-IOSCO). 2012. “Principles for Financial Market Infrastructures.” Basel.

European Central Bank (ECB). 2018. *Report from the Commission to the European Parliament and the Council on the Implementation and Impact of Directive 2009/110/EC.* Frankfurt.

European Central Bank (ECB). 2020. “Eurosystem Oversight Framework for Electronic Payment Instruments, Schemes and Arrangements, Draft for Public Consultation.” Frankfurt.

Global System for Mobile Communications (GSMA). 2016. “Safeguarding Mobile Money: How Providers and Regulators Can Ensure That Customer Funds Are Protected.” London.

Greenacre, Jonathan. 2018. “Regulating Mobile Money: A Functional Approach.” Oxford.

Greenacre, Jonathan, and Ross P. Buckley. 2014. “Using Trusts to Protect Mobile Money Customers.” *Journal of Legal Studies* 59–78.

International Association of Deposit Insurers (IADI). 2020. “Deposit Insurance and Financial Inclusion: Current Trends in Insuring Digital Stored Value Products.” Basel.

International Monetary Fund (IMF). 2008. *Current Developments in Monetary and Financial Law Volume 4*. Washington, DC.

International Monetary Fund (IMF). 2020. “Chile: Technical Assistance Report – Central Bank Services to Nonbank Financial Institutions.” Washington, DC.

International Monetary Fund (IMF). 2021. “Fintech and Payments: Regulating Digital Payments and e-Money.” Financial Soundness Indicators, Washington, DC.

International Monetary Fund, Bank for International Settlement, and Financial Stability Board (IMF-BIS-FSB). 2009. “Guidance to Assess the Systemic Importance of Financial Institutions, Markets and Instruments: Initial Considerations, Report to the G-20 Finance Ministers and Central Bank Governors.” Washington, DC.

International Telecommunication Union (ITU). 2016. “Access to Payment Infrastructures, Focus Group Technical Report.” Geneva.

Khiaonarong, Tanai. 2014. "Oversight Issues in Mobile Payments.” IMF Working Paper 14/123, International Monetary Fund, Washington, DC.

Khiaonarong, Tanai, and Terry Goh. 2020. “Fintech and Payments Regulation—Analytical Framework.” IMF Working Paper 20/75, International Monetary Fund, Washington, DC.

King, Darryl, Mark Buessing-Loercks, and Froukelien Wendt. 2020. Chile—Central Bank Services for Nonbank Financial Institutions, IMF Country Report 20/160. International Monetary Fund, Washington, DC.

Mancini-Griffoli, Tomaso, Maria Soledad Martinez Peria, Itai Agur, Anil Ari, John Kiff, Adina Popescu, and Celine Rochon. 2018. “Casting Light on Central Bank Digital Currency.” IMF Staff Discussion Note SDN/18/08. International Monetary Fund, Washington, DC.

Monetary Authority of Singapore. 2019. “Consultation on the Payment Services Act 2019: Scope of E-Money and Digital Payment Token”. Singapore.

Monetary Authority of Singapore. 2020. “Consultation on the Payment Services Act 2019: Proposed Amendments to the Act.” Singapore.

Oliveros, Rosa M., and Lucia Pacheco. 2016. “Protection of Customers’ Funds in Electronic Money: A Myriad of Regulatory Approaches.” *BVA Research—Financial Inclusion Watch*, October 28.

Ramos, David, Javier Solana, Ross P. Buckley, and Jonathan Greenacre. 2016. “Protecting Mobile Money Customer Funds in Civil Law Jurisdictions.” 65 *ICLQ*, 705.

Sahay, Ratna, Purva Khera, Miss Stephanie Y Ng, and Sumiko Ogawa. 2021. “Is Digital Financial Inclusion Unlocking Growth?” IMF Working Paper 20/09. International Monetary Fund, Washington, DC.

Sahay, Ratna, Martin Čihák, Papa N’Diaye, Adolfo Barajas, Srobona Mitra, Annette Kyobe, Yen Nian Mooi, and Seyed Reza Yousefi. 2015. “Financial Inclusion: Can It Meet Multiple Macroeconomic Goals?” Staff Discussion Note 15/17, International Monetary Fund, Washington, DC.

PUBLICATIONS

E-Money: Prudential Supervision, Oversight, and User Protection

Departmental Paper No. DP/2021/027

ISBN 978-1-5135-9340-1