FOCUS NOTE

RISKS IN FAST PAYMENT SYSTEMS AND IMPLICATIONS FOR NATIONAL PAYMENTS SYSTEM OVERSIGHT

Part of the World Bank Fast Payments Toolkit

SEPTEMBER 2021

WORLD BANK GROUP

CONTENTS

FINANCE, COMPETITIVENESS & INNOVATION GLOBAL PRACTICE

Payment Systems Development Group

1 SETTING THE CONTEXT

The World Bank has been monitoring closely the development of fast payment systems (FPS) by central banks and private players across the globe.[1] This comprehensive study of FPS implementations has resulted in a policy toolkit. The toolkit is designed to guide countries and regions on the likely alternatives and models that could assist them in their policy and implementation choices when they embark on their fast payments journeys. Work on the fast payments Toolkit was supported by the Bill and Melinda Gates Foundation. The toolkit can be found at *fastpayments.worldbank.org* and consists of the following components:

- The main report *Considerations and Lessons for the Development and Implementation of Fast Payment Systems*
- Case studies of countries that have already implemented fast payments
- A set of short focus notes on specific technical topics related to fast payments

This note is part of the third component of the toolkit and aims to provide inputs on aspects of oversight from a fast payment perspective. It identifies the oversight requirements appropriate for an fast payments and provides central banks with both an indication of the extra capacity needed to conduct effective oversight when an FPS will be in place and a tool for ensuring that the FPS will be designed so that it is consistent with sound standards of safety and efficiency.

2 BACKGROUND

The retail payment landscape has changed dramatically in recent years worldwide. One such development involves improvements in the speed and convenience for users of retail payment services. Enhancements to payment speeds, driven by demand for (near) real-time retail payments, is a notable trend across jurisdictions, and internet banking, mobile payments, and other technological developments have increased the flexibility and convenience of making retail payments. As a result, the number of jurisdictions with services and systems that allow users to conduct (near) real-time payments on a continuous basis has grown impressively since 2010, and prospects are good for further substantial growth in the years to come.

In particular, fast retail payment services have been deployed (or are being developed) in many jurisdictions. In several jurisdictions, stakeholders in national payment systems are growing more and more interested in fast payments, on both the supply side and the demand side, as providers compete to offer better services and users demand more of them.

3 ROLES OF THE CENTRAL BANK IN THE CONTEXT OF FAST PAYMENTS

In the context of an FPS, and depending on its design, the central bank may play diverse and important roles.[2] The central bank may act as the settlement agent of the system, the entity operating the system, the trustee for holding participant funds (in a deposit-based model; see below), and the catalyst of system development, and it fulfills the oversight role in relation to this specific type of retail payment system. In the context of activities oriented toward the development and modernization of the national payment system, the central bank can undertake measures aimed at establishing the system or provide support to the entities that take the initiative. In any case, the establishment of an FPS should be preceded by discussions on the potential need to create the system, which would involve the payment industry and all relevant national payment system stakeholders more broadly. The central bank would be responsible for holding this policy dialogue. Its roles can be further detailed as follows.

Settlement agent: Acting as the settlement agent is one of the roles most frequently fulfilled by the central bank in the context of an FPS. As a settlement agent, the central bank performs final settlements of payments cleared through the FPS. Settlement in central bank money guarantees a payment's final and irrevocable nature and enhances the reliability of payments processed in the system. Settlement in central bank money is aimed at limiting or removing the credit and liquidity risks that are associated with the asset used for settlement.[3]

Trustee: This role involves the central bank in operating an account for the necessary processing of payments in the FPS. This account is used either to collect participants' funds as security for payments being executed in the system or to set aside the liquidity of the participants, which is then used for settlement. Such a solution, which is typically adopted by FPS that are based on the deposit model, guarantees the integrity of the funds deposited in the account in case of the bankruptcy of a participant or the entity operating the system (if this is not the central bank) and their exclusive use for FPS settlement only. As an alternative to the real-time settlement model or deferred settlement model, an FPS can operate on the basis of the so-called "deposit model." Here payments are executed based on deposits preaccumulated by the participants and held in a dedicated account. Each participant's account has a defined limit; the aggregate transaction amount is covered by the prefunding of the dedicated account. Transactions are executed only up to the level of the limit set for a given participant. If the limit for the sent orders of a given participant is exceeded, the payment is rejected. This limit is often referred to as the "net debit cap." Participants manage the level of their liquidity in the settlement account of the system and, depending on the situation, may complement the required limit or transfer the surplus of funds collected over the limit to their account.[4]

System owner and operator: In some cases, the central bank owns and operates its own system (either ACH or real-time gross settlement, or RTGS), in which fast payments are also processed. In such cases, the ACH/RTGS system, in addition to executing interbank orders, enables direct, immediate execution of large volumes of retail payments in the 24-hour mode (for example, the SIC system operated by the Swiss National Bank). Under a different variant, the RTGS system includes a dedicated but separate and yet connected module for the processing of fast payments (for example, the New Payments Platform in Australia). Under yet another variant, the FPS is an entirely separate—standalone—system, and the RTGS settles only FPS payments (for example, FAST in Singapore).

Catalyzer: The central bank is typically involved in the process of creating an FPS. This may come at the instigation of the central bank, or it could follow the initiative of some banks or other payment service providers (PSPs) as they consider the business potential in the domestic market for retail payment services and identify areas for potential improvements.[5] As a result of such an exercise, they may evaluate whether demand for creating an FPS exists in the country, and the central bank would be engaged in the process of evaluating the opportunities and challenges and determining whether to proceed and how best to support the process if the decision to move forward is made.

Overseer: As overseer of the national payment system, the central bank holds the responsibility to oversee the FPS and the provision of fast payment services. As discussed at length below, the goals of oversight include ensuring the safety and efficiency of the FPS and services, setting regulations and standards, monitoring PSPs' compliance with rules and regulations, and maintaining public confidence in the FPS.

4 RISKS IN FAST PAYMENTS

Fast payments are a specific type of retail payments. As with other retail payment services, actors involved in fast payment transactions on both the demand and supply sides face various types of risk. The main risk categories considered are those mentioned in chapter 2 of the *Principles for Financial Market Infrastructures* (cited earlier): legal, credit, liquidity, and operational risk. Special attention is paid to security risks, particularly fraudulent activity, due to the potentially important role that security plays in user confidence in retail payment services in general and fast payments in particular. An additional area that deserves special attention is reputational risk, which is the risk of losing revenue or customers as a result of negative publicity or a loss of confidence (whether based on fact or generated by misperceptions).

Legal risk: Fast payments, like other retail payment services, need to be supported by sound legal arrangements according to their specific design, operation, and use. PSPs need clarity on the rules and regulations that apply when they process fast payments. Rules could be general (that is, not specific to fast payments), but the speed that characterizes fast payments could make it more challenging to fulfill some of the requirements. In fast payments, it is especially important to have clear rules on payment finality and the post-transaction resolution of fraudulent or erroneous transactions, and to make sure that netting is legally recognized. The related customer liability aspects must also be considered.

Credit risk: Credit risk in fast payment services normally does not arise between the payer and payee but may exist between their PSPs. The payer's PSP would normally require funds to be present in the payer's account to initiate a fast payment, and the payee's PSP will immediately credit the funds with finality in the payee's account. Should the payer's PSP allow payments to be made on a credit-push or debit-pull basis, this would normally be a consequence of a bilateral agreement between the service provider and the customer**,** and the credit risk would be managed by the PSP. Credit risk may arise between PSPs in the FPS depending on the settlement model. If settlement takes place in real time and before the PSP of the payee credits the funds in the account of its customer, credit risk does not arise. If settlement is deferred, the PSP of the payee will advance the funds to its customer before receiving them from the PSP of the payer, and credit risk arises between the PSP of the payee and the PSP of the payer. In this case, the use of prefunding or collateralization arrangements would mitigate such risk. The main difference between fast payments and other payment services is that, in the former, the payee's PSP would normally be unable to block or recover the funds from the payee, because they have been credited irrevocably, and the payee may have used them immediately for other transactions.

Liquidity risk: For payers, liquidity risk in fast payments would not be different from that with other payment services. For payees, liquidity issues are mitigated in an FPS, because the funds are available immediately and with finality, whereas in other types of services the funds are paid later or, in some cases, conditionally, so that payments could be reversed or subject to conditions. In an FPS, however, irrespective of the settlement model, liquidity risk arises between PSPs, because PSPs require liquidity to ensure inter-PSP settlement. In an FPS with deferred settlement, liquidity would be needed only at the end of each settlement cycle, yet liquidity risk may arise if the system conducts inter-PSP settlement cycles outside normal business hours. In this case, such tools as prefunding, liquidity or collateral pools or agreements with liquidity providers can be used to ensure that sufficient funds are available for settlement. The adequacy of these tools to support, when needed, settlement cycles outside normal business hours may be an important consideration in an FPS with deferred settlement. In particular, this requires considering scenarios where the net debit cap is exceeded or where the collateral-management and large-value-payment systems are not functioning (due, say, to a business holiday).

Operational risk: Continuous availability nearly 24 hours a day, seven days a week, 365 days a year (24/7/365) is very demanding in terms of operational reliability for the FPS and its participating PSPs. Due to the speed of FPS, any operational incident that results in the delay or interruption of fast payment services would be immediately observable by users. Delays in processing are not easily accommodated in an FPS, as they will not allow the provision of an immediate payment experience to users. As a result, the impact of an operational incident might materialize much earlier than in traditional retail payments, in which a service interruption or slowdown might go unnoticed. Additionally, as users grow accustomed to fast payment services and choose to send their payments on the payment's due date (rather than a few days in advance), if the FPS is unavailable due to an operational incident, the users would be immediately affected and could incur penalties for late payment or have insufficient funds for other transactions. An FPS is exposed to security risk, as a specific type of operational risk, which can be defined as the risk that an actor's assets may be compromised following the unauthorized use, loss, damage, disclosure, or modification of those assets, originating from both internal and external sources, and is highly interrelated to operational risks in an actor's IT systems and processes.

Fraud risk: Fraud risk is a subtype of operational risk that merits further discussion due to its potential importance in an FPS. Fraud could encompass various situations, including (i) the manipulation of the payer or payee by a fraudster, resulting in the issuance of a payment instruction by the payer acting in good faith, (ii) the initiation of a payment instruction by a fraudster (who has fraudulently obtained the payer or payee's sensitive payment data), or (iii) the modification of an attribute (such as the account number, transaction amount, or name of the payee or payer) of a genuinely issued payment instruction intercepted by the fraudster. These fraud types might affect all actors in the payment chain, including end users, PSPs, and the FPS overall, and they are common to both fast and traditional retail payments. However, considering the end-to-end speed and, in particular, the immediacy of funds availability, an FPS may be a more attractive target for fraud than a traditional retail payment system. If funds are available to the payee immediately and unconditionally, a fraudster could quickly attempt to withdraw the funds before the fraud is detected, and measures to reverse or recall fraudulent fast payments may have limited effectiveness.

Risk to data integrity and privacy: The use of FPS would require data and privacy protection. As for all digital financial services, breaches of privacy and data security may result in identity theft, harm to financial records, fraud, and other risks. Mitigating such risks would necessitate legal and regulatory provisions that, among other things, clarify the rights of users, define data types, give users control over their personal data, and set out the legal obligations of data controllers and processors when interacting with data users and with each other. In delivering fast payments services, PSPs should consider the aspects of privacy protection involved, and oversight should make sure that they do so effectively.

Reputational risk: Financial or operational problems experienced by any entity involved in the processing of fast payments could lead to reputational impacts for that entity or for the system as a whole. This type of risk affects mainly the clearing and settlement arrangements and the PSPs participating in the system. It could also affect users, as consumers or merchants might also suffer reputational damage if their payments are delayed due to an FPS malfunction. The sources of reputational risk in an FPS are similar to those faced by traditional retail payment systems. Yet expectations raised by the speed and time availability of an FPS may lead to a quicker materialization of the risk in the event of service degradation. Reputational risk might also affect the central bank or other authorities if they have given the fast payment initiative their explicit support, and especially if they own and operate the FPS.

5 OVERSIGHT REQUIREMENTS IN FAST PAYMENTS

As a retail payment system, the FPS could be designated as of system-wide (or critical or prominent) importance and be subject to appropriate oversight standards.[6] The relevant oversight criteria discussed in this note should encompass the following four relevant dimensions of FPS: (a) legal basis, (b) governance, (c) risk management, and (d) efficiency and effectiveness. The oversight criteria discussed below build on a combination of three sets of oversight tools: the *Principles for Financial Market Infrastructures*, cited earlier; the criteria for effective fast payments developed in the United States under the aegis of the Federal Reserve Banks;[7] and the oversight requirements for payment instruments adopted by the European System of Central Banks.[8]

The criteria can be used both at the design stage of the FPS and to assess FPS performance. The criteria could thus be used to identify system weaknesses and vulnerabilities that require remedial actions. On request by the central bank, the FPS operator would be responsible for implementing the criteria, setting system rules that are consistent with the criteria, and ensuring that all relevant entities operating in the system comply with the rules. In its capacity as overseer, the central bank would make sure that the FPS operator delivers on the criteria (and all other oversight requirements determined by the central bank), and the central bank would hold the FPS operator to account for observing the requirements.

5.1 LEGAL FRAMEWORK

The FPS should have a sound legal basis. Consistent with relevant national laws, the governance authority of the FPS should establish rules and contractual arrangements for governing the system in such a way that it provides a complete, unambiguous, and enforceable legal and regulatory framework for the proper functioning of the system.

The legal basis should have requirements, standards, protocols, and procedures that govern the rights and obligations of all relevant entities operating in the FPS (that is, participating PSPs, fast service providers, and users). The legal basis should address the following:

- Authentication of all entities, payments, or messages connected to a payment
- Legal responsibility of PSPs
- Payment-order initiation/authorization and termination of authorization
- Cancellation of payments
- Delayed and failed payments
- Payment finality and settlement
- Timing of sending and receiving payments
- Records as proof of payment for payers and payees
- Resolution of disputed payments among users and PSPs[9]

The legal basis has to provide clear and unambiguous rules on payment-settlement finality. The FPS should define the time after which a payment is final—that is, the associated transfer of value between the payer and the payee is irrevocable and unconditional, including under netting arrangements.

The FPS should require the payer's PSP to approve each payment following payment initiation to assure that the payer's account has good funds. In assuring good funds, the FPS should provide for customers to be fully informed by their PSPs about account-management implications and any related fees. Also, the permissibility of overdrafts should be decided by an appropriate regulatory authority, and the FPS should demonstrate compliance with all regulatory requirements relating to overdrafts and credit, as applicable. The finality of settlement should happen after good funds approval and not later than when funds are made available to the payee.

The legal basis should provide for clear, risk-based, proportional rules on market integrity. The objective is to prevent the abuse of fund transfers for the purpose of financial crime, to detect such abuse should it occur, to support the implementation of restrictive measures, and to allow relevant authorities to access the information promptly. Rules should be in line with the International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation, which the Financial Action Task Force adopted in 2012. Such standards determine, among other things, which information about the payer and the payee PSPs have to attach to fund transfers.

The legal basis should provide for consumer protection rules. These rules and procedures should allocate in a clear and transparent way the legal and financial responsibilities of all relevant entities in the FPS in the event of losses deriving from unauthorized, fraudulent, or erroneous payments. In particular, the FPS should delineate the roles, responsibilities, and liability allocation that would protect consumer, business, and government payers against losses related to fraud or errors.

The legal basis should provide for rules to protect data privacy and integrity. These should secure information that should not be disclosed, including by setting limitations on the collection of users' and providers' data and on the disclosure of payment data to third parties and their use of it, and by protecting data access and use in the FPS and at users' and providers' locations. The rules for data privacy and integrity should (i) identify the nature and type of user data that may be required for security, legal-compliance, and authentication purposes within the FPS; (ii) indicate how users may get visibility into the data collected on them and limit sharing of such data; and (iii) identify and allocate legal and financial responsibilities in the event of data breaches at the FPS or at users' and providers' locations.

5.2 GOVERNANCE

The FPS should implement effective, accountable, and transparent governance arrangements that promote the provision of safe and efficient services. The internal decision-making process of the FPS should appropriately reflect the legitimate interests of the system's stakeholders.

Weak governance may have adverse effects on the FPS and eventually on the quality of its services, which could ultimately cause serious financial losses to its stakeholders.[10] Governance arrangements should aim to protect the trustworthiness of the FPS and to promote public confidence in it by placing a high priority on safety and efficiency. They should assign clear and direct lines of responsibility and accountability within the FPS; achieve effective decision-making in crises and emergencies; and ensure that the risk-management and internal control functions have sufficient authority, independence, and resources. The governance arrangements should be publicly disclosed.

The governance arrangements of the FPS should be inclusive. They should allow for input and representation from diverse stakeholders (irrespective of ownership), and they should consider the public interest when making decisions and rules. In particular, they should proportionately enable stakeholders or stakeholder groups to influence the outcomes of the decision-making process. This could be achieved by giving stakeholders or stakeholder groups appropriate representation in the governing body and/or by establishing with them effective channels of communication and consultation. The governance arrangements of the FPS should address and manage actual, perceived, or potential conflicts of interest.

5.3 RISK MANAGEMENT

The FPS should establish a sound risk-management framework for managing legal, credit, liquidity, operational, and other risks across the end-to-end spectrum of the payment process. The risk-management framework should enable the FPS to prevent, detect, and respond promptly to disruptions. In particular, it should enable the FPS to

- Address risks related to settlement;
- Address the risk of unauthorized, fraudulent, or erroneous payments; and
- Provide incentives (that is, positive, negative, financial, or nonfinancial) for the FPS operator and providers to address and contain the risks they pose to others.

5.4 SETTLEMENT

The risk-management framework should provide for tools for mitigating settlement risk. Where feasible, an FPS should settle in central bank money. The FPS should ensure that all relevant entities are fit to perform their role in the system by identifying the financial risks involved in the payment process and by having the appropriate measures defined to address these risks. The risk-management framework should provide for measures to mitigate exposures to credit and liquidity risks arising from any lag between transaction finality and settlement and to ensure that credit exposures among participants are fully covered. Also, credit and liquidity risk issues that may affect users should be addressed 24/7/365. In an FPS with deferred settlement, the credit risk borne by PSPs can be managed through limits (to the aggregate net positions of PSPs), frequent settlement cycles, loss-sharing agreements, collateralization, prefunding arrangements, or an agreement with one or more liquidity providers. In an FPS with real-time settlement, the liquidity needs extend beyond normal business hours. This might require procedures to ensure that sufficient liquidity is available in advance (for example, through supplementary funding in the FPS settlement accounts of the PSPs or provided by the central bank). In an FPS with deferred settlement, liquidity needs could be mitigated, as participating PSPs would require funds to cover only the net debit position at a specific settlement time.

Participants in the FPS should be given access to the information needed for them to evaluate and mitigate financial risks. However, sensitive information should be disclosed to the relevant actors only on a need-to-know basis.

5.5 OPERATIONAL RISK AND OPERATIONAL RESILIENCE

Operational risk, including fraud, could have a serious impact on FPS settlement. (See box 1.) Operational risk results from the failure of internal processes and systems caused by human error or external events and could lead to financial losses for one or more of the parties using the FPS, possibly undermining user confidence in it. Thus, the governance arrangements of the FPS should ensure that all relevant entities in the system have adequate policies and procedures

BOX 1 OPERATIONAL RISK IN FPS[11]

FPS are unlikely to eliminate much of what is considered customary operational risk. In fact, they may introduce new sources of operational risk. The new systems and processes of an FPS will have to coexist and integrate with legacy payment complexes that are largely batch environments.

An FPS that is unavailable for a few minutes can cause several hundred payments to fail and the consequences of any downtime to become even more serious than in traditional systems.

Operating in a 24/7/365 environment also affects how PSPs perform end-of-day batch tasks. With real-time payments flowing uninterrupted, PSPs can no longer afford the luxury of having downtime to process end-of-day runs, which have to be done while still processing payments from customers. This requires PSPs to run two processing sites, live, enabling the providers to switch from one site to another if downtime on one infrastructure is required.

A 24-hour operation that doesn't afford downtime and is required to operate continuously while moving ever-increasing volumes is largely unique in the context of banking and legacy payments. Not only are ceaseless operations of the nature being considered more demanding and less forgiving on their face, they are arguably countercultural across a swath of payment franchises in the world of banking.

Such operations could differ substantially and qualitatively from those that have come before. In spite of the many developments that the payment industry has experienced throughout its history and, in even more recent times, due to the dramatic improvements in technology, it has never dealt with a similar change so far. And the industry may rely too much on the occurrence of the natural downtimes that exist in many operations and that are used for maintenance, repair, and cross-system assimilation, and it may turn out to be unprepared to act in a no-interruption environment.

Shouldn't planned downtimes then be considered as a policy tool for an FPS? Planned downtime might serve to mitigate the risk that continuous operation may pose to the FPS and its stakeholders, and since an FPS could facilitate faster runs on banks, planned downtime, or the notion that downtime may be decided for policy purposes, might prove to be useful in slowing or halting a run. In any case, planned downtimes of the FPS and the systems of its participants should be intimated in advance to the public at large, to enable them to make alternate arrangements for their payments.

in place to mitigate operational risk and to ensure business continuity. In this last regard, entities that use outsourced services should make sure that their business continuity is protected against possible contingencies affecting their service suppliers. In principle, the impact of an operational incident could be mitigated by measures similar to those used in other non-fast payment deployments: rigorous processes for the identification and mitigation of operational risk, including cyber resilience (see below), redundancy, and business-continuity arrangements to ensure the timely recovery of services in the event of a major disruption. The timely communication of information to stakeholders in case of operational incidents should be part of these operational risk-management processes.

5.6 RESILIENCE

The FPS should have mechanisms and systems to ensure high levels of end-to-end availability and reliability under both normal and stressed operating conditions. The FPS should define target-availability metrics. It should also have business-continuity and disaster-recovery plans to ensure the timely recovery and resumption of critical services in the event of an outage or cyberattack. The FPS should have mechanisms to minimize the chance that an adverse event would cause other market participants to fail to meet their obligations (that is, that it would trigger system-wide risk). The FPS should demonstrate that sufficient resources are devoted to business continuity and resilience, and it should conduct regular contingency testing across all operators and providers of its end-to-end systems.

5.7 SECURITY AND SAFETY

The FPS should have identification and verification procedures for enrolling and transacting with providers and users. These procedures will be used by the FPS operator and providers to authenticate providers and users to access the system. The FPS should have mechanisms to ensure that payments reach the intended payees at the intended payee accounts. For example, the FPS might (i) require the payee's PSP to communicate explicit acceptance of a payment before finalizing the transaction, (ii) provide a mechanism for sending a prenotification or test message to help confirm the identity of the payee and to validate the existence of the payee's account, and (iii) require monitoring for payment anomalies. The FPS should apply effective user-authentication controls across all delivery channels and may vary the authentication procedure based on the risk profile of a given transaction. The FPS should enable the user to be authenticated initially to the system (at enrollment and prior to transactions) and also require PSPs to reauthenticate users based on the risk profile of a transaction. The FPS should be able to adopt new and decommission old authentication models based on the evolving threat landscape. In particular, the FPS could be integrated with a national digital ID system.

The FPS should be able to comply with rules and regulations concerning AML and combating the financing of terrorism. This involves both operational and other risk issues. Operational issues, such as inadequate or failed internal processes or decisions made by people, can leave the system vulnerable to money laundering. Other risks play a similar role, since prominent or repeated breaches can harm the reputation of PSPs with regulators and stakeholders (including consumers), as well as the reputation of the country vis-à-vis standard-setting bodies and the international community. Technology can be a precious ally in the AML fight. (See box 2.)

The FPS should have procedures to authenticate payments.[12] The FPS should require each payment to be initiated only with the explicit and informed consent of the payer to the payer's PSP, unless the payment is preauthorized prior to payment initiation. If the FPS allows preauthorization, it should enable the payer to preauthorize the payer's PSP to make one or more payments based on defined parameters, as relevant to those payments (for example, the account from which funds are drawn, payee, frequency, time and date, amount, amount limits, duration of authorization, and so on.) The set of pre-authorizations made by the payer should subsequently be made visible to the payer. If the FPS allows preauthorization, it should enable the payer to revoke any preauthorization of payments, or to change relevant preauthorization parameters, easily and in a timely manner.

Based on the rules for consumer protection under the legal basis, the FPS should have controls and mechanisms to protect user data. These should prevent the unintended exposure of user data, both digital and physical, which should be protected in transit and at rest, before, during, and after a transaction. The FPS should require that all entities have in place robust controls and mechanisms (including for users), appropriate to their roles, to protect sensitive information through the end-to-end payment process. The FPS should have controls and mechanisms to protect from unnecessary disclosure sensitive information needed for account setup, transaction setup, and problem resolution. For example, to initiate or receive the payment, the payer and payee should not need to know each other's account numbers or other sensitive information. Also, the FPS should have controls and mechanisms to protect any sensitive information that is needed to process and complete a payment. For example, the payer and payee should not learn of one

BOX 2 FAST PAYMENTS: ENORMOUS POTENTIAL VERSUS FINANCIAL CRIME RISKS[13]

Clients want their payments to be processed quickly because, for them, it increases efficiency, transparency, convenience, and financial control. For small and medium-sized companies, this form of payment processing can alleviate liquidity stress and counterparty risk. More broadly, people have grown accustomed to things moving fast, so they have little patience and understanding when payment processing is slow. Fast payments allow sellers and buyers to exchange money and purchase services in seconds. Funds are received in the payee's bank account almost immediately, instead of requiring a few business days. That can make a significant difference to the cash flow of a small business in particular, and it means less time spent waiting for money to clear from the buyer's point of view. Fast payments are a common requirement in the new economy: The current generations of customers (millennials and beyond) want to be able to make payments anytime, anywhere, using their mobile devices.

But…

Fast payment processing also makes it more difficult to detect financial crimes such as money laundering and financial fraud. Criminals want to move money as quickly as possible through a number of accounts at different international banks to disguise the origin of the funds. There is no faster way to do this than with fast payments. How can a PSP detect money laundering in a real-time world when transaction monitoring is conducted in a batch process?

It is difficult enough for financial institutions to monitor against money-laundering violations when it takes three to five days for a transaction to be cleared, or at best overnight. With fast payments, the nearly impossible becomes totally impossible using conventional methods, as transactions clear in a matter of milliseconds. *Conventional* here refers to suspicious transactions being put in a queue and investigated in batch mode, where anti-money-laundering (AML) systems generate too many false positives (typically between 2 percent and 15 percent of all transactions) and therefore impose a huge workload on PSPs and investigators. With fast payments, this problem is greatly increased because PSPs are under pressure to meet the agreed level of service.

Technology and Risk Management

Transaction-monitoring systems built on current technology and machine learning offer a credible answer. Combining algorithms that learn from past results with the expertise and knowledge of AML-compliance officers, the system learns to identify false positives, and compliance officers can focus on alerts where the probability is high that money laundering is actually occurring. Another recently developed technology, called visual mapping, provides insights into how fast payments are moved around. Suspicious payments can be tracked as they move between customer accounts, regardless of whether the payment amount is split between multiple accounts or the accounts belong to the same or different financial institutions. The software creates a visual map of where and when money has moved, providing new insights and intelligence that fraud and compliance teams can use to take action. By bringing together transactional data from multiple financial institutions and running sophisticated algorithms, such solutions can identify the so-called "mule accounts" that are used to launder money and conduct other illegal activity. Many of these accounts are not set up by the criminals themselves but by a number of scams, including phishing and spam email and instant messaging.

However, while technology is a necessary condition for successful FSP compliance with AML, it is not sufficient. Even with advanced technology, PSPs need to increase their staffing to meet the challenge and ensure that they have enough staff with sufficient knowledge and authority to be available to review transactions quickly. To keep pace, some banks have outsourced simple customer due-diligence functions or moved them offshore. That said, the trend is definitely toward investing in more technology. As a recent article in *The Economist* put it, "Now, the biggest question for bank controllers is how many humans they can replace with bots without compromising compliance. . . . Banks are going into partnership with some of the hundreds of 'Regtechs' that have sprouted in recent years." Technology must be a large part of the solution, but banks will need to take care and seek expert independent advice when reviewing the new regtech apps, as the regulators and the markets will penalize them should their techno-experiments fail.[14]

another's account numbers or other sensitive information at any point throughout the end-to-end payment process. Note that sensitive information should be defined by the FPS consistent with the applicable national law.

An FPS should protect users from the risk of fraud.[15] Most of the measures applied in traditional systems to mitigate fraud risk (whether ex ante measures to detect fraud, such as security screening, or ex post measures, such as SMS alerts for users) might be used to help detect and manage fraud cases in fast payments. Some of these measures may take advantage of the information that accompanies fast payments; many FPS have detailed information about the sender, recipient, time of transaction, and geographic references that can enhance payment analysis to detect fraud. However, these measures could be less effective in an FPS due to the small amount of time between payment initiation and execution. For this reason, an FPS may face challenges in being able to complete the necessary security screening on payments while at the same time meeting end-user expectations for speed.[16] Yet, although screening could be performed quickly and automatically, the management of payments identified as suspicious might require interventions that could slow the process. Limits on the amounts of individual transactions are a potential mitigating measure to cap payers and intermediary institutions' exposure to fraudulent operations. Such limits would also make the fast-payment deployment less attractive for fraudsters.

The FPS should require and facilitate the timely and frequent sharing of information about fraud across all relevant stakeholders and systems. The FPS should require the sharing of information to facilitate the management and monitoring of fraud (for example, patterns suggestive of risk, known instances of fraud, known vulnerabilities, the significance of the information, and effective mitigation techniques). Information shared for anti-fraud activities should be used only for the purpose of managing fraud. Whenever possible, personally identifiable information should be excluded from information sharing; if shared, such information should be encrypted. The FPS should indicate how the proprietary data of entities other than PSPs would be aggregated, managed, and protected for purposes of sharing fraud information. The FPS should facilitate information sharing that supports the real-time and ex post management and monitoring of fraud, and it should provide timely updates and alerts. The FPS's information-sharing mechanisms should be easy to implement, update, and maintain. The FPS's information-sharing mechanisms should support differential access to contents based on the roles and responsibilities of each entity (that is, operator, provider, or regulator). The FPS's information-sharing mechanisms may include a central trusted repository to perform such functions as storage and aggregation of the information. The FPS should have the ability to aggregate fraud information to spot patterns that may not be visible at the level of an individual entity.

The FPS should have a robust system of controls in place to address and foster security, including but not limited to the integrity and protection of data. The control system should be integrated with the existing risk-management processes. In more detail, the FPS should provide layered and robust technical, access, operational, procedural, and managerial controls and strong technical access components and controls, including the following:

- Identity verification and access management
- Data encryption in transit and at rest
- Data quality and integrity controls
- Data-breach prevention and detection
- Layered security controls
- Components and controls that leverage industry standards
- Data retention and disposal controls
- Operations security, monitoring, and incident response
- Communications and network security

The FPS should be robust against cyber risk and resilient to it. It is important that the FPS identifies its critical business functions and the supporting information assets that should be protected, in order of priority, against compromise. The FPS should implement appropriate and effective controls and design systems and processes in line with leading cyber resilience and information-security practices to prevent, limit, and contain the impact of a potential cyber incident. The FPS should be able to detect the occurrence of potential cyber incidents and ready to take appropriate countermeasures against breaches. The FPS should also design and test its processes to enable the safe resumption of critical operations within two hours of a disruption and to complete settlement by the end of the day of the disruption, even in the case of extreme but plausible scenarios. Once employed within the FPS, the elements of its cyber resilience framework should be rigorously tested to determine their overall effectiveness.[17]

The FPS should monitor PSP compliance with risk-management requirements on an ongoing basis**.** All participating PSPs should adhere to the FPS's requirements relevant to their role and fulfill all related obligations and responsibilities. The FPS should have effective processes in place to monitor and enforce compliance by all relevant entities, including by adopting appropriate sanctions in the event of noncompliance.

The FPS operation should be consistent with the protection of market integrity. The FPS should require PSPs to put in place effective procedures to detect transfers of funds that lack the required information and to determine whether to execute, reject, or suspend such transfers of funds.[18]

Finally, based on the rules for consumer protection under the legal basis, the FPS should have processes and time frames for handling disputed payments. These would arise from fraudulent or erroneous activities and would require mechanisms (i) to block funds availability (in a way that is consistent with any applicable laws and/or regulations) if an unauthorized, fraudulent, or erroneous payment is identified by the receiving PSP prior to payment finality, and (ii) to hold rule violators accountable. The FPS should clarify how PSPs should act to resolve errors and fraudulent or unauthorized payments. The FPS should also provide mechanisms for any party to the transaction to request prompt voluntary return of funds from the payee or the return of funds as required by law.

5.8 EFFICIENCY AND EFFECTIVENESS

The FPS should efficiently and effectively meet the requirements of its participants and users, including when choosing the clearing and settlement arrangement; the operating structure; the scope of products cleared, settled, and delivered to users; and the technology and procedures. The FPS should offer convenient baseline features and facilitate the provision of value-added services to users and support cross-border payments. The FPS should be interlinked with other payment systems and other financial market infrastructures, including, for instance, collateral-management systems. Also, access to the FPS should be open to all nonbank PSPs that intend to offer fast payment services. The FPS should have clearly defined goals and objectives that are measurable and achievable, such as in the areas of minimum service levels, risk-management expectations, and business priorities, and it should have mechanisms for regularly reviewing its efficiency and effectiveness.

The FPS should provide the central bank with all relevant information and data on the pricing structure of its services. An FPS ecosystem normally features multiple points of pricing. The pricing strategy employed at each point may differ, but the pricing scheme and fee structure charged to users by participants depend on the pricing scheme adopted by the FPS and the participants. As the FPS and central bank evaluate the overall level of competition within the system, information and data on pricing, covering participation fees and user charges, especially if benchmarked against the same information and data from FPS in other countries, constitute essential inputs.

5.9 COMPETITION

The FPS should allow PSPs to compete to offer services. The FPS should allow the choice of PSPs based on factors such as services (range and quality) and prices and consumer preferences more broadly. The FPS should allow any entity to switch easily among PSPs and/or to use multiple PSPs. The FPS should require PSPs to disclose in advance to their customers all information necessary to make it easy to understand the total cost of using their services.

The FPS should allow PSPs to provide value-added services. The FPS should not prevent PSPs from offering additional services beyond the FPS's defined baseline features as long as the PSPs meet participation requirements, and the FPS should possibly facilitate such offerings. The FPS should allow PSPs to integrate with the FPS by adopting open and accessible standards. The FPS should be interoperable with payment format standards (for example, ISO 20022), and it should utilize a message format that

- Interfaces or interoperates with existing payment format standards that are relevant to use cases targeted by the FPS;
- Enables cross-border interoperability;
- Is cost effective to adopt;
- Facilitates innovation; and
- Is adaptable to future needs and standards by permitting a mechanism for update.

5.10 ACCESSIBILITY

The FPS should enable any authorized entity to initiate and/or receive payments to or from any other entity (consistent with applicable legal restrictions). The FPS should facilitate payments to or from all types of payment accounts (or e-money-storing devices) based in the national jurisdiction and held at licensed PSPs and to or from all bank and nonbank PSPs. The FPS should authorize the use of "open-banking" practices and application programming interfaces that allow PSPs to access their clients' account information, upon client consent via dedicated interfaces. The FPS should demonstrate how all entities choosing to use it can be sure that their payments can reach any and all payees. The FPS should address the needs of the unbanked or underserved to send or receive payments affordably, and it should set up a credible plan for achieving widespread adoption. The plan should demonstrate credibility by showing that adopting the FPS is technically feasible for PSPs and explaining how PSPs are motivated to participate and make the system available to users. If the FPS includes multiple operators or networks, it should have a credible plan to achieve interoperability across these entities. The plan should demonstrate credibility by showing that a payment initiated through one operator, network, or provider can be received by a user served by another operator, network, or provider. Finally, consistent with relevant law provisions, the FPS should allow participating PSPs to make fast payment services available to their customers through agents. The activity of PSP agents would be under the oversight of the central bank.

11. USABILITY

The FPS should provide a straightforward and simple user experience and be available anytime, anywhere, any way, using a variety of access points. The FPS should be available to users in a variety of circumstances, and through a variety of channels, devices, and platforms (for example, without a mobile device, with a mobile device, remotely with a mobile device, and online). The FPS should enable an authorized entity to initiate a payment with limited information (for example, with a name, email address, and/or a phone number) as appropriate for each use case and in a way that sufficiently supports receiver authentication. The FPS should be accessible to users 24/7/365, including to initiate the payment, have visibility into payment status, and receive final availability of good funds. The FPS should be easy to use, accommodate varying levels of user proficiency with technology, and address the usability needs of individuals with disabilities, the elderly, and individuals with limited language proficiency.

12. PREDICTABILITY

The FPS should provide a reliable and standard user experience for its baseline features. The FPS design should ensure that the system can deliver a defined baseline of core features. Baseline features of the payment experience (for example, timing, legal rights, costs, and risks) should be defined, documented, and communicated so that they are well known to users and compliant with consumer protection and commercial law. Aspects that might vary between payments (for example, fees or timing) should be communicated by the PSP to the user in advance and at the time of each payment. Communications should be appropriate for the audience, uniform, clear, concise, and easily understood. To facilitate a consistent experience for users, the FPS should adopt standard communication and messaging protocols. Finally, error-resolution protections, rights, and liabilities of the payer and payee should be clearly defined and easy to understand for all parties.

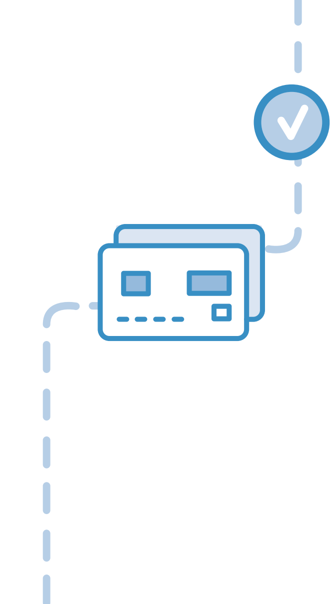
13. SCALABILITY AND ADAPTABILITY

The FPS should be able to adjust readily to ongoing environmental developments and thus scalable and adaptable. The FPS should readily support projected transaction volumes, values, and use cases. The FPS technical design should support projected use cases and demonstrate the capacity not only to handle projected volumes and values, including increased transaction volumes and values during peak times or periods of stress, but also to accommodate a cushion above projections. The FPS technical design should be readily adaptable to developments originating from technology, the economy (for example, financial system failures and economic crises), regulations, and customer demands.

The FPS should support payments in multiple use cases and be adaptable to new payment use cases in the future. Examples of use cases include business-to-business, low-value, just-in-time supplier payments; business-to-person, high-value payments (for example, medical insurance claims); business-to-person, low-value payments (for example, wages for temporary workers); person-to-person payment (for example, payments to friends); person-to-business, remote, real-time payments (for example, emergency bill payments).

14. CROSS-BORDER FUNCTIONALITY

The FPS should enable convenient, cost-effective, timely, secure payments to and from other countries. The FPS should allow for interoperability with similar FPS in other countries. Relevant interoperability considerations might include differences in messaging standards, languages, character sets, mandatory data elements, party/account identifiers, regulatory considerations, and the timing of settlement and good funds availability. The FPS should facilitate access to PSPs that are active in cross-border payments as well as to foreign-remittance service providers. The FPS should require PSPs to make advance disclosure (both prior to and at the time of the payer initiating the payment) of fees, exchange rates, and other user costs, as well as the timing of good funds availability and any risks with the payment, consistent with regulatory requirements. The FPS should allow conversion from one currency to another as necessary for cross-border payments. If the FPS does not have cross-border functionality at implementation, it should have a credible plan for implementing cross-border payments in the future. The plan should demonstrate credibility by showing the timeline for cross-border implementation and how the other considerations of this criterion will be addressed.



6 CONCLUSION

This note was intended to offer guidance on the oversight of FPS. It identified the oversight requirements appropriate for an FPS and provides central banks with both an indication of the extra capacity needed to conduct effective oversight when an FPS will be in place and a tool to ensure that the FPS will be designed so that it is consistent with sound standards of safety and efficiency.

Oversight requires cooperation at various levels, from cooperation between regulators, supervisors and overseers to cooperation between the authorities and all other relevant stakeholders. The aims of such cooperation are to foster communication and consultation that enables authorities to support each other as they fulfill their mandates, and to solicit collection action from stakeholders when needed. Cooperation needs to be effective in normal circumstances and should be adequately flexible to facilitate effective communication, consultation, or coordination, as appropriate, including during periods of market stress and in crisis situations.

7 ACKNOWLEDGMENTS

Organization	Contributor
World Bank	Biagio Bossone (Lead Author)
	Harish Natarajan
	Nilima Ramteke
	Holti Banka
	Oya Ardic

NOTES

1. According to the Committee on Payments and Market Infrastructures (CPMI), a fast payment can be defined as a payment in which the "transmission of the payment message and the availability of 'final' funds to the payee occur in real time or near-real time on as near to a 24-hour and seven-day (24/7) basis as possible."
2. For a comprehensive review of the various FPS models, see *Instant Payments Systems—Analysis of Selected Systems, Role of the Central Bank and Development Directions* (Narodowy Bank Polski, Warsaw, June 2015).
3. See Committee on Payment and Settlement Systems and Technical Committee of the International Organization of Securities Commissions (IOSCO), *Principles for Financial Market Infrastructures* (Bank for International Settlements, Basel, April 2012), Principle 9 (Money Settlement). In October 2014, the Committee on Payment and Settlement Systems was renamed the Committee on Payments and Financial Market Infrastructures.
4. Express Elixir in Poland and BiR in Sweden are examples of this type of model.
5. The Reserve Bank of Australia's role spearheading the launch of the New Payments Platform is an example of the catalytic role that central banks can play in the development of FPS.
6. Designation is the process whereby the central bank, in its capacity as overseer of the national payment system (NPS), identifies NPS entities (including systems, services providers, and payment instruments or schemes) and classifies them according to specific classes of risk, such as systemically important, of system-wide (or critical or prominent) importance, and others—that is, the level of risk that could emerge from their operation and the extent to which such risk could spill over to other NPS entities, the financial system, and the broader economy or affect public trust in the NPS and the national currency. For each class of risk, the central bank would then identify appropriate and proportional oversight standards and requirements and require the system to observe them.
7. This section draws on *Faster Payments Task Force, Faster Payments Effectiveness Criteria* (Federal Reserve Banks, January 26, 2016).
8. See European Central Bank (ECB), *Harmonised Oversight Approach and Oversight Standards for Payment Instruments* (ECB, February 2009).
9. Disputed payments may originate from errors, unauthorized transactions, or disputes in the payment process.
10. The term stakeholders refers not only to the entities that operate in the FPS but also more broadly to the financial and nonfinancial industry that is involved in the production and delivery of fast payment and related services, the community of consumers and merchants, and the general public at large.
11. The content of this box draws on Julius Weyman, "Risks in Faster Payments," Retail Payments Risk Forum Working Paper (Federal Reserve Bank of Atlanta, May 2016).
12. Financial authorities and international financial organizations have highlighted the relevance of developing a robust cyber resilience framework to maintain the functioning of services of financial market infrastructures even after a cyberattack. In June 2016, the CPMI and IOSCO released the report *Guidance on Cyber Resilience for Financial Market Infrastructures,* which provides financial market infrastructures with guidelines for developing and enhancing their cyber framework, focusing on the recovery of critical services within two hours after the occurrence of an incident. In line with such guidance, the ECB has developed a powerful tool that can be adapted to systems at different levels of sophistication; see *Cyber Resilience Oversight Expectations for Financial Market Infrastructures* (ECB, December 2018).
13. The content of this box draws on Paul Hamilton, "Instant Payments: Enormous Potential versus Financial Crime Risks," AML Knowledge Centre, https://aml-knowledge-centre.org/instant-payments-enormous-potential-versus-financial-crime-risks/.
14. *The Economist,* "The Past Decade Has Brought a Compliance Boom in Banking," May 4, 2019.
15. In May 2018, the CPMI issued the report *Reducing the Risk of Wholesale Payments Fraud Related to Endpoint Security.* While focusing on large-value-payment systems, the approach recommended in the report offers valid recommendations and insights that can be usefully implemented retail payment systems.
16. As reported by the CPMI, in some instances, end users may be willing to sacrifice some level of speed or service availability to track payment activity and mitigate the risk of fraud. For example, in Korea, concerns about a rise in telecommunications fraud led to the introduction in October 2015 of the "delayed transfer system" under which a payer can delay the timing of otherwise fast payments for a period set in advance by the payer.
17. Financial authorities and international financial organizations have highlighted the relevance of developing a robust cyber resilience framework to maintain the functioning of services of financial market infrastructures even after a cyberattack. In June 2016, the CPMI and IOSCO released the report *Guidance on Cyber Resilience for Financial Market Infrastructures,* which provides financial market infrastructures with guidelines for developing and enhancing their cyber framework, focusing on the recovery of critical services within two hours after the occurrence of an incident. In line with such guidance, the ECB has developed a powerful tool that can be adapted to systems at different levels of sophistication; see *Cyber Resilience Oversight Expectations for Financial Market Infrastructures* (ECB, December 2018.
18. Guidance relevant to this purpose is contained in European Banking Authority, European Securities and Markets Authority, European Insurance and Occupational Pensions Authority, and Joint Committee of the European Supervisory Authorities, Final Guidelines, JC/GL/2017/16 (European Supervisory Authorities, September 22, 2017). The report elaborates joint guidelines under Article 25 of Regulation (EU) 2015/847 on the measures payment service providers should take to detect missing or incomplete information on the payer or the payee, and the procedures they should put in place to manage a transfer of funds lacking the required information.

WORLD BANK GROUP