TC NOTES

PRACTICAL **LEADERSHIP**
AND **GUIDANCE** FROM
TORONTO CENTRE

REGULATION AND SUPERVISION OF RETAIL PAYMENT SYSTEMS

JANUARY 2023

TORONTOCENTRE
Global Leadership in Financial Supervision

Global Affairs Canada
Affaires mondiales Canada

Sida
SWEDISH INTERNATIONAL DEVELOPMENT COOPERATION AGENCY

REGULATION AND SUPERVISION OF RETAIL PAYMENT SYSTEMS

TABLE OF CONTENTS

REGULATION AND SUPERVISION OF RETAIL PAYMENT SYSTEMS

Introduction[1]

Payment systems are the rails on which financial transactions – person to person (P2P), person to business (P2B), business to business (B2B), person to Government (P2G), Government to business (G2B), and Government to person (G2P) take place. The efficient functioning of these rails enables a faster and frictionless exchange of goods and services, and contributes to economic growth, financial inclusion, and financial stability. During the past two decades, central banks and other supervisory authorities have recognized the importance of retail payment systems and have taken several regulatory and supervisory measures.

Historically, banks were the key providers of payment services. Since the transaction accounts of payers are primarily with banks, the discharge of payment obligations can happen through banks. Banks can be subject to regulation and supervision for both their banking business by banking supervisors, and for their payment services – either by the banking supervisors or by supervisors designated in payment system legislation. But new issues for regulation and supervision have emerged from the use of innovative technology in accessing transaction accounts, and the entry of non-bank players (including FinTech and Big Tech) to the provision of payment services.

Payment systems are of two types:
Large Value Payment Systems (LVPS). These meet the needs of wholesale financial market participants through individual transactions that are large in value but low in number. Their processes are highly standardized and closely supervised by central banks because of their systemic implications and because central banks also use these systems for their monetary policy operations. Central banks and securities supervisors have collaborated to evolve the principles of financial market infrastructure for regulating and supervising financial market infrastructures, including LVPS.[2]

Retail Payment Systems (RPS). The public uses RPS for day-to-day transactions, which are low in value but very large in number. These systems are varied, voluminous and fast-changing. The users of RPS include individuals, households and small businesses with different demographic, economic, and social circumstances. There are many payment instruments (cash, cheque, payment cards, online funds transfer), payment channels (point of sale, internet, mobile, ATM, contactless cards, wearable devices), and institutions (banks and non-banks) providing payment services.

This Toronto Centre Note focuses on the regulation and supervision of RPS. These offer considerable advantages for their users, and scope for competition and innovation. But they also carry risks to their users, and in some cases to financial stability.

---

[1] This Toronto Centre Note was prepared by Abhaya Prasad Hota. The author thanks Clive Briault for his editorial suggestions. Please address any questions about this Note to publications@torontocentre.org
[2] Committee on Payment and Settlement Systems and Technical Committee of the International Organization of Securities Commissions (2012).

The importance of efficient digital RPS was highlighted during the COVID-19 pandemic. A near-normal digital payment infrastructure meant that funds transfers and the online ordering of goods and services could be carried out seamlessly in many countries. National governments could make disaster relief payments to millions of beneficiaries without any time lag, and social distancing norms could be easily met.

Regulatory and supervisory authority

Any financial service, including payment systems, needs a sound legal basis to regulate and supervise it. There is no standard definition of "retail payment system" adopted by all countries in their respective payment system legislation. India, for example, defines a payment system as one that:

"[E]nables payment to be effected between a payer and a beneficiary involving clearing, payment or settlement service or all of them, but does not include a stock exchange. This includes the systems enabling credit card operations, debit card operations, smart card operations, money transfer operations or similar operations."

Legislation usually provides powers for a responsible authority (or authorities) to authorize an institution to offer payment services; to issue regulatory standards and supervisory guidelines; to monitor adherence to these rules and guidelines; and to intervene as necessary through supervisory intervention and the use of formal enforcement powers.

In many countries the central bank undertakes these roles for RPS. This is often for historical reasons (for example, many central banks used to manage cheque clearing systems) or because the central bank has played a role in developing the payment systems.[3] Indeed, the Committee on Payment and Settlement Systems[4] published a report in May 2005 on central bank oversight of payment and settlement systems, which stated:

"*Oversight of payment and settlement systems is a central bank function whereby the objectives of safety and efficiency are promoted by monitoring existing and planned systems, assessing them against these objectives, and where necessary, inducing change."*

However, country practices vary and have been evolving rapidly, as described in Box 1. As with national stock exchanges, clearer distinctions have been introduced between the operators of RPS and their regulators/supervisors, not least to avoid conflicts of interest.

Box 1: Regulatory and supervisory authorities for RPS: some examples

In the **United States**, RPS regulation and supervision is dispersed across multiple states and federal authorities. It is treated more as a consumer protection issue than a service requiring banking-style regulation and supervision. However, the Federal Reserve plays a key role in standard setting, compiling statistics, research, etc. The Federal Reserve also acts as a significant RPS operator in competition with private players, particularly in

[3] In India, the Reserve Bank of India was the regulator, supervisor, and operator for the bulk of the RPS (except for the card payment system) until the commercial banks established a retail payments utility in 2009.

[4] The Committee on Payment and Settlement System (renamed in 2014 as the Committee on Payments and Market Infrastructures) is an international standard setter that promotes, monitors, and makes recommendations about the safety and efficiency of payment, clearing, and related arrangements.

cheque clearing, automated clearing house processing, and the new retail instant payment service called Fed Now.

In the **United Kingdom**, a new Payment System Regulator was created in 2013 to regulate and supervise major RPS.

In **Japan**, RPS are overseen primarily by the clearing networks set up by the bankers' association on a self-regulation basis, with minimal intervention from government or the central bank. Recently, however, the legislation was amended to transfer oversight responsibility to the Bank of Japan.

In **Australia**, RPS are regulated by a combination of regulators, self-regulatory bodies, and federal government.

In **Canada**, Payments Canada operates the key payment, clearing, and settlement systems on a self-regulation basis, supervised by the Bank of Canada.

Similarly, in **South Africa**, the Payments Association of South Africa operates as a self-regulatory payment system management body, recognized in legislation, to help the South African Reserve Bank manage payment systems.

In some countries, government departments dealing with financial services issues have taken administrative consumer protection actions on RPS in areas such as complaints handling, financial literacy, amount limits for card payments, and fraud prevention.

Supervisory objectives and approaches

The **objectives of RPS regulation and supervision** also differ across countries. These objectives typically include some combination of:

- Maintaining the safety and security of payment systems.
- Maintaining the operational resilience of payment systems.
- Promoting the efficiency of payment systems.
- Protecting consumers.
- Effectively handling complaints and redress.
- Promoting competition in the market for payment services.
- Supporting financial stability.
- Supporting financial inclusion and affordability, financial literacy, and gender equality.

Some of these objectives may be shared between the payment system regulatory and supervisory authority (or authorities) and other authorities. For example, in some countries general consumer protection laws cover payment services as well.

Depending on its country-specific mandates/objectives, each relevant regulatory and supervisory authority for RPS needs to establish the usual **key components of supervision**, including:

- Setting standards for regulated entities through rules and guidance, in addition to any requirements set through national legislation.
- Designating some major RPS providers and operators as systemically important, where appropriate, and subjecting them to higher regulatory standards and more intensive and intrusive supervision.[5]
- Authorizing entities, and – where applicable – introducing an "approval" or "suitability" regime for key individuals within some or all regulated entities.[6]
- Using regulatory reporting, off-site analysis, and on-site reviews, examinations (including visits to processing centres), and interviews with directors, senior management, and heads of control functions to build an understanding of a regulated entity's risks, governance, and risk management.[7] Since RPS may involve multiple regulated entities, including some small entities, it may not be possible or risk-based for supervisors to undertake on-site visits to all regulated entities.[8]
- Using a risk-based and proportional approach to supervision, including an assessment of the risks to supervisory objectives posed by each regulated entity; the potential impact if these risks occurred; and the governance, controls, and financial resources of the regulatory entity.[9] Table 1 sets out some key supervisory concerns and issues relating to various RPS entities and activities.
- Conducting supervisory interventions in response to risk assessments and breaches of regulatory requirements and supervisory expectations.[10]
- Launching disciplinary and other enforcement actions.

Most supervisors of RPS rely heavily on **reporting by regulated entities**. Regular reporting typically includes:

- Volume and value of transactions during the period.
- Number of active customers (senders and receivers).
- Number of corporate customers using RPS to pay salary, pension, and dividends, or to collect bills.
- Digital payment infrastructure data such as the number of automated teller machines (ATMs), Point of Sale (POS) or Quick Response Code-based acceptance points, or the number of merchants acquired for POS and e-commerce transactions.
- System downtime, if any, and whether payment system operators (PSO) or payment service providers (PSP)[11] could resume operations within a timeframe specified by the supervisory authority.
- Number of customer complaints received, and the number pending beyond the turnaround time specified by the supervisory authority.
- Geographical footprints of the transactions, if the supervisory authority has mandated geo-tagging transactions.
- Major changes in systems and procedures at the regulated entity.

[5] See Committee on Payment and Settlement Systems (2001).
[6] See Toronto Centre (2017a) for a discussion of suitability regimes for individuals.
[7] Toronto Centre (2022) discusses the use of on-site interviews to assess the quality and effectiveness of a financial institution's corporate governance.
[8] See Toronto Centre (2020) for a discussion of how to apply risk-based supervision to smaller firms.
[9] A series of Toronto Centre Notes describe the key features of risk-based supervision. In particular, see Toronto Centre (2018a and 2018b).
[10] See Toronto Centre (2019a).
[11] See Table 1 for a description of these and other entities involved in retail payment systems.

Supervisory authorities are increasingly using technology and analytical tools ("Sup Tech") to **process data collected from regulated entities**. These tools help supervisors monitor risks and compliance with standards, and identify outliers and trends. They also help develop the relationship of payment system data with other economic indicators, including those relating to financial inclusion. For example, these tools can help supervisors identify the risk of a PSO or PSP:

- Failing financially.
- Not adhering to appropriate governing standards.
- Not being able to handle payment system transactions efficiently.
- Not using fraud prevention tools and security control guidelines.

Supervisors can also call for additional reports and information from regulated entities based on warning indicators. These warnings may come from regular reporting, market feedback, information received from other authorities, or specific events (such as conduct and resilience failings) at individual regulated entities.

Supervisors in some countries have made use of innovation testing "sandboxes," especially for innovations that appear to introduce new services or new processes that should benefit consumers, but where the appropriate regulatory and supervisory approach is uncertain. Live testing takes place in a controlled and carefully monitored environment so the potential impact can be assessed.[12]

Regulated Entities (REs) and activities

Unlike large value payment systems, retail payment systems are varied. They range from long-standing cheque-clearing processes to newer systems such as instant payments, invisible payments, or contextual payments (see Table 1). Faster payment systems that facilitate real-time fund transfers are increasingly common. Private crypto asset-based payment transactions in retail sectors are also being experimented with in a few countries, as are Central Bank Digital Currencies (CBDC).

Table 1: Retail Payment Systems entities and activities

Entities and activities	Description	Primary regulatory and supervisory concerns
Payment Service Providers (PSPs) Banks and non-banks that maintain transaction accounts for customers and facilitate retail payment	A **Payer PSP** must arrange payment if the customer is authenticated and the customer has adequate balance in their account. The PSP at the beneficiary's end is called a Receiver PSP. A **Receiver PSP** can also initiate a payment transaction by placing a "collect" request to the Payer PSP, who in turn organizes the authentication of the payer. PSPs can also appoint outsourced partners such as third-party application service	The supervisory objectives of ensuring the safety, security, and efficiency of payment systems may best be achieved through a heightened focus on a PSP's operational resilience and on consumer protections such as complaint handling mechanisms.

[12] See also Toronto Centre (2017b).

transactions through various channels (branches, internet, ATM, mobile etc.)	providers that provide the interface to business correspondents and agents to facilitate easy access by retail customers. The entry of FinTechs and Big Techs as these third parties is rapidly changing the RPS landscape.	
Payment System Operators (PSO) There can be several types of PSO based on payment instruments or payment channels, including: • ATM/POS Network • Mobile Payment Systems • Automated Clearing House operators for bulk and repetitive transactions • Faster Payment System • Bill Payment System or Toll Collection System • Cross-border payment system • Credit Card system • Card Networks	**PSOs** provide the technology platforms for PSPs to connect and exchange payment information. PSOs, in consultation with the PSPs, prepare the technical standards for connectivity and operating procedures for inter-bank settlement. They used to be called the "Clearing House" when cheque clearing was the dominant form of RPS. **ATMs** - Over the years, ATMs have increasingly allowed customers of one bank to use ATMs operated by a different bank, facilitated by switching and settlement arrangements provided by the ATM networks. These networks also offer clearing and settlement of POS transactions. **Mobile Payment System** – Making payments through a mobile phone has become common in many countries. This channel-specific payment system may cover payments for all purposes – bill payment, P2P funds transfer, e-commerce payment, or even B2B payments. Usage is growing in all of these categories. It has evolved from SMS-based payment to Unstructured Supplementary Service Data (USSD) and App-based payments. Near Field Communication (NFC)-based smart phones can also be used as contactless payment cards. **Automated Clearing House (ACH) system** – Designed for bulk and repetitive payments like salary, pension, annuity, and dividend payments, utility bill payments, and periodic instalment payments to repay loans. There are also examples of bill repositories and bill aggregators. The utility providers upload the bills as generated, and the	The degree of regulatory and supervisory attention to PSOs may depend in part on the volume and value of transactions, the customer base, the importance of the operators to trade and commerce in the economy, and the degree of exposure to issues such as cyber security. A separate authorization/license is usually issued for each PSO. There may also be umbrella payment entities with multiple PSOs.[13] The supervisory focus on PSOs has been primarily on using off-site and on-site supervision to assess a PSO's: • Corporate governance • Operational resilience • Security of transactions • Adoption of technical standards • Fair treatment of consumers.

[13] For example, the National Payments Corporation of India is licensed to operate eight different payment systems, with each system having its own membership and operating guidelines.

	aggregators ensure collection through a variety of payment systems as opted for by the customers – ACH being just one of them. FinTech firms have offered a new user experience by creating a database of all types of bills a customer pays. **Faster Payment Systems** (FPS) provide real-time fund transfers, enabling instant credit to beneficiary accounts – on both a "send" and a "collect" basis. Experiments are in progress to interlink national FPS systems for **cross-border payments**. Once payment instruction reaches the destination bank, the transaction is handled like any other domestic transaction. Since the cost of remittance is often still very high (around 5% of remittance value), central banks and other authorities have been seeking simplifications and cheaper alternatives, including interconnecting the domestic remittance networks of multiple countries for real-time fund transfers. **Card payment systems** have evolved during the last 50 years, from credit cards to ATM cards to debit and prepaid cards. Global Card Networks collaborated to introduce international standards in card design and institutional identification numbers. They have also reviewed security standards in the form of Payment Card Industry Data Security (PCI-DSS) and Payment Application Data Security Standard (PA-DSS).	Cross-border payments can result in foreign exchange restrictions overlapping with payment system regulation and supervision. Cross-border payment systems are therefore regulated by both foreign exchange regulators (usually the central banks) and payment system regulators. Cross-border transactions are also typically subjected to more rigorous anti-money laundering and countering terrorist financing checks. A credit card system has an added regulatory and supervisory dimension due to the element of credit underwriting. This aspect of credit card payment is typically handled by the regulatory authority dealing with credit. Only issues related to transaction processing fall under the domain of the payment system regulator.
Pre-Paid Issuers (PPI) **Wallet service providers** **e-Money Issuers**	**PPI** and **e-Money issuers** can be banks or non-banks that hold prepaid transaction accounts and enable account holders to make low-value payments without having to access bank accounts. They can be closed-loop (accepted only at the outlets of the issuer), semi-closed (accepted within a network where the issuer has an arrangement with the network participants), or open (accepted at all outlets conforming to technical and participation standards).	The degree of supervision may depend on the volume and value of transactions. The supervisory focus here tends to be mostly on: • Consumer protection – treating deposits

	The bulk of PPI operators are FinTech firms, which have brought significant improvements in customer experience. E-commerce marketplaces such as Amazon have also sought PPI licenses in many geographies so they can provide a better payment experience for sales taking place on the platform. Some non-bank e-lending firms have started disbursing loans to borrowers' pre-paid accounts instead of bank accounts, thereby increasing the volume and value of pre-paid transactions.	with e-Money providers similarly to bank deposits through escrow arrangements for non-bank issuers, and imposing a ceiling on the amount of balance that can be kept in the PPI accounts. • Security of transactions. • Operational resilience.
Payment Aggregators and Payment Gateways	Large commercial entities handle voluminous transactions – for both payments and collections. Specialist institutions like **Payment Aggregators** have emerged to play an intermediary role, particularly for the collection of e-commerce transactions. They act as the bridge between merchants and the acquiring banks. They enable the merchants to collect their proceeds through various payment systems using the payment gateways. They process sensitive payment system data, and act as the custodian of the collected proceeds of the merchants until passed on to them. Therefore, in many geographies they are subjected to regulation. **Payment Gateways** are platform providers that facilitate transactions of various types through various channels for clearing and settlement.	The supervisory focus here relates to the nature of the operations of payment aggregators as collecting agents for merchants. Supervisors need to focus on the additional risks this generates in the form of credit and liquidity risks to the merchants if the aggregators fail to transfer the collected proceeds on time.

Regulatory and supervisory responses to developments in retail payment systems

The retail payment systems landscape has changed substantially during the past decade, due to the accelerated adoption of digital payments and the entry of FinTech firms offering digital payments. These developments – common to almost all countries – have given rise to several new RPS systems that have supplemented or replaced the previous "plain vanilla" systems. Many new operators and service providers have entered the payment systems space and have been operating on the fringe of regulation and supervision.

New RPS have brought many advantages for consumers, including the availability of new products, payment channels and services; greater convenience and flexibility; and greater innovation and competition. This in turn has enhanced financial inclusion. However, this has also brought risks, not least for consumer protection and financial stability. These risks include weaknesses in the financial viability and governance of some new entities; data privacy concerns; mis-selling risks; a lack of transparency and disclosure; cybersecurity risks; and unregulated entities operating outside the regulatory perimeter.[14]

In response to these developments and risks, regulators and supervisors of RPS usually focus on the following key areas:

Periodic review of regulatory architecture

A common approach to the regulatory and supervisory architecture for RPS is to consult with stakeholders and publish a medium-term **Vision Document** or **Strategic Action Plan**. In addition to the government, central bank and supervisory authorities, stakeholders include payment system operators, payment service providers, consumers, and consumer forums. Some countries have built formal consulting expert panels, advisory groups, and task forces. These may be helpful in the co-ordinated development of RPS, and in determining proportionate regulation and supervision for emerging payment systems or emerging entities.

An action plan may include:

- More clearly defining the regulatory and supervisory authority, and any institutional changes required by country-specific circumstances.
- Bringing previously unregulated activities/entities into the regulatory perimeter.
- Creating new frameworks for authorization, regulatory reporting, supervision, and enforcement.

Box 2: Action plan examples

The Government of **Australia** commissioned a detailed review of payment systems in 2020, which made several recommendations 'to ensure that the regulatory architecture is fit-for-purpose for the years to come.' The recommendations included expanding the scope of the Reserve Bank of Australia's designation power; introducing a new designation power for the Treasurer; and introducing a single, tiered payments licensing framework that replaces the need for providers to obtain multiple authorizations from different regulators.

In **Canada,** extensive discussions and debates resulted in major reforms to the Retail Payments Activities Act in June 2021. The Act provides the legal framework for the Bank of Canada to supervise payment service providers. It complements initiatives by Payments Canada, which had a mandate through the Canadian Payments Act to establish and operate national systems for payment clearing and settlement.

In the **United Kingdom**, HM Treasury was planning during 2022 to expand the regulatory perimeter to capture new types of systemic payment firms, following the growth of FinTech companies and crypto assets.

[14] See Toronto Centre (2019b, pages 7-9) for a fuller discussion of these risks.

In **India**, the central bank and the designated regulator and supervisor for payment systems has developed an action plan that includes:

- reviewing the relevant legislation to broaden the scope of regulation;
- establishing a Payments Advisory Council to help regulate and supervise payment and settlement systems;
- considering a framework to regulate and supervise all significant intermediaries in the retail payments system;
- revisiting guidelines for pre-paid instruments and mobile wallets; and
- setting up Self-Regulatory Organizations for some payment system activities.

Self-Regulatory Organizations in Retail Payment Systems

As the number of RPS proliferate, it may be useful for regulators and supervisors to ask payment system operators and service providers to develop their own standards in areas such as system security, service charges, customer protection, and complaint handling. This can be achieved by creating Self-Regulatory Organizations (SROs), recognizing them as industry bodies for consultation, and authorizing them to implement the standards once approved by the supervisory authority. SROs can therefore be granted some authority, and can themselves be supervised by the supervisory authority in terms of how they exercise this authority. This can release supervisory resources that can be better focused on issues of systemic importance.

There can be more than one SRO for RPS players, including:

- PSOs in ATM deployment;
- Pre-paid Instruments;
- Merchant Acquirers; and
- Payment Gateways and Payment Aggregators.

Consumer protection

When assessing the risks to consumers in both established and new RPS, supervisors have typically focused on:

Disclosure and transparency – Consumers should be provided with adequate information about the risks, benefits, and liabilities of using digital payment products and related services before they subscribe to them. This should include the customer privacy and security policy. Consumers should also be informed clearly and precisely about their rights, obligations, and responsibilities related to digital payments and any problems that may arise from service unavailability, processing errors, and security breaches.

Security – Consumers should be made aware of commonly known threats such as phishing, vishing, reverse-phishing, and remote access of mobile devices. They should also be advised on how to safeguard their account details, credentials, PIN, card details, devices, etc.

New features - Whenever new operating features or functions are introduced to online delivery channels, consumers should receive clear instructions to properly use these features. This is particularly important for features relating to security, integrity, and authentication.

Complaints – RPS providers should be clear about how a consumer can file a complaint, how a complaint will be handled, and the timeline for responding to and resolving a complaint. In some countries, supervisors have set maximum timeframes for dealing with a complaint. Some have

established a Digital Payment Ombudsman, in addition to an Ombudsman for other financial services, to whom consumers can take complaints if they have not been resolved to their satisfaction by the RPS provider.

Operational resilience

The concept of operational resilience, and the ways in which financial sector supervisors can assess it, are discussed in Toronto Centre (2021). Operational resilience covers controls and measures to both (a) prevent operational disruptions from occurring, and (b) enable rapid response to and recovery from disruptions that do occur, so key systems can be restored as soon as possible.

To be efficient and effective, an RPS needs to provide continuous availability and accessibility; safe initiation of payment transactions; an assurance that beneficiaries will receive funds according to payment system rules; and the privacy and integrity of customer data. This in turn depends on the operational resilience of the RPS. Supervisors should therefore pay particular attention to whether system operators and other providers have sufficient operational resilience in areas such as:

- High availability infrastructure with fallback arrangements to ensure transaction processing continuity. This includes setting up disaster recovery arrangements so the failure of a primary site does not affect business continuity.
- Regular disaster recovery drills.
- Scalable architecture with an ability to create additional capacity with minimum time lag.
- Sound operating practices.
- Regular upgrades of technology infrastructure (hardware, systems software and application software).
- Usage data that show the level of free space available to process peak volume.
- Recovery time and recovery point objectives to minimize loss of data and disruption.
- Industry-approved standards for business continuity (such as ISO 23001), information security (such as ISO 27001), and data security.
- An adequate number of trained staff.

Supervisors should have the authority to penalize RPS providers and operators for serious or repeated service disruptions, and for failures to restore services within a specified timeframe (such as within 24 hours) after a disruption. For example, the Monetary Authority of Singapore recently imposed additional capital requirements on a commercial bank for disruptions to its digital retail banking services. The Reserve Bank of India has restricted a large commercial bank from issuing credit cards to new customers until it can demonstrate sufficient operational resilience.

Cyber security

Cyber attacks are an important potential source of operational disruptions and fraudulent activities. Cases of cyber frauds in RPS have grown rapidly with the growth of digital payments. Fraudsters are working hard to penetrate the security walls of PSOs and PSPs. Their techniques aim to deceive and manipulate consumers into giving out confidential information like account numbers, payment card numbers, date of birth, or passwords.

It is not possible to anticipate and prevent all cyber attacks, but supervisors should expect RPS entities to have strong protections in place. They should also be able to recover rapidly from a

cyber attack and restore key systems, products, and services. Toronto Centre (2018d) covers the supervision of cyber security risks for all financial institutions. RPS supervisors should focus in particular on assessing whether entities have in place the controls listed in Box 3.

Box 3: Cyber security controls for digital RPS

Generic security controls

- Secure communication protocols for digital payment channels.
- Protection and safe storage of sensitive information.
- Firewalls and Distributed Denial of System (DDoS) mitigation techniques.
- Effective logging and monitoring capabilities to track user activities.

Application Security Life Cycle

- "Security by design" approach to developing digital payment products and services.
- Multi-tier application architecture to segregate the application, database, and presentation layers in digital payment system applications.
- Regular security testing, including review of source code, vulnerability assessment and penetration testing of digital payment system applications.

Authentication Framework

- Use of multi-factor authentication.
- Blocking accounts after a set number of failed log-in or authentication attempts.

Fraud Risk Management

- PSOs and PSPs should document and use a process for identifying and reporting suspicious transactional behaviour.
- Monitoring of system alerts for transaction velocity, excessive activity on a new account, unusual patterns, prohibited zones/rogue IPs, etc.
- Fraud analysis to identify the reason for fraud occurrence and to determine how to prevent such frauds.
- Staff training in fraud prevention.
- Incident response and business continuity planning.

Data Privacy and Data Storage

- Maintaining the confidentiality of customer data.
- Meeting data security standards (for example PCI-DSS and PA-DSS).

Financial inclusion

Digital channels for making deposits, paying remittances, and paying utility and other bills can be a convenience for consumers and small businesses. They are also ways to create a credit profile that can make it easier to access credit. In this context, digital RPS can become critical to meeting financial inclusion objectives. This direct relationship between financial inclusion and inclusive digital payment systems is discussed in G-20 High Level Principles for Financial Inclusion (2016) and the CPMI-World Bank Report on Payment Aspects of Financial Inclusion (2016).

Supervisory authorities can play a role in enhancing financial inclusion through their actions to protect consumers; to require payment systems to be robust, safe, and efficient; to foster competition and innovation; and to improve levels of financial literacy.[15] To meet objectives relating to access, financial inclusion, and gender equality, some supervisory authorities require that system operators and service providers allocate time and efforts to set up digital acceptance points in remote areas and promote consumer awareness and understanding. Or they may require that operators and service providers contribute to a retail payment infrastructure development fund.

Supervisory authorities can also collect data that can be used to monitor progress on financial inclusion. For example, the availability of financial services in a remote area can be captured from the number of new-to-formal finance customers sending or receiving money. Payment system data can also show access and usage by women and men.

Supervisors may also have an interest in RPS pricing. This may be because affordability for consumers is important for delivering financial inclusion. It may also be because collusive or monopolistic pricing is judged unfair for consumers, or is contrary to a supervisory authority's competition objective.

Interoperability

Regulators and supervisors may play a role in promoting interoperability in RPS. In particular, they may require that all operators and providers meet common technical standards that enable them to receive and act upon payment messages from other entities. "Open Banking'' and ''API Banking" technology has developed in recent years, enabling the sharing of bank-held customer permissioned data under a regulated framework. The importance of this approach, and related regulatory and supervisory concerns, are explained in the Basel Committee Report (2019) on open banking and application programming interfaces.

Card payment mechanisms (credit card and debit card) are completely interoperable in many countries, even globally. Cards of most issuers can be accepted by merchants with very little customization due the adoption of common technical standards. Pre-paid cards also tend to be interoperable, although this is limited when the pre-paid instrument is in the form of a mobile wallet. With the maturity of mobile payment systems, attempts are being made to make pre-paid instruments (other than in card form) more interoperable, such as through QR code-based payment mechanisms. Some regulators have mandated the interoperability of all types of pre-paid instruments to fast-track digital adoption.

Non-bank Pre-Paid Issuers (PPI)

Pre-Paid Issuers hold the funds of their customers in their fiduciary capacity, and the amount involved is often quite large. Regulators and supervisors in many countries therefore require non-bank pre-paid issuers to maintain outstanding balances in an escrow account with a commercial bank. The amount so maintained should be used only for making payments to participating merchant establishments/beneficiaries; and no loan should be permissible against such deposits.

[15] These supervisory actions are consistent with the CPMI-World Bank Report on Payment Aspects of Financial Inclusion (2016), which highlighted the importance of efficient, accessible, and safe retail payment systems for greater financial inclusion.

FinTech and Big Tech

Retail payment services that used to be the monopoly of banks are increasingly being provided by non-bank service providers, in particular those using various forms of FinTech.

One concern relates to competition, in particular where large technology-based firms (Big Techs) may dominate a market.[16] During the last 10-15 years, these Big Techs have captured a sizeable market share in digital payments in some countries, and indeed globally. Since their operations are global and the platforms built for one geography can easily be used for multiple geographies, they have the potential to roll out new services faster and cheaper than smaller competitors. Big Techs such as Google Pay, Amazon Pay, Apple Pay, WhatsApp Pay, and Facebook Pay have global ambitions. In China, two players – Alipay (owned by Alibaba, the China equivalent of Amazon) and WeChat Pay (owned by Tencent, the China equivalent of Facebook) – dominate the retail payment space.

In some countries, this risk has been left to the competition authorities, with no role assigned to the payment system regulator. But in other countries, the payment system regulator has imposed volume restrictions on the processing of transactions by Big Techs. In India, the Big Techs participating in the most popular faster payment system, the Unified Payments Interface, built a market share of more than 90% of the monthly volume of about 6.5 billion transactions a month. As a regulatory move, a volume cap of 30% of the system volume for a single entity has been introduced. In addition, a cap of 100 million registered users for payment transactions has been imposed on WhatsApp Pay, although WhatsApp has a user base of 400 million in India for other services. Discussion on a "light touch" regulation over Third Party Application Providers has also begun.

Crypto assets and Central Bank Digital Currency

Crypto assets are a virtual form of money secured by cryptography and exchanged for value as agreed between the users, not by any legal authority as is the case with paper currency. The exchange value is determined by demand (supply being limited) and acceptance of currency by choice.

Large crypto asset exchanges – such as Bitcoin, Bitcoin Cash, Ethereum, Ripple, USD Coin, and Gemini – claim their coins are now being widely used as an alternative instrument for retail payments, even for small transactions. Bitcoin is accepted in some countries as payment for rent and utilities.

Regulatory concerns arise in part because it is still not clear which specific activity to regulate, or whether a payments system regulator should step in with regulatory and supervisory measures.

Central Bank Digital Currency (CBDC) is another emerging development. Many central banks across the world are either examining or have expressed interest in issuing CBDC. This is partly as a digital alternative to currency notes, and partly as a response to the challenges posed by private crypto asset issuers.

[16] Financial Stability Institute (2021) also identifies the potential of Big Techs to emerge as monopolies by taking over smaller service providers and using their technical and financial power as a major concern.

A few central banks in the Caribbean region and Africa, the People's Bank of China, and Reserve Bank of India have launched CBDC as experiments. A dozen more central banks are likely to launch during 2022-25. A common thread running through these experiments is that the CBDC is being issued and circulated to the public through a network of financial institutions, as happens with paper-based currency, rather than directly to the public. While some central banks plan to issue token-based CBDC, others are planning for account-based CBDC, like wallets.

Once its issuance occurs in a big way, CBDC would have to be designated as another retail payments system, operated by the central bank. It is now being debated how to regulate and supervise CBDC.

Conclusion

Retail payment systems are varied, and there are many operators and service providers. The principles for financial market infrastructures do not all apply to the supervision of RPS. However, certain key elements such as the collection of data (transactional data and incidences of failed resilience) are treated as basic tools for off-site surveillance. Therefore, timely reporting of data (preferably in standardized format) by various categories of PSOs and PSPs becomes crucial.

A risk-based and proportional supervision approach - based on the surveillance data, other information reported to the supervisory authority, and on-site supervision - can be taken to the assessment of risks to supervisory objectives. These objectives typically include some combination of the safety and security, operational resilience, and efficiency of payment systems; consumer protection and effective complaints handling; promoting competition; financial stability; and financial inclusion.

Supervisory interventions can then be undertaken where appropriate to reduce inherent risks, to improve governance and controls, and to enhance the robustness and financial resources of RPS entities.

References

Basel Committee on Banking Supervision. *Report on open banking and application programming interfaces*. November 2019.

Committee on Payment and Settlement Systems. *Core Principles for Systemically Important Payment Systems*. January 2001.

Committee on Payment and Settlement Systems. *Central bank oversight of payment and settlement systems*. May 2005.

Committee on Payment and Settlement Systems and Technical Committee of the International Organization of Securities Commissions. *Principles for financial market infrastructures*. April 2012.

Committee on Payments and Market Infrastructures and World Bank Group. *Payment aspects of financial inclusion*. April 2016.

Financial Stability Institute. *Fintech and payments: regulating digital payment services and e-money*. July 2021.

G20. *High-Level Principles for Digital Financial Inclusion*. July 2016.

Toronto Centre. *Assessing the Suitability of Key Individuals in Financial Institutions*. May 2017a.

Toronto Centre. *Regulatory Sandboxes*. November 2017b.

Toronto Centre. *Risk-Based Supervision*. March 2018a.

Toronto Centre. *Implementing Risk Based Supervision: A Guide for Senior Managers*. July 2018b.

Toronto Centre. *The Post-Crisis Challenges Facing Supervisors*. July 2018c.

Toronto Centre. *Supervision of Cyber Risk*. September 2018d.

Toronto Centre. *Turning Risk Assessments into Supervisory Actions*. August 2019a.

Toronto Centre. *Supervising FinTech to Promote Financial Inclusion*. December 2019b.

Toronto Centre. *Risk-Based Supervision for Securities Supervisors (and Other Supervisors of Small Firms)*. February 2020.

Toronto Centre. *Operational Resilience: The Next Frontier for Supervisors?* April 2021a.

Toronto Centre. *Supervising Corporate Governance: Pushing the Boundaries*. January 2022.