FOCUS NOTE

CONSUMER PROTECTION IN THE CONTEXT OF FAST PAYMENTS

Part of the World Bank Fast Payments Toolkit

SEPTEMBER 2021

WORLD BANK GROUP

CONTENTS

FINANCE, COMPETITIVENESS & INNOVATION GLOBAL PRACTICE

Payment Systems Development Group

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

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 across the world has resulted in a policy toolkit. The toolkit was 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 FPS journeys. Work on the FPS Toolkit work 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 consumer protection pertaining to fast payments. Consumer protection is critical to ensuring that customers have a positive user experience and have adequate information to transact responsibly.

2 BACKGROUND

The digitalization of financial services has extended the reach and accessibility of financial services in both developed and developing countries. Electronic transactions are frequently more convenient, faster, and cheaper to carry out, and new products and access channels have emerged that make using financial services easier and more accessible for the previously unbanked segments of the population. For example, more countries globally are adopting fast payments, which allow customers to conduct electronic payment transactions in (near-) real time through internet banking, via mobile banking, in branches, at ATMs, or at such transaction points as stores. Fast payments offer an innovative solution for replacing cash-based transactions and have already led to strong uptake in countries such as China, India, and Mexico.

While the introduction of fast payments has made the completion of electronic payment transactions easier, it has also added complexity to the inter-participant and participant-consumer relationship. For example, for fast-payment transactions, the payer needs to be vigilant when making transactions, as the (near-) real-time transfer of credit is usually not eligible for repudiation. This also requires adjusted rules and processes for remedial actions. Fast payments also enable the introduction of various innovative payment products, often introduced by third-party overlay service providers that might not be regulated or subject to the same security standards.

Furthermore, these new digital financial services and access channels also entail new risks that clients need to understand. For example, new types of fraud have emerged, making adequate security frameworks for financial services paramount to protecting the privacy and identity of the financial consumer. The increasing use of algorithms and data for profiling clients can lead to financial exclusion or distorted behavioral patterns that need to be mitigated. And clients need to have adequate digital literacy and information to be able to use digital financial services responsibly.[2]

Given the above, the rollout of fast payments should be accompanied by a suitable consumer protection regime. There is worldwide consensus among governments and regulators that a strong and adequate consumer protection regime for financial services is essential for the sound deepening of financial systems. Strong consumer protection frameworks help clients make well-informed decisions on the available financial services, prevent widespread abusive practices in the financial sector, and contribute to building trust in these services. This particularly applies to fast payment services, where a suitable consumer protection framework is a core element for a sound user experience and healthy market growth.

In line with the World Bank's *Good Practices for Financial Consumer Protection: 2017 Edition and the World Bank's Consumer Risks in FinTech* (2021), this technical note refers to *consumers* primarily as the individuals who make payments (payers). Similar issues, however, also apply to microentrepreneurs and small enterprises or consumers who receive payments. Where relevant, the latter is also discussed.

3 CONSUMER PROTECTION FRAMEWORK

A consumer protection framework refers to the set of laws, regulations, and codes that enable the fairness of transactions between financial service providers and their customers.[3] Consumers do not possess the same level of market power as financial service providers or payment system operators. Regulations and business-conduct rules, therefore, are important to ensure that consumers are treated fairly and that providers are responsible for their business conduct. Consumer confidence and trust are the key aspects that enable high adoption of noncash payment methods, so standards for the safeguarding of funds, the protection of client information, and the operational reliability of services are important to preserve.

Over the years, the G20/OECD[4] and the World Bank Group have issued a number of high-level principles and good practices on financial consumer protection.[5] For retail payment services, for example, the World Bank's *Good Practices for Financial Consumer Protection* (2017) identifies six core areas that should be covered in an adequate consumer protection scheme for electronic payments. These areas are ideally complemented with efforts to enhance the financial capabilities of customers, to stimulate the responsible uptake of services from the demand side.

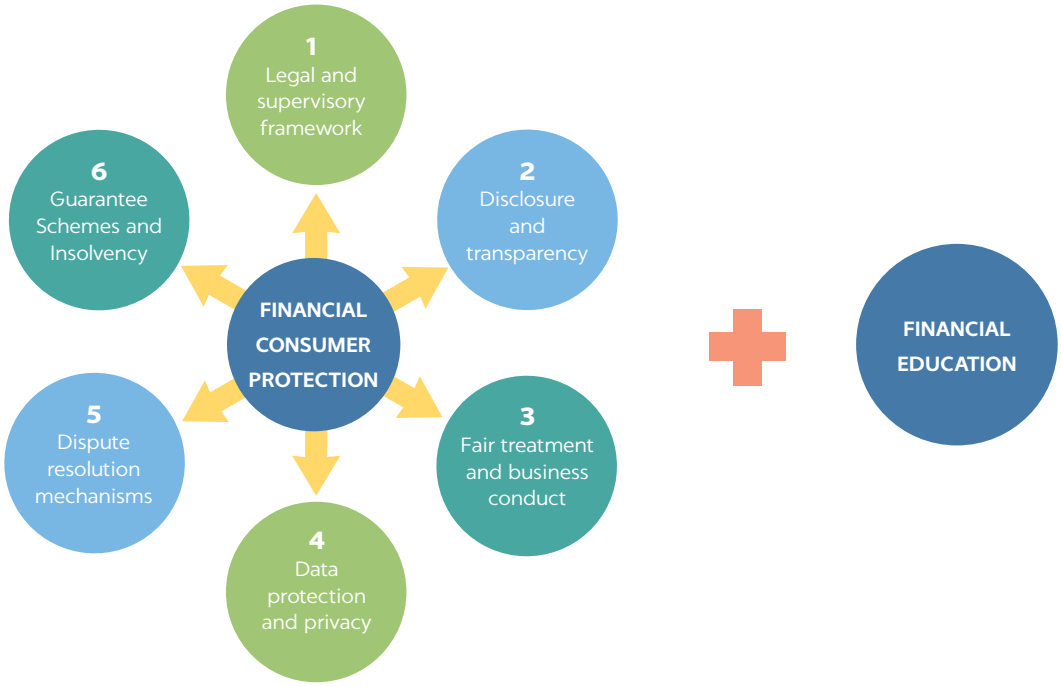
This technical note is structured around these six core aspects of financial consumer protection that the World Bank in 2017[6] established as good practices for retail payment services. (See figure 1.) The good practices are referred to as "*Good Practices* (2017)" throughout this document.

3.1 LEGAL, REGULATORY, AND SUPERVISORY FRAMEWORK

Good Practices (2017) calls for clarity in the legal framework for consumer protection and for the creation of a level playing field between the involved payment service providers (PSPs). Ideally, the applicable legal and regulatory framework should be technology neutral and proportional to the inherent risks, and it should require that all PSPs are formally authorized or licensed by a suitable oversight body. The latter should establish minimal fit-and-proper standards, mandate adherence to governance and internal controls, and implement safety measures to protect the client's funds. *Good Practices* (2017) also calls for clarity in roles in supervision and enforcement and for the establishment of effective and risk-based supervision activities.

Over the last two decades, progress was made in many countries to establish a legal framework for the national retail payment system and to bring the core PSPs under some form of oversight. Regulation and oversight of the retail payment system is usually vested in a country's central bank, which at times also (co-)owns and operates the retail payment system(s). Usually, the central bank also regulates the access of financial service providers to the payment and settlement system and, as part of this, can set important business-conduct rules that also cover issues related to consumer protection.

FIGURE 1 **Overview of Good Practices for Retail Payment Services**



Source: Good Practices (2017), annex A (Retail Payment Services)

Licensing and supervising banks and other financial service providers is usually done by the financial-sector supervisory body, but in certain cases non-bank financial service providers are either covered by a separate oversight entity or not yet regulated. The supervisory bodies usually have well-established processes for on- and off-site supervision of their constituents, and some also cover selected issues related to consumer protection. In recent years, non-bank PSPs were integrated into some regulatory frameworks and are now required to become licensed and supervised and mandated to follow common business-conduct rules (for example, the European Union, Malaysia, and Mexico).

In addition to the consumer protection rules included in the legal frameworks described above, additional legal frameworks and players are usually part of a country's consumer protection framework. Rules on data privacy, cybersecurity, electronic contracts, and signatures are frequently covered by other legal frameworks and government bodies and apply to the entire commercial sector or legal entities in a country. In some countries, dedicated consumer protection laws also apply to financial services. The latter tend to be structured around products and services, creating a level playing field among different providers. Regulation and enforcement of these laws can be delegated to the financial supervisor or directly enforced by the assigned consumer protection body (for example, in Australia, Mexico, and the United States).

Finally, industry associations and payment scheme operators play an important role in setting technical and business-conduct standards for their participants, and international standard-setting bodies develop guidelines and standards for the sound operation of payment systems.

For retail payment systems, the multitude of involved players and frameworks can make effective regulation, oversight, and enforcement of consumer protection standards complex. This particularly pertains to FPS, which can involve an array of financial service providers and access channels and, through this, add complexity to the existing consumer protection frameworks. FPS participants can include regulated and supervised banks, non-bank deposit-taking institutions, and other non-bank PSPs. Furthermore, third-party service providers can offer overlay services, agent services, or innovative digital solutions for easy access to transaction accounts.

Considering this complexity, the FPS studied for this technical note generally rely on a combination of the following four pillars for putting in place a clear and effective framework for consumer protection in payment systems, including FPS:

- **The general legal framework governing the payment systems:** The legislation and regulations issued by the payment system overseer, usually the central bank, set the legal basis for the operation and oversight of the FPS and determine core safety, transparency, and data-

protection standards. Countries increasingly also issue dedicated regulations and standards for electronic payments, which include consumer protection standards across products, and, through this, create clarity and a level playing field across payment providers.[7] Enforcement usually hinges on the central bank and the financial supervisor (see below) and, in some countries, also on the consumer protection agency.

- **Reliance on existing, well-tested, and broad supervisory arrangements for financial institutions:** In many FPS, only fully supervised financial institutions are authorized as direct participants (for example, Australia, Bahrain, Chile, the European Union, and Thailand). These institutions are covered by well-established prudential and operational rules, adherence to which is regularly supervised through on- and off-site supervision. Usually, the existing regulations already cover market-conduct and selected consumer protection aspects.
- **The rule book and technical standards of the FPS:** The FPS rule sets the operational and safety requirements for direct participation in the scheme, and it also includes oversight mechanisms, such as certification schemes through external auditors/experts, to monitor compliance. In some instances, the rule also includes rules and standards related to consumer protection, including on pricing, transparency, dispute resolution, and data protection. Some FPS also directly include overlay services, which are offered as a central feature of the scheme and, through this, set strong consumer protection standards. This includes, for example, customer authentication and QR code systems, which are discussed below.
- **Tiered access:** In some jurisdictions, smaller financial institutions and third-party financial service providers can become indirect participants, relying on a direct participant for the provision of access to the FPS and settlement schemes, as well as adherence to core safety and technical standards and market-conduct rules.

Furthermore, the review noted the following two different approaches toward establishing a consumer protection framework for fast payments:[8]

- **Rule-based approach:** The regulators or scheme operators lay down clear and well-defined guidelines to be followed by all PSPs to protect the customers. It is applied uniformly throughout the industry and requires supervision to enforce. The drawbacks of this method are its inflexibility and the need to adjust the standards to new scenarios over time.
  - **In Europe,** the European Commission is responsible for proposing legislation for the European Union. It issued the revised European Payment Services Directive (PSD2) as the major law for regulating the payment and settlement systems in Europe. The guidelines described in the legal framework set the frame and minimum standards to be adhered to, which then have to be translated and refined into national law. The legal framework is further enhanced with regulatory technical standards issued by the European Banking Authority that provide, among other things, strong customer authentication requirements for the PSPs. In addition, the General Data Protection Regulation for data-protection requirements are applicable. The European Central Bank performs the dual role of overseer/competent authority and is supported in this role by national central banks and supervisory authorities.
  - **In Bahrain,** the Consumer Protection Law of 2012 is the main legislation for consumer protection, including for financial services. Its implementing regulations were issued in 2014 by the Ministry of Industry, Commerce and Tourism. In addition, the central bank sets provisions related to the financial industry and supervises their enforcement. It has set regulations on transparency, fair pricing, and confidentiality, to which all participants in the FPS have to adhere.
- **Principle-based approach:** This method focuses more on adhering to global best practices or those published by leading bodies, such as the Organisation for Economic Co-operation and Development, the G20 countries, and the International Financial Consumer Protection Organisation, which work extensively to protect the rights of customers. The approach relies on financial institutions' knowledge of the market and encourages thoughtful solutions, rather than mandating mechanical compliance with the rules. The drawbacks of the method are that it is difficult to ensure compliance and requires flexibility on the part of both the regulator and the payment system operators.
  - **In India,** the Reserve Bank of India (RBI) has proposed setting up a self-regulatory organization to improve security, customer protection, and pricing in India's digital payment systems. The RBI aims to make the self-regulatory organization act as the conduit between the central bank and the payment providers and provide best practices on security, customer protection, and pricing.
  - **In the United States,** the operator of Real-Time Payments (RTP) is advocating (as part of its connected banking initiative) for new technology standards and infrastructure, risk-management requirements, and

BOX 1 EXAMPLE OF HOW A CONSUMER PROTECTION FRAMEWORK NAVIGATES THE COMPLEXITY OF THE FPS AND FINANCIAL SYSTEM

In the United States, the clearinghouse operating the fast payment system RTP is regulated jointly by the Federal Reserve Board, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation (FDIC). These government agencies also regulate and supervise individual participating financial institutions and set prudential and operational standards for the financial institutions under their oversight.

Consumer protection aspects are regulated and supervised primarily by the Federal Reserve Board and the FDIC, while the Consumer Financial Protection Bureau oversees enforcing all federal consumer protection rules, handling consumer complaints, and enhancing financial literacy of consumers. Furthermore, all financial accounts involved in the FPS are subject to the deposit insurance of the FDIC, giving the FDIC a role in supervision.

Fast payment transactions fall under the Electronic Fund Transfer Act and Regulation E issued by the Consumer Financial Protection Bureau. The regulation sets the core rules for financial consumer protection for electronic fund transfers that directly or indirectly involve an account at a financial institution. The regulation establishes a level playing field across the involved financial institutions, helps harmonize regulatory approaches, and brings third-party service providers and fintechs into the financial consumer protection framework.

Source: Own elaboration

legal agreements, which it is developing through collaboration with the industry. For example, it has developed model contracts between banks and fintechs to facilitate collaboration and to bring the guidelines on consumer protection issued by the Financial Consumer Protection Bureau to life.

3.2 DISCLOSURE AND TRANSPARENCY

Access to information is an important element of consumer protection mechanisms. Adequate disclosure of product features and transparency regarding pricing and redress mechanisms are particularly important for the introduction of new products and services, as they help create trust and confidence among consumers and can reduce risks. FPS should therefore incorporate adequate disclosure and transparency measures from the start, to foster responsible uptake of services.

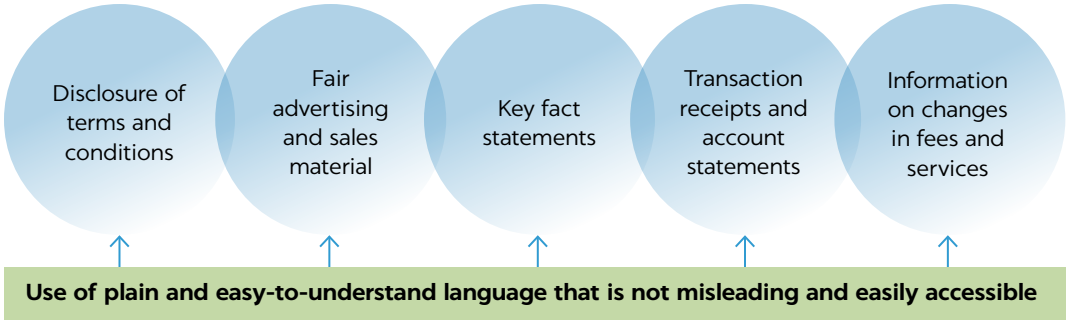
Good Practices (2017) calls for easily accessible information that uses plain and easy-to-understand language and terms, is presented in a timely manner, and does not include misleading or false information. The terms and conditions should be disclosed prior to entering into a formal agreement, and key characteristics of the service, such as fees and charges and the rights and responsibilities of each party, should be disclosed to the customer in writing. The latter can include electronic formats. In line with Principle 4 of the *G20 High-Level Principles on Financial Consumer Protection*,[9] key fact statements should ideally be included to highlight the main features, and to allow comparability across PSPs. *Good Practices* (2017) also recommends making the issuance of receipts mandatory, as well as the periodic provision of account statements. The latter should reflect all electronic transactions that were conducted during the timeframe. The frequency of these periodic communications should be commensurate with the nature of the payment service and the risk involved. Finally, changes in prices and terms should be communicated in a timely manner to the consumer, and customers should be given a right to exit the contract if they disagree with the changes.

Highlighted below are a few approaches taken to regulate and enhance actual disclosure and transparency of information in fast payments.

Pricing and Terms and Conditions

In most jurisdictions, some guidance is provided on the disclosure and format of terms and conditions, and on other information materials. This is usually part of the general consumer protection regulations of financial services, which were recently adjusted in a number of countries to extend their reach to new financial service providers, including third-party service providers.

FIGURE 2 **Core Elements of Disclosure and Transparency Standards**



Source: Own elaboration

- **In the United States**, the Electronic Transfer Act mandates that fees for electronic transfers should be disclosed either when a consumer contracts for an electronic fund transfer service or before the first electronic fund transfer is made. Changes in the terms and fees need to be communicated to the client 21 days prior to the change.
- **In China,** participant institutions are free to determine the applicable charges to the end users. The recently issued Order of the People's Bank of China (2020),[10] however, calls for disclosing information (including fees) and using information that is conducive to the acceptance and understanding of financial consumers.
- **In Europe,** the PSD2 directives provide guidelines on pricing that member states should incorporate into their national legislations. Article 84 establishes that users should be informed about the real charges and costs of payment services and that nontransparent pricing should be forbidden.
- **In India,** PSPs are required to depict the terms and conditions clearly, to use simple language, and to disclose all applicable fees, including for account expiration/dormancy.

In several jurisdictions, stakeholders are also working on alternative approaches to improving the disclosure of terms and conditions and the delivery of information to consumers. For example, to improve disclosure, efforts are ongoing to simplify products and their features and, through this, to enhance understanding and fulfil disclosure requirements. Unified QR code standards and other overlay services can play a crucial role in harmonizing and implementing transparency and disclosure standards. They are under development in a number of countries. Furthermore, some schemes or regulations foster the development of joint terms for easing the comparison of fee structures, and they conduct consumer testing by employing behavioural science to determine more effective ways for information to be communicated or shared with consumers.

Transaction Receipt

As in other electronic payment schemes, users of fast payments are usually notified either via text, email, or any other convenient method of communication of the initiation/completion of a transaction. *Good Practices* (2017) suggests that the receipt should include information about the PSP, location details, the amount and time of the transaction, a reference number and identification detail of the payment instrument, and details on the relevant counterparty, as well as all fees and charges (including the exchange rate, where applicable). In a direct debit transfers, the consumers (payers) should also receive both a confirmation that an attempt would be made to collect the payment from their account on a specified date and the status of the debit (after transaction).

In most studies of fast payment schemes for this note, a receipt is made mandatory or is automatically included as a feature in the payment scheme itself:

- In **Mexico**, the central bank regulates the provision and content of the receipt to be issued by the participant in the Interbank Electronic Payment System (SPEI) system and also offers a portal where the end users can look up the receipt or verify the status of the transaction independently.
- **In the United States,** the Electronic Fund Transfer Act establishes that a customer should receive a receipt for any payment made over US$15 and clarifies that the receipt should include the amount, date, type of transfer, and code for identification of used account, as well as information on the location.
- **In Bahrain,** the FPS platform sends both the payee and the beneficiary an SMS confirmation of the conducted transaction.

- **In Kenya,** the transaction is done through a bank's mobile application. As part of the agreed transaction procedures, the end user has to confirm the details of the transaction and enter a PIN to complete the transaction. The user then automatically gets an electronic confirmation for the transaction with the transaction details.
- **In Europe,** PSD2 determines that the payer should immediately, upon completion of the transaction, receive information about the transaction, including the amount and currency, transaction details allowing identification of the transaction and the payee, and information on the charges. The latter should include a breakdown, where applicable (including, if applicable, the exchange rate). The originator account-servicing PSP is also obliged to inform the originator (payer) immediately if the funds have not been made available to the beneficiary (payee).

Regulators and FPS operators also provide for other transparency and disclosure measures. Account statements reflecting fast payment statements are mandatory in most systems, as they rely on licensed deposit-taking financial institutions for which these standards are already well established. To encourage end consumers to check the authenticity of a prospective PSP, a number of FPS operators and central banks publish lists of licensed or authorized PSPs on their websites and provide harmonized information and promotional material.

- **In the United Kingdom,** the Financial Services and Markets Act of 2000 or the UK Consumer Credit Act of 1974 requires, for example, that financial service providers disclose in their advertisement both that they are a regulated entity and the name of the regulator. This can enable consumers to verify claims and undertake background check of the service provider.[11] The payment system operator also publishes a suite of information on its website, ranging from regulatory framework and approach to guidance about complaints against PSPs.
- **In Australia,** information transparency is being enhanced by the common use of an overlay service. Most financial institutions signed up to the joint overlay service Osko, and 80 percent of transactions on the New Payments Platform (NPP) are channeled through Osko. The owner of Osko launched a marketing campaign that included a variety of digital and physical channels (including flyers, digital media, brochures, and outdoor advertisements) and also provided marketing material to the individual financial institutions. This facilitated common messaging and made it easier for end users to understand the service.
- **In Bahrain,** the payment service operator also operates the main payment app and has rolled out national campaigns to raise the awareness about BenefitPay transactions.

The Central Bank of **Ireland** has developed an innovative system to monitor disclosure and fair advertisement.[12] The Central Bank of Ireland uses the Probability Risk and Impact System, which deploys a high-level business-intelligence tool to analyze such key metrics as sales data, the volume of complaints, advertising spending, and social media queries to identify potential consumer detriments and to take action to mitigate them. Based on the findings, the bank believes in taking strong and transparent action to deter poor practices, achieve compliance, and encourage transparency.

3.3 FAIR TREATMENT AND BUSINESS CONDUCT

An important part of consumer protection is ensuring the fair treatment of customers and fostering sound business conduct among the market players. In addition to protecting the consumer, the latter can help harmonize standards and procedures and, through this, facilitate the development and uptake of specialized services that can create economies of scale, foster interoperability, and include smaller players in the system. This is turn can help foster fair competition in the market and bring additional benefits to the customer.

General Aspects of Fair Treatment and Business Conduct

Good Practices (2017) highlights a number of standards that should be adhered to in order to foster the fair treatment of customers. The regulatory regime governing the payment system, for example, should ensure that PSPs do not include terms or conditions that are unfair to and restrictive for the consumer. In some countries, PSPs try to discharge themselves of any liability, including for their technical systems, the reliability of their operations, or the actions of their agents. These clauses, if present, should be deemed void and not legally enforceable. Customers should also be given access to clearly defined and accessible redress mechanisms (see discussion below), as well as easy-to-use options for cancelling or unsubscribing from a payment method. The latter is particularly relevant for preventing market distortion, as it can inhibit a customer from changing the service provider.

As for disclosure and transparency rules, rules on fair business practices are frequently already covered in the applicable consumer protection framework for banks and other deposit-taking institutions but might need to be added or put on a level playing field for non-bank PSPs participating in FPS.

- A few countries, such as **Malaysia**, have put in place a review arrangement where *all* PSPs are required to have their terms and conditions vetted before enacting them with consumers. The supervising authority has powers to direct the PSPs to modify the terms if it comes across such clauses that are restrictive in nature.
- **In India,** all PSPs are mandated by law to inform their consumers of the pending expiration of their prepaid instrument at least 30 days beforehand.
- **In Australia,** standard-form contracts were introduced to help mitigate the scope of ambiguity or malpractice in terms of conditions being imposed on financial consumers. Unfair conditions are defined in a principle-led way in the legislation, covering in its ambit various practices that can be considered unfair for the consumers.
- **In Mexico,** guidelines on the service level to the end customers were established by the FPS, including guidelines for compensation for damages.

As part of fair business conduct, FSP operators and participating PSP should also protect their systems against fraud and security breaches and put measures in place to ensure operational reliability. Some of the security concerns include data breaches, phishing, account takeovers, and man-in-the-middle attacks. Guidelines and rules on security and fraud protection are traditionally set by central banks or the government agencies in charge of regulating the payment system, setting the parameters within which to stay. In many FPS studied, the FPS operator also directly incorporated minimum technical standards in the scheme rule book and requires compliance verification as part of the onboarding process and on a regular basis thereafter. In Australia, for example, the scheme operator requires that PSPs have real-time fraud protection and detection controls in place. As this can set hurdles for participation for smaller entities, alternative approaches are emerging. In Mexico, fraud protection is directly integrated into the payment system. The toolkit's technical note on fraud protection and anti-money-laundering and countering the financing of terrorism has further details on this.

To limit large-scale fraud and facilitate liquidity management, most FPS also set transaction limits, and some provide for the bank or the customers to set individual transaction limits in line with their own risk preference and policies. FPS also increasingly allow the use of aliases, such as mobile phone numbers, nicknames, or other forms of ID, or integrate QR codes and request-to-pay features. As discussed in separate notes of the toolkit, features like this can help reduce mistaken transactions and enhance the safety and user experience of the customer.

Finally, strong customer authentication standards are an important aspect for consumer protection, as they help reduce fraud and prevent identity theft. This is particularly important in fast payments, where the transaction is final once processed. However, customer authentication processes can also lead to overly complex and cumbersome processes for customers and, through this, hamper the customer experience of fast payments. It is therefore important to strike a balance between safety and convenience for customers. The toolkit includes a note dedicated to customer authentication that details standards and emerging trends.

Fair Competition

Fair competition between market participants and the promotion of interoperability in payment systems are core driving forces for market development and consumer protection. Most FPS initially started off allowing only banks into the system, as these entities are subject to full regula-

BOX 2 INITIATIVES TO PREVENT FRAUD IN AUSTRALIA

In Australia, several players contribute to combatting fraud:

- New Payments Platform Australia collaboratively brings together leading security and fraud experts from each of the participating banks to manage, monitor, and undertake activities aimed at combatting any fraud related to the New Payments Platform.
- IDCARE, a national nongovernmental organization providing identity and cyber support technical advice to individuals, offers effective guidance for responding to security threats and concerns and mitigating possible harm.
- The website Scamwatch, which is run by the Australian Competition and Consumer Commission, provides information to consumers and small businesses about how to recognize, avoid, and report scams.

Source: Own elaboration

tion and supervision. This also allowed testing the system before adding new players. In Mexico, for example, other government-licensed and supervised financial entities were eventually admitted after two years,[13] and in Malaysia the first non-bank financial service providers are now in the process of rolling out the overlay services (that is, the Duitnow app and DuitNow QR code). Implementation experience, however, also shows that, even within the banking system, many smaller institutions find it difficult to fulfill the technical requirements for direct participation in a fast payment scheme and opt not to participate.

Moving ahead, it will therefore be important to ensure that PSPs do not engage in anticompetitive practices, and to promote that payment scheme operators enable the participation of a wide variety of PSPs over time. Some countries, for example, have introduced regulations to oblige banks to offer fast payments or are considering this option.[14] In general, risk-based participation requirements should be considered, where feasible, and indirect participation in the scheme facilitated. The following two approaches for indirect participation have emerged so far:

- **Indirect participation** through a direct FPS participant that has to ensure that the indirect participant meets certain minimum standards to access the participant's systems and is eligible for clearing services provided by the participant. In this scheme, the participant is then usually in charge of monitoring compliance with minimum standards.
- **Direct participation** in the FPS platform for the payment transaction itself (in part through overlay services), but access to the settlement system through a direct participant, which in general is a fully licensed bank.

Furthermore, *Good Practices* (2017) suggests that the financial-sector regulators and payment-system overseers should regularly assess market competition (and publish the results) and foster transparency and competition through the public provision of comparator websites and tables. The benefit of monitoring the market can be seen in the European Union, where a recent study on fees charged for electronic transfers shows that commissions charged for SCT Inst transactions vary greatly not only between the involved players but also within institutions (in comparison to fees charged for using other electronic-transfer options).[15] This can make it difficult for the customer to get an overview and points to market distortions that warrant further assessment to determine whether regulatory measures would be needed.

The following two other trends in the area of competition should be mentioned:

1. To facilitate the introduction of fast payments and prevent distortions between market participants, some authorities and FPS operators issued rules regarding the pricing of fast payments to the customer. These include limiting charges to either the sender or recipient, setting pricing rules by type of customer, or eliminating/issuing caps on the pricing for smaller payments.
   - **In Bahrain,** prices are determined uniformly by the payment platform operator for the FPS Fawri+. To promote the uptake of fast payments, Fawri+ transactions of up to BD 100 are free of charge for end users, and the fees for Fawri+ transactions of between BD 101 and BD 1,000 are set at BD 0.10. No charges can be levied for cash withdrawals at own service points, but the acquiring PSP/bank can apply a maximum charge of BD 0.10 per transaction for using other service points.
   - **In Chile,** participant banks are not allowed to charge individual customers but can levy a transaction fee on corporate customers.
   - **In Portugal,** a recent amendment to the financial consumer protection law establishes thresholds per transaction and monthly volumes of transactions, below which financial institutions cannot charge their account holders for fast payment transactions carried out through third parties.
   - **In Malaysia,** transaction fees for DuitNow transfers of RM 5,000 and below need to be waived for individuals and small and medium-sized enterprises. For transactions above RM 5,000, a fee of MR 0.50 may be applicable. In practice, a number of banks are waiving this fee as well.
   - **In Mexico,** the central bank (which owns and operates the system) prohibits levying charges on the payment receiver but allows the FPS participants to collect fees from the payment sender. To facilitate oversight and transparency, all FPS participants are required to register their customer fees at the Banco de México, which monitors the charges and discloses them for ease of price comparison. For payments involving the digital platform CoDi, participants are not authorized to charge any fees to the involved senders and recipients.
   - **In Thailand,** the Bank of Thailand regulates user charges for financial transactions. For the FPS PromptPay, no user charges can be levied for payments through digital channels, such as internet banking and mobile banking, whereas nominal charges for channels such as ATMs and branches can be set. In prac-

tice, these charges vary from nil to B 10 for individuals and from B 10 to B 15 for juristic persons.

- **In Europe,** a 2008 regulation on cross-border payments mandates that banks apply the same charges for domestic and cross-border electronic payment transactions in euros. Discussions are currently underway whether further rules should be introduced, as in a number of countries and service providers, the fees charged for instant payments have been shown to be higher than the fees charged for traditional electronic payments.[16]

2. A number of countries currently also explore options for extending their national FPS to cross-border transactions. These are already feasible in selected countries studied for this review. To handle cross-border payments or transfers in payment systems involving several currencies, rules on pricing and the disclosure of the foreign exchange rate used for the conversion would be beneficial from a disclosure point of view:
   - **In Hong Kong SAR, China,** fast payments supports national-level transactions in both Hong Kong dollars or Chinese renminbi. Customers can register a multicurrency account into which both Hong Kong dollars and Chinese renminbi can be transferred. Settlement is done by two different mechanisms—Hong Kong Monetary Authority for Hong Kong dollars and Bank of China (HK) for Chinese renminbi—as the systems are not interoperable between each other. This approach eliminates the need for currency conversion.
   - **In Europe,** SCT Inst transactions are denominated in euros, but the payer's or payee's underlying account can be denominated in other currencies. The originator and beneficiary are charged separately and individually by the originator and beneficiary bank, respectively. Charges for end user are not capped. For cross-border transactions, however, the European Union's legislation introduced the obligation to charge the same fee level as for similar transactions at the national level. The exchange rate needs to be made explicit on the receipt.

3.4 DATA PROTECTION AND PRIVACY

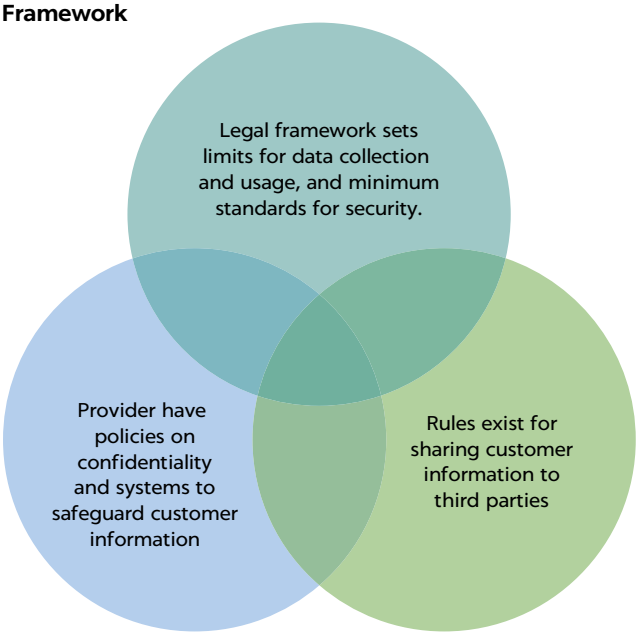
Electronic payments leave a trail of data. This data can provide valuable information for financial service providers about the size and periodicity of financial transactions of a client and potentially enhance a person's access to financial services. In combination with other data, such as location, timing, and purpose of transaction, however, the data can also give financial service providers, merchants, and other commercial entities valuable insights into a customer's behaviors that they can leverage for cross-selling and the marketing of other financial and nonfinancial products and services. The amount of collected data is a concern for consumers, who worry about the security of their collected identity and personal data. It will therefore be important to ensure that the available data is not subject to abuse or breach of security and that it is not unduly shared with third parties.

Data protection and privacy is a particular concern for FPS, as these systems over time can involve a larger range of service providers and cooperation partners. FPS will increasingly include, directly or indirectly, nonfinancial service providers such as telecommunication companies and social media players who are, to a varying degree, covered by data-protection requirements. FPS frequently also use overlay services of third parties to enhance the customer experience (that is, the interfaces developed by Osko in Australia) and involve a range of service delivery points through third parties (that is, agent networks, merchants, mobile apps). Considering this diversity, minimum standards for data protection and privacy across all stakeholders in FPS will need to be ensured to protect the consumer.

International best practice suggests that the collection and usage of data should be properly regulated, and that adherence should be supervised for all involved players. *Good Practices* (2017), the World Bank's work on this topic, suggests that rules should be established on the type and amount of data that can be collected, as well as on the processing of this data.[17] Furthermore, providers should be obliged to disclose to the customer which information will be collected, for how long, and for what purposes. Where relevant, providers should be required to seek the customer's consent on the collection and sharing of the person's data prior to sharing the information, and legislation should set clear rules and limits for the sharing of data with third parties. Sensitive information such as the value and volume of transactions should be shared only with authorized credit bureaus or any other authorized agencies, ensuring confidentiality and security during the process of transmission. Finally, the issue of ownership of such data needs to be covered in the regulation.

All data collected by the PSP should be in line with data privacy and confidentiality requirements as mandated by the law, and compliance should be supervised on a regular basis. Customers should have access at no or minimal cost to the information that is being maintained by the PSPs. To ensure complete confidentiality and security of the consumer data, PSPs should put in place adequate safeguards, such as different levels of permissible access to customers'

FIGURE 3 Core Components of a Data-Protection Framework



Source: Own elaboration based on Good Practices (2017)

data for employees. It is particularly important that PSPs have appropriate security arrangements in place to protect consumers from fraud, scams, and identity theft or unsolicited marketing.

Provided below is an overview of some of the data-protection rules for fast payments that were established in individual countries.

- **Europe:** The General Data Protection Regulation governs rules and measures on data security and privacy. It is applicable not only to member states of the European Union but also to all institutions providing services to citizens of the European Union. It requires institutions to obtain consumer consent before sharing data and to anonymize the data, and it sets minimum standards on data storage and transmission across borders as well as measures to undertake in case of security breach.
- **India:** The Payment System Act governed by the Central Bank in India prohibits financial institutions from sharing consumer data with any third-party service provider unless it is required by law or the consent of the consumer was received beforehand.
- **Bahrain:** In line with the kingdom's efforts to regulate and organize the cybersecurity framework in Bahrain, the government has issued several laws and pieces of legislation related to cybersecurity and personal data protection. Directives from the Central Bank of Bahrain on the Electronic Fund Transfer System require participants to have comprehensive information-security policies, standards, measures, and controls to ensure the confidentiality, integrity, and availability of consumer data. For example, all customer information has to be encrypted and stored in a secured manner. Licensed PSPs must ensure that any information in their control or custody will not be used or disclosed unless (i) they have the customer's or licensee's written consent, (ii) disclosure is made in accordance with the licensee's regulatory obligations, or (iii) the licensee and members of the credit bureau are legally obliged to disclose the information based on the Central Bank of Bahrain law.

FPS providers generally require all stakeholders to comply with standards that are similar to those mandated for other payment systems in the jurisdiction. This generally includes encryption or tokenization of data. Data fraud, for example, should be addressed by keeping sensitive data in a secure area of the consumer's device (if needed) and combining it with the traditional PIN/password mechanism that is not stored in the device. In this scheme, even if there is a data breach in the central system, there is no sensitive data to be stolen. The implementation of such schemes should be a flexible yet standardized solution, so as not to constitute a barrier to financial innovation. A few FPS have also put in place centralized databases or set clear rules on the type of consumer data that API services can access.

- **United States:** RTP operating rules include provisions regarding the treatment of confidential information by the operator TCH and participating financial institutions. This includes encryption requirements for the storage and transmission of RTP message data. PSPs holding customers' accounts are subject to existing consumer-privacy laws regarding the proper use of consumer data and restrictions on the disclosure of such information to third parties. Additionally, the compliance criteria require PSPs that access the RTP system through banks to develop and implement administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information, as well as to ensure the proper disposal of customer information
- **Kenya:** The Pesalink in Kenya operated by IPSL does not share any consumer data with the participating banks. IPSL holds the consumer data for a period of seven years for compliance purposes.
- **Australia:** Australia's NPP is governed by a privacy policy that describes how the operator NPPA manages the personal information that it may collect, hold, use, or disclose for the purposes of its functions and activities. The

system uses the central database PayID, which securely stores all PayID information and is operated by SWIFT. PayID sits in the infrastructure of NPP, where it is a part of the core capability of the platform and is an enabler that can be used by any overlay service. For security reasons, users need to register a PayID with their financial institutions. The process for users to register a PayID can differ between financial institutions but is fully encrypted.

3.5 DISPUTE-HANDLING MECHANISM

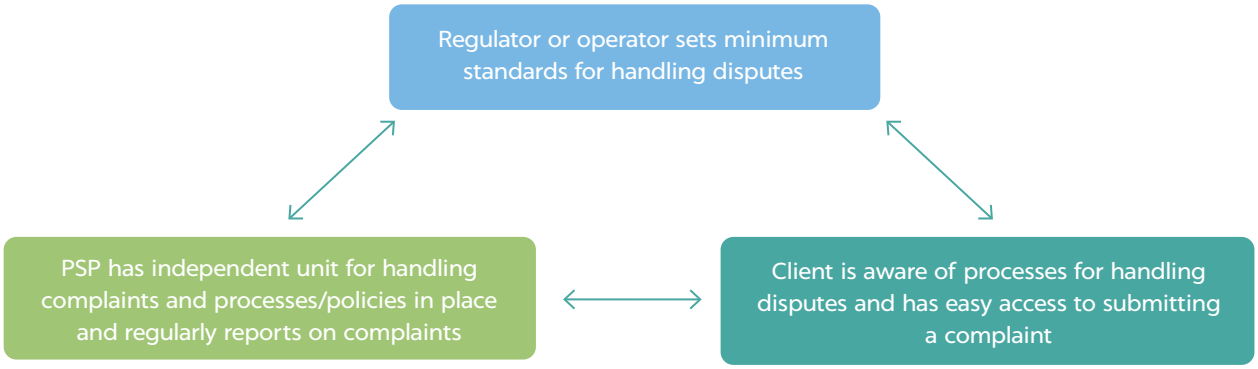
An effective dispute-handling process is of particular importance for fast payments, where transactions (once authorized) are final, and errors are difficult to remedy afterward. To create trust in the fast payment system and protect the consumer, the user needs to be aware of the irrevocability of a fast transaction and to have access to clear and easy-to-understand information about formal dispute-resolution methods, such as mediation, arbitration, or litigation. The customer also needs to understand what constitutes a fraud, how to prevent and report it, and what liability could arise. Providing this information is foremost the role of the PSP itself but can be supported through public-information campaigns from such stakeholders as the FPS operator or government institutions active in the area of financial education and consumer protection.

Receiving and following up on the reported dispute is generally the responsibility of the involved PSPs. International experience, however, suggests that the regulator and FPS operator should set minimum standards and provide guidance on the procedures that PSPs need to put in place. The intent should not be to prescribe rigid procedures, but to guide the PSPs on how to handle consumers' grievances in an effective manner. For example, the PSP should be mandated to have in place an adequate structure that handles complaints in a fair and transparent way. This is usually best done by a dedicated unit. Furthermore, the consumer should have access to a range of easily accessible channels for submitting a complaint (for example, by phone, email, or online) and should receive a confirmation number and information on the timeframe for resolution. Communication with the customer at all levels of the escalation process should be timely.

Most jurisdictions analyzed have minimum rules for dispute resolution in place that apply to the FPS. One such example pertains to the processes that were established by the Hong Kong Monetary Authority in collaboration with the industry. The processes are detailed but leave enough flexibility for the PSP to tailor them to internal procedures and policies. At the same time, the harmonized rules allow PSPs to convey the core procedures for dispute resolution as well as the rights and obligations of clients through broad information campaigns. Some of these guidelines/standards can also be integrated directly into the design of the payment scheme and, through this, be harmonized across participants.

- In **India,** it is mandatory for PSPs to provide an option in their app to raise a dispute/complaint by providing a transaction reference/ID number.
- In **Europe,** the PSD2 regulation, among other provisions, requires PSPs to lower consumers' liabilities for unauthorized payments, and it introduced an unconditional ("no questions asked") right for in the case of direct debits in euros.
- In the **United States**, the Electronic Fund Transfer Act establishes the types of error resolutions that should be subject to dispute resolution (including unauthorized and incorrect transfers and errors in the bookkeeping, receipt, or statement). The act also establishes timelines

FIGURE 4 **Core Elements of a Holistic Dispute-Handling Mechanism**



Source: Own elaboration

for dispute and error resolution. If these timelines cannot be met, the financial institution needs to re-credit any disputed funds to the customer at least temporarily.

- In the **United Kingdom,** the customer needs to report an unauthorized transaction to the sending financial institution. If the financial institution finds clear evidence of a genuine mistake, it needs to send a request to the receiving financial institution to re-transfer the amount within 20 days of the complaint. In case the banks are unable to provide solutions for the disputes, customer can report to Financial Ombudsman Service to resolve the dispute.
- In **Nigeria**, the central bank provides general rules for handling disputes. Based on these, the Shared Agent Network Facility and stakeholders agreed on standard dispute-handling procedures to which the agents need to adhere in case of a failed or disputed transaction at an agent location. The rules mandate, for example, that the agent should capture the complaint in the logbook and upload the information for the client into the dispute form on the Shared Agent Network Facility app to initiate the resolution process. The client receives a copy of the dispute as proof. The framework also provides timelines for resolution.

The types and frequency of complaints should be regularly monitored by the PSP, the FPS operator, and the financial supervisory authority. Recurrent problems can point to underlying problems with product design, gaps in service standards, or the need to strengthen internal processes or standards. Periodically analyzing this information is therefore in the interest of the PSP and can be an important trigger for putting in place remedial measures. The same applies for FSP operators and regulators. The Banco de Portugal regularly collects and publishes statistics on complaints received, including which institution received the greatest number of complaints annually. This acts as a strong incentive for service providers in Portugal to have in place a robust policy for addressing customer grievances and to remedy problems identified through recurring complaints. Similar processes are also in place in Germany. In many countries, the frequency of mis-transferred funds and consumers having problems inputting the payee's information has supported the development and integration of services such as QR codes or the use of aliases. In Europe, the frequency of mis-transferred funds also highlighted the need to add an additional step into the payment process to double-check the recipient's information.

International best practice also calls for putting in place out-of-court options for those customers who are dissatisfied with the resolution suggested by the PSP. Depending on the country, these out-of-court options include nonprofit consumer advocacy groups, private or public ombudsman schemes, or dedicated consumer protection agencies of the government. In Germany, for example, the associations of financial institutions operate such an ombudsman scheme, which is free for clients. In Mexico, the government has put in place a dedicated consumer protection agency for financial services, while the Australian Financial Complaints Authority is a nonprofit entity with membership from industry and customer representatives. As a common characteristic, these out-of-court mechanisms are available to the client *after* the client has sought resolution through the financial institution, and they cover a broad range of financial services.

BOX 3 DISPUTE-RESOLUTION PROCESSES FOR MISTAKEN/FRAUDULENT TRANSFERS—THE CASE OF HONG KONG SAR, CHINA

The Hong Kong Monetary Authority worked with industry stakeholders to develop a detailed set of procedures for following up on reported mis-transfers by consumers. All banks and stored-value facilities need to follow the following procedures:

1. The payer needs to report the mis-transfer of funds to the payer's PSP. To be able to follow up on the complaint, the payer needs to provide proof of the transaction and to consent formally to the sharing of this information with the payee's PSP and, if needed, the Hong Kong police.
2. The PSP of the payer has to acknowledge receipt of the complaint by post, e-mail, or SMS no later than the close of business of the next business day after receiving the transferrer's report.
3. Within two working days after receiving the complaint, the payer's PSP has to contact the payee's PSP (a) to inform the transferee of the matter and (b) to confirm with the payee if any funds were mis-transferred and, if so, to obtain authorization to return the mis-transferred funds.
4. The payee's PSP then has to provide the payee with the necessary information to determine whether the funds were mis-transferred. This information can include the payee's bank statements, transaction records, or details of the relevant transaction, such as the payee's bank account number, transaction date, transaction amount, transactional channel, and transactional narrative (if any).
5. If the payee's PSP does not receive a response from the payee within a reasonable period, it should contact the payee through registered mail to obtain the authorization to return the mis-transferred funds.
6. The payee's PSP is responsible for documenting the work done and providing a written confirmation listing the dates, all the actions taken in negotiating with the payee, and the final results. This confirmation needs to be shared with the payer's PSP within 15 working days from the date of the receipt of the request.
7. Throughout the process, the PSP of the payer is also required to maintain proper records and documentation, so that it can answer queries raised by the payer.
8. The payer's PSP has to send a final written response to the payer within a reasonable period (normally not exceeding 20 working days from the date of the receipt of the payer's claim). The final written response should include written confirmation from the payee's PSP with details of the dates and all the actions taken in the negotiation and the results, without disclosing the personal data of the payee. Such information
   (a) Could assist the police to assess whether the matter suggests a case of crime; and
   (b) May facilitate the payer to consider taking further appropriate actions, if deemed necessary.
9. If the funds cannot be recovered through the above process, the payer's PSP has to inform the payer of available follow-up actions—such as reporting to the police or seeking independent legal advice on possible actions for recovering the funds.
10. Even after a negative written response has been given to the payer, both PSPs are obliged to continue helping the payer seek the payee's authorization to return the mis-transferred funds.
11. Once authorization is obtained from the payee to return the funds, the payee's PSP has to return the funds to the payer's PSP as soon as practicable. The payer's PSP then has to return the funds to the payer as soon as practicable.

The guidelines also require that all authorized institutions must train their staff sufficiently on how to handle enquiries regarding mis-transfers of funds and the type of assistance to provide to the customer.

Finally, banks and stored-value facilities have to undertake customer education through appropriate channels to remind customers to avoid errors while transferring fund transfers. This also includes a reminder that they should return any funds that were erroneously sent to them and informs them about possible criminal liability if they do not consent to this return.

Source: Hong Kong Monetary Authority and own elaboration

4 CONCLUSION

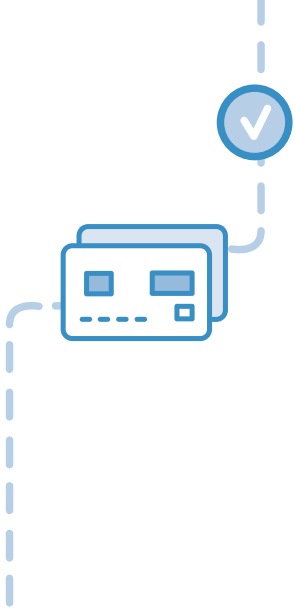
Fast payments are rapidly evolving around the world, and they increasingly involve non-bank PSPs and new access channels. So far, most non-banks have either remained indirect participants in FPS or focused on providing overlay services, but a number of countries are exploring options for letting them become direct participants. Fast payments also bring new benefits and challenges for the consumer, including new risks, such as the instant finality of payment transactions and the use of new access channels. Together with the integration of new service providers, this should be accompanied by an adequate consumer protection framework as detailed in this technical note.

When designing the consumer protection rules, particular attention has to be placed on ensuring a level playing field for all service providers involved while at the same time devising measures that remain commensurate with the risks of the involved services and providers.

International best practice highlights that the regulatory authority and/or the FPS operator should set clear rules and guidelines in the area of consumer protection, covering disclosure and transparency, business conduct, fair treatment of clients, and data privacy, and mandating the existence of accessible and effective dispute-resolution mechanisms. The note has highlighted a number of approaches that countries have taken to implement these mechanisms.

Consumer protection guidelines, however, can also be drivers for market development and innovation. The introduction and increasing acceptance of QR codes and other app-based services have not only had a positive impact on uptake of services by consumers but also, with the right customer-centric and protective design, positively affected how easily payers and payees can be identified or information can be made transparent to customers. The guidelines and standards determined by regulators and system operators should bear this in mind when working on approaches to address consumer protection.

Finally, consumer protection measures need to be complemented with information and education campaigns for customers. Harmonized standards, design, or mechanisms can facilitate outreach to customers in a cost-effective way.



5 ACKNOWLEDGMENTS

Organization	Contributor
Central Bank of Portugal	Maria Lúcia Leitão
	David M. Pereira
	Patrícia Guerra
Deloitte India	Deloitte India
Financial Services Regulatory Authority, Canada	Taryn Pimento
	James Langlois
	Fern Karsh
The International Financial Consumer Protection Organisation (FinCoNet)	Cathy Kelly
Organisation for Economic Co-operation and Development (OECD)	Miles Larby
	Matthew Soursourian
Reserve Bank of Australia	Richard McMahon
	Daniel Chippeck
	Fisher Chay
World Bank	Ilka Funke (Lead Author)
	Margaret J. Miller
	Gian Boeddu
	Harish Natarajan
	Nilima Ramteke
	Holti Banka

NOTES

1. According to the Committee on Payments and Market Infrastructures, 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 an overview of the benefits and risks of digital financial services, see Organisation for Economic Co-operation and Development, *Financial Consumer Protection Policy Approaches in the Digital Age: Protecting Consumers' Assets, Data and Privacy* (OECD 2020).
3. Consultative Group to Assist the Poor (CGAP).
4. See, for example, Task Force on Financial Consumer Protection, *G20 High-Level Principles on Financial Consumer Protection* (OECD, 2011) and World Bank Group, *Good Practices for Financial Consumer Protection: 2017 Edition* (World Bank, 2017).
5. The *G20 High-Level Principles* covers (i) the legal, regulatory, and supervisory framework, (ii) the role of the oversight body, (iii) the equitable and fair treatment of consumers, (iv) disclosure and transparency, (v) financial education and awareness, (vi) responsible business conduct of financial service providers and authorized agents, (vii) the protection of consumer assets against fraud and misuse, (viii) the protection of consumer data and privacy, (ix) complaints handling and redress competition, and (x) competition.
6. See World Bank Group, *Good Practices for Financial Consumer Protection*, annex A (Retail Payment Services).
7. See, for example, the Electronic Fund Transfer Act in the United States, the law on transparency and regulation of financial services (2018) in Mexico, or the guidelines on financial consumer protection issued by the People's Bank of China in 2020.
8. Consultative Group to Assist the Poor (CGAP).
9. *G20 High-Level Principles*.
10. Order of the People's Bank of China (2020) No. 5 pertaining to implementation measures for the protection of the rights and interests of financial consumers.
11. http://fitproper.com/documentos/referenciales/Good_Practices_Financial_CP.pdf
12. From the speech of the Governor of Central Bank of Ireland, https://www.bis.org/review/r170310b.pdf.
13. SPEI grants access only to financial institutions that are supervised by one of the national government bodies in charge of supervising financial institutions. Financial cooperatives (*Cooperativas de Ahorro et Crédito*), for example, are under a delegated supervision scheme and thus not part of the scheme yet. All scheme participants need to comply with the same set of requirements, which ensures equal access.
14. For example, Banco de México introduced an obligation for banks to offer retail payments for payments below Mex$8,000 (currently about $390) on a 24-hours-a-day, seven-days-a-week basis.
15. For a discussion of fee structures, see, for example, European Consumer Organisation, *Consumers and Instant Payments* (BEUC, 2021), https://www.beuc.eu/publications/beuc-x-2021-027_consumers_and_instant_payments.pdf.
16. For a discussion of fee structures, see, for example, European Consumer Organisation, *Consumers and Instant Payments* (BEUC, 2021), https://www.beuc.eu/publications/beuc-x-2021-027_consumers_and_instant_payments.pdf.
17. World Bank Group, *Good Practices for Financial Consumer Protection*, annex A (Retail Payment Services), and World Bank, *Consumer Risks in Fintech: New Manifestations of Consumer Risks and Emerging Regulatory Approaches* (World Bank, 2021).


WORLD BANK GROUP