SOUTH AFRICAN RESERVE BANK

National Payment System Department

Consultation paper on cyber-resilience

December 2022

Contents

1. Introduction and background

1.1 In terms of section 10(1)(c) of the South African Reserve Bank Act 90 of 1989, as amended (SARB Act), the South African Reserve Bank (SARB) is required to perform such functions, implement such rules and procedures, and, in general, take such steps as may be necessary to establish, conduct, monitor, regulate and supervise payment, clearing or settlement systems. The SARB plays an important role in ensuring the safety, efficiency and resiliency of the national payment system (NPS).

1.2 The NPS encompasses the entire payment process, from payer to beneficiary, and includes settlement between banks. The process includes all the tools, systems, mechanisms, institutions, agreements, procedures, rules and laws applied and utilised to effect payment. Therefore, the NPS comprises various participants that play different roles, from issuing payment instruments, through providing payment services to third persons, to processing payment instructions as well as payment clearing and settlements.

1.3 The payment landscape has evolved significantly over the past two decades, with digitisation, financial technology (fintech), automation and artificial intelligence (AI) changing the manner in which payments are made. The rapid growth in digitisation and automation has introduced alternative payment solutions that are faster, more cost-effective and more efficient. However, these technologies also increase information technology (IT) security and cyber-risk in the payments industry as payment institutions become more dependent on computer networks and third-party IT service providers. This requires an increased level of resilience against cyber-incidents, as cyber-attacks on IT infrastructures, particularly those that are critical, could lead to a disruption that might develop into systemic events in the NPS, thus impacting negatively on the soundness, integrity, safety and efficiency of the NPS.

1.4 The financial services sector (including the payments sector) may be a target for cyber-crime owing to the large volumes of valuable information held and the large amount of money that a single data breach may generate. As the

use of technology in financial services grows, cyber-risk increases, leading to the need for improved resilience to cyber-attacks within the financial services sector. Although the sector has sufficient controls in place to mitigate against cyber-risk, cyber-threats continue to evolve and have become more sophisticated and complex. Therefore, the financial services sector should also be dynamic and fully aware of new and evolving threats and vulnerabilities to ensure that the mitigating efforts and measures remain relevant, agile and effective.

1.5 The financial services sector in South Africa experiences financial losses every year as a result of cyber-crime. According to the South African Banking Risk Information Centre (SABRIC) Annual Crime Statistics Report of 2021[1], gross digital banking fraud losses increased from R310 484 349 in 2020 to R438 238 743 in 2021. The banking sector remains one of the primary targets of cyber-attacks in South Africa, and the increased usage of digital banking products for payment has significantly increased the likelihood of cyber-attacks.

1.6 According to a report published by Accenture[2], South Africa had the third-most cyber-crime victims worldwide in 2020 The report highlights the major incidents that occurred in 2019, including the distributed denial of service (DDoS) attack on several South African banks and financial institutions which resulted in a loss of access to services. Furthermore, the report indicates that malware attacks in South Africa increased by 22% in the first quarter of 2019 compared to the first quarter of 2018, which translates into just under 577 attempted attacks per hour. Card-not-present fraud on South African-issued credit cards accounted for 79.5% of all losses and 100% in mobile banking fraud. In 2021, multiple banks in South Africa were affected by a ransomware attack through a debt recovery solutions provider that the banks had partnered with. The ransomware attack exposed approximately

[1] SABRIC Annual Crime Statistics Report 2021, available at sabric-crime-stats-2021_fa.pdf

[2] Accenture, Insight into the cyber threat landscape in South Africa, 2020. An insight into the threat landscape of South Africa (accenture.com)

1.4 million personal records of South Africans.[3] Lastly, in 2022, South African credit reporting agency TransUnion experienced a cyber-attack that resulted in the personal records of 54 million South Africans exposed.[4]

1.7 Although the banking sector is one of the most attractive targets for cyber-attacks, non-bank payment service providers may also become a target and an entry point of cyber-attacks into the NPS. This emanates from the increased participation of non-banks in the payments landscape, underpinned by technology and digital innovations.

1.8 Given the challenges that cyber-crime introduces in the financial sector, it is imperative that cyber-resilience is ensured within the NPS through a framework that requires payment institutions to maintain robust cyber-resilience controls. The resilience of payment institutions will minimise disruptions within the NPS and will contribute to maintaining the confidence of consumers in payment services. Furthermore, it is vital that financial market infrastructures (FMIs), as essential platforms in the NPS, are also resilient to cyber-threats and cyber-attacks, as their operational failure would have an impact on financial stability and the soundness of the NPS.

2. Definitions

2.1 *Cloud computing:* A model for enabling convenient, on-demand network access to a shared pool of configured computer resources (e.g. a network, servers, storage facilities, applications and other services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[5]

2.2 *Cyber-event:* Any observable occurrence in an information system. Cyber-events sometimes provide an indication that a cyber incident is occurring.

[3] ITWeb, SA banks caught up in ransomware attack on debt collector,2021.
SA banks caught up in ransomware attack on debt collector | ITWeb
[4] Businesstech, TransUnion cyber-attack hackers demand R255 million ransoms, 2022.
TransUnion cyber-attack – hackers demand R225 million ransom (businesstech.co.za)
[5] BIS, Payments aspects of financial inclusion in the fintech era,2020.
Payment aspects of financial inclusion in the fintech era (bis.org)

2.3 *Cyber-incident:* A cyber-event that jeopardises the cybersecurity of an information system and/or the information that the system processes, stores or transmits, or which violates the security policies, security procedures and/or acceptable use policies, whether resulting from malicious activity or not

2.4 *Cyber-resilience:* The ability of an organisation to continue carrying out its mission by anticipating and adapting to cyber-threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber-incidents.[6]

2.5 *Cyber-risk:* The combination of the probability of cyber-incidents occurring and their impact.

2.6 *Cybersecurity:* The preservation of confidentiality, integrity and availability of information and/or information systems through the cyber-medium. In addition, other properties (such as authenticity, accountability, non-repudiation and reliability) can also be involved.7 .

2.7 *Cyber-threat:* A circumstance with the potential to exploit one or more vulnerabilities that adversely affects cybersecurity.[8]

2.8 *Data breach:* A compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to data transmitted, stored or otherwise processed.[9]

2.9 *Payment institution:* An entity that is designated, authorised, registered or regulated under the National Payment System Act 78 of 1998 (NPS Act).

[6] Financial Stability Board, Cyber Lexicon, 2018, available at Cyber Lexicon (fsb.org)
[7] Financial Stability Board, Cyber Lexicon, 2018, available at Cyber Lexicon (fsb.org)
[8] Financial Stability Board, Cyber Lexicon, 2018, available at Cyber Lexicon (fsb.org)
[9] Financial Stability Board, Cyber Lexicon, 2018, available at Cyber Lexicon (fsb.org)

3. Purpose and scope

3.1 The purpose of this paper is to contribute to a process of developing a cyber-resilience framework within the NPS.

3.2 The scope of the paper covers cyber-resilience in respect of payment institutions, payment clearing and settlement systems, as well as payment FMIs.

4. Policy objectives

4.1 This paper outlines the importance of cyber-resilience within the NPS in relation to the achievement of the SARB's mandate of ensuring the safety and efficiency of the system. This paper specifically seeks to advance the achievement of the following goals of the National Payment System Framework and Strategy (*Vision 2025* document):

4.1.1 *Financial stability and security:* A high level of cyber-resilience by payment institutions as well as payment clearing and settlement systems contributes to the stability and security of the NPS. The evolution of payment activities and infrastructures as well as the leveraging of technological advances has increased exposure to cybersecurity risk. Therefore, a cyber-resilience framework within the NPS would contribute to the resilience of payment institutions as well as payment clearing and settlement systems to cyber-threats. Cyber-resilience within the NPS would also assist in mitigating the likelihood of systemic events resulting from disruptions caused by cyber-attacks on payment institutions which, if not contained, might have a contagion effect on other payment institutions within their payment network or on interbank activities.

4.1.2 *A clear and transparent regulatory and governance framework:* All payment institutions providing the same payment services/activities should be subjected to the same regulation and governance framework that is appropriate for the potential risk that may be introduced. A transparent cyber-resilience regulatory and governance framework that applies to all

payment institutions as well as payment clearing and settlement systems is essential in maintaining and enhancing the stability and safety of the NPS.

4.1.3 *Transparency and public accountability:* All payment institutions should be subjected to public accountability and should share relevant management information to foster collaboration in managing cyber-threats and cyber-incidents. Access to relevant management information would help to address possible threats and vulnerabilities within the NPS. It is important that the payment industry collaborates and shares relevant information to assist in trend analysis and to enable the payment industry to strengthen cyber-resilience measures.

5. An overview of the cyber-threat landscape in the national payment system

5.1 The most prominent entry point of cyber-attacks into the NPS is through the end-point user or consumer. Thus, the retail payment environment is one of the main areas where cybersecurity breaches occur. Cyber-criminals target consumers through different payment mechanisms that are available to them by using the types of cyber-attacks indicated in Figure 1 below and further discussed in paragraphs 5.1.1 to 5.1.6. Cyber-attacks on consumers can be viewed as a major source of disruption to the NPS and may lead to loss of confidence in the NPS.

Figure 1: Cyber-attacks and related fraud

5.1.1 *Social engineering and phishing:* Social-engineering attacks involve criminals impersonating trusted officials/sources to lure unsuspecting victims into divulging personal information. Real-time scams and credential/personal information harvesting are the most common types of social-engineering attacks. The consequences of these attacks may be the takeover of an account and the creation of fraudulent accounts which in turn may lead to financial losses to the victims.

5.1.2 *Authorised Push Payment (APP) fraud:* APP fraud occurs when a cyber-criminal tricks the payer into making an authorised payment into a fraudulent account. There are two types of attacks relating to APP fraud: malicious direction and a malicious payee. In the case of malicious direction, a victim makes a payment under the impression that the payee account details are legitimate, whereas in the case of a malicious payee attack, victims make push payments to scammers posing as legitimate service providers.

5.1.3 *Mobile-related attacks:* These are cyber-attacks on payments made using mobile devices. Data breaches initiated through phishing, malware and mobile operating system access permissions are prevalent in mobile-related attacks due to ineffective mobile payment security and may result in data and financial losses.

5.1.4 *Automated teller machine (ATM) cash-out attacks:* ATM cash-out attacks involve cyber-criminals breaching banks' or card payment processors' fraud detection controls in order to withdraw cash from ATMs. The cyber-criminals gain remote access to a card management system to alter fraud prevention controls such as withdrawal limits or the personal identification numbers (PINs) of compromised cardholder accounts. This is commonly undertaken by inserting malware via phishing or social-engineering methods into a financial institution's or system operator's infrastructure.

5.1.5 *Card-not-present fraud:* In card-not-present fraud, cyber-criminals obtain the victim's card information through various ways, such as phishing, hacking or card skimming. Once the information has been obtained, various transactions

can be performed, such as online purchases with the stolen card information, recurring payments of small amounts and/or gift cards, and online vouchers that enable cyber-criminals to purchase goods in the physical world as opposed to purchasing them online to avoid the traceability of such transactions.

5.1.6 *Multi-vector attacks:* These are attacks on payment institutions through multiple entry points within their networks by taking advantage of the weaknesses in the institutions' end-point security. This type of attack can cause extensive disruption within the NPS if there are participants with inadequate/weak cybersecurity controls where entry may be gained through such participants to disrupt the broader NPS.

5.2 The SABRIC Annual Crime Statistics Report of 2021 highlights that social engineering continues to be the main method of cyber-attacks used to target users of digital payment channels. Digital banking fraud decreased by 18% in 2021 compared to the increase of 33% in 2020, but there was a 45% increase in gross losses in 2021 Card-not-present fraud losses for South African-issued credit cards accounted for 77% of gross credit card fraud losses, while the share of card-not-present fraud with debit cards amounted to 55.3% of gross debit card fraud losses. Mobile banking fraud made up 38% of digital banking crime incidents. According to the 2021 International Criminal Police Organization (INTERPOL) African cyber-threat assessment report, South Africa had 230 million threat detections in total and had the highest targeted ransomware attempts from January 2020 to February 2021[10]

5.3 The most common types of reported cyber-incidents in the South African banking sector are ransomware, malware, DDoS attacks and phishing. Third-party service providers are also a critical cyber-attack entry point in the banking sector. In 2020 and 2021, some of the reported cyber-incidents were through compromises on third-party service providers. These incidents on

[10]INTERPOL, African Cyberthreat Assessment Report,2021.
INTERPOL report identifies top cyberthreats in Africa

third-party providers led to clients' personal information being compromised, which included their identification information and banking account information. The reported phishing incidents were mostly related to attacks on bank users, giving the attackers access to users' electronic mailboxes which enabled them to send out more phishing emails to internal and external parties.

5.4 The evolution of digital payments has prompted payment institutions worldwide to prioritise the safety of consumers. This has involved payment institutions and card networks continuously investing resources to protect the payments ecosystem. The innovations by the payments industry include tokenisation, biometric identification, quick response codes as well as Europay, Mastercard and Visa (EMV) technology. However, despite all these efforts being in place, cyber-threats in digital payments are still prevalent and require further efforts by entities in the NPS to counter cyber-risks.

5.5 Fraud in the wholesale payment system has also become prevalent through compromises to the end-point security of operators and participants. Cyber-resilience interventions by participants in the wholesale payment ecosystem can contribute significantly to improved confidence in the NPS and in the maintenance of financial stability.[11] According to a report published by the United States (US) Federal Reserve Bank of New York[12] on *Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis*, wholesale payment networks are attractive to cyber-attackers as the data on wholesale payments provides valuable information on flows between financial institutions. An attack on a single payment institution within the network could have great spill-over effects and cause disruption in the wholesale payment network.

5.6 In 2016, the Bangladesh central bank's Society for Worldwide Interbank Financial Telecommunications (SWIFT) credentials were used to transfer

[11] BIS, Reducing the risk of wholesale payments fraud related to endpoint security, 2018. Reducing the risk of wholesale payments fraud related to endpoint security (bis.org)

[12] Federal Reserve Bank of New York, Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis ,staff report 909, 2021.Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis - FEDERAL RESERVE BANK of NEW YORK (newyorkfed.org)

US$ 81 million from its account, which led to the introduction of the SWIFT Customer Security Controls Framework. The framework consists of mandatory security controls for users to implement on their local SWIFT infrastructure. Through these controls, cybersecurity risk is mitigated at user level and there is less likelihood of a disruption in the payment network.

5.7 Many financial institutions, including payment institutions, have opted to contract third-party service providers as an alternative risk transfer mechanism in respect of cyber-risk. In this regard, payment institutions may benefit from lower costs and an additional layer of cybersecurity by transferring risk to third-party IT service providers. These arrangements, which include the use of cloud technology, have become one of the measures used to improve cyber-resilience. As financial institutions' exposure to cloud services increases and as cloud service providers (CSPs) become systemically important, cloud dependency is becoming more prone to increasing concentration risk and tail risks[13]. It is further observed that cyber-attacks on CSPs and other third-party IT service providers have become an entry point on institutions.[14] In addition, as most financial institutions are likely to move parts of their IT operations to the cloud environment, this could potentially create a highly concentrated cloud service environment with the potential to pose a risk for single points of failure.

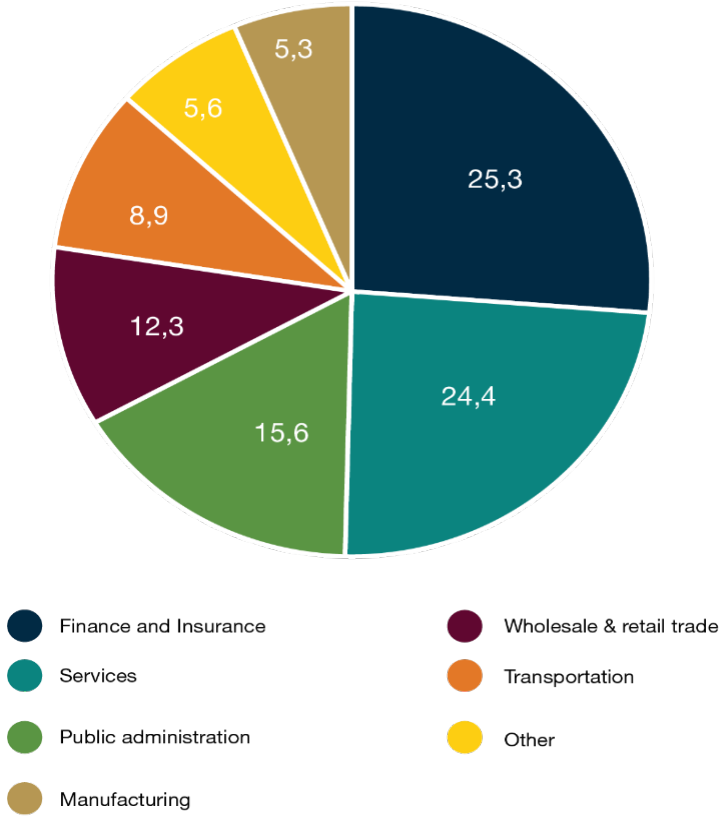
5.8 Since the COVID-19 pandemic, there has been a shift in the cyber-threat landscape as ransomware became the most common cybersecurity threat faced by many institutions irrespective of the sector.[15] Payment institutions' reliance on remote working during the pandemic introduced new threats related to the intense use of technology infrastructure. In this regard, the move to the utilisation of digital platforms exposed users to high risk of cyber-attacks. According to the Bank for International Settlements (BIS)[16], the financial

[13] Tail risk is the risk of events that have a low probability of occurring but are disruptive when they occur.
[14] BIS, the drivers of cyber risk, BIS Working Papers No 865, 2020.
The drivers of cyber risk (bis.org)
[15] Allianz Global Corporate and Specialty, Allianz Risk Barometer 2022,
Allianz_Risk_Barometer_2022_FINAL.pdf
[16] BIS, Covid-19 and cyber risk in the financial sector, BIS Bulletin No 37,2021.
Covid-19 and cyber risk in the financial sector (bis.org)

sector has experienced more frequent cyber-attacks than other sectors since the COVID-19 pandemic started, particularly targeting payment institutions, insurers and credit unions.

5.9 The remote working arrangements adopted in this period were not anticipated to last as long as they have, and most institutions had business continuity plans designed for short-term periods. However, due to the lasting effects of the circumstances brought about by COVID-19, business processes needed to be adapted to the 'new normal'. Remote desktop protocols and virtual private networks (VPNs) are some of the access technologies that business had to adopt, which created new cyber-threats, particularly through phishing attacks on users with the intention of gaining access to networks.

Figure 2: Covid-19-related cyber-events by sector



Source: *BIS Bulletin no. 137*

6. Cyber-risks in the national payment system

6.1 The cyber-environment exposes payment institutions as well as payment clearing and settlement systems to potential operational, legal and reputational risks, including business interruptions, data loss, fraud, breach of privacy and network failures, which may result in financial losses. The level of cyber-resilience contributes positively to the operational resilience of payment institutions as well as payment clearing and settlement systems and is a key factor in the overall resilience of the broader NPS. In this regard, the resilience of payment institutions as well as payment clearing and settlement systems to cyber-attacks would contribute effectively to the safety and efficiency of the NPS.

6.2 Table 1 depicts the risks that the various sectors of the NPS are exposed to due to cyber-threats.

Table 1: Risk exposures relating to cyber-threats in the NPS

Stakeholder/system	Risks
NPS	*Cyber-risk threatens the stability and security of the NPS.* • The systemic effect and extent of disruption that cyber-threats present to the NPS threatens the stability and security of the NPS. • The presence of cyber-events in the retail payment environment leads to loss of confidence in the safety of the NPS.
FMIs	Cyber-attacks on FMIs could lead to the following: • *systemic financial shock:* This can result in a systemic effect on the participants involved and a knock-on effect to the financial system. • impact on both cross-border and domestic transactions between the FMI participants. • *the FMI failing to settle obligations:* The failure of an FMI to settle obligations by the end-of-value date may have an impact on financial stability, as the liquidity condition for participants in the settlement system depends on the certainty of the assumption that transactions are considered final.

	• impact on the operational risk of an FMI, as the inability of an FMI to resume operations within two hours of a disruption caused by a cyber-attack may indicate lack of robust business continuity planning. This can further lead to lack of confidence that settlement participants have in an FMI. • loss of confidence in the FMI and the operator of the FMI, such as the SARB as the owner and operator of the South African Multiple Options Settlement (SAMOS) system.
Payment institutions	*Financial loss* • Financial losses from cyber-incidents for both the payment institutions and the customer. This may then lead to loss of consumer confidence in the payment service providers (PSPs). *Operational risk* • Lack of recovery from a cyber-attack may lead to disruptions in the operations of a payment institution, which may lead to loss of services and financial losses. *Reputational risk* • A number of cyber-incidents reported will negatively impact on the safety of payment institutions' payment activities and reputation. *Disruption of services* • Successful cyber-attacks and lack of prompt recovery may lead to disrupted services and in turn financial losses.
Merchants	*Loss of revenue and increased service chargeback rates* • Stolen client financial information and credentials as a result of cyber-fraud for the purposes of conducting fraudulent card-not-present transactions has an adverse impact on the merchant, as the merchant may have to reimburse cardholders on a chargeback request and thus result in loss of revenue. *Loss of consumer confidence* • Lack of cybersecurity on merchants' e-commerce sites may result in high rates of data breaches and stolen consumer information and credentials. This will result in loss of confidence in merchants' e-commerce sites and thus loss of potential revenue.

End user	*Digital identity theft and data breaches that lead to financial losses* • Theft of digital identity and financial data emanating from data breaches leads to account takeover or fraudulent accounts in the victim's name. This in turn may result in financial losses for the end user. • *Reduced adoption of digital payments* The prominent presence of cyber-attacks may impact on the adoption of digital payments as end user lose confidence in the safety of digital payment platforms. This may lead to end users reverting back to cash and may have an adverse impact on digital financial services that promote financial inclusion.

7. Benefits of cyber-resilience in the national payment system

7.1 Cyber-resilience plays a crucial role in the stability and efficiency of the NPS. Table 2 depicts the different benefits that cyber-resilience presents to NPS participants.

Table 2: Benefits of cyber-resilience for NPS participants

Stakeholder	Benefits
NPS	*A safe and efficient NPS* • The resilience of the NPS to cyber-threats contributes to the continuous safety and efficiency of the NPS. *Financial stability and security* • Cyber-resilience in the NPS will assist in mitigating financial shocks caused by cyber-attacks that may impact on financial stability. *Maintaining confidence in the integrity of the NPS* • A robust cyber-resilience framework should improve the overall resilience of the NPS as it may limit the possibility of systemic cyber-events that may lead to loss of confidence in the system.
FMIs	*Contributing to the efficient functioning of the NPS* • FMIs that are resilient to cyber-attacks are in a position to discharge their functions with minimal disruption.

	Financial stability • An FMI's ability to resume critical operations rapidly and safely in the event of a disruption, including a cyber-attack, contributes positively to financial stability as obligations will be settled timeously. *Reduction in systemic effect in the event of a cyber-attack* • Robust cyber-resilience frameworks ensure that FMIs have response and recovery plans in place coordinated with participants within their ecosystem to ensure that there are minimal contagion effects in the event of large-scale cyber-attacks.
Payment institutions	*Maintained consumer confidence* • Resilient payment institutions' systems enable business continuity post cyber-attacks, leading to maintained consumer confidence in the payment institution. *Promotion of innovation in a safe NPS* • An NPS that is resilient to cyber-attacks and cyber-threats as a result of the resilience of payment institutions promotes an enabling environment required for payment innovations to grow in a safe and secure payments environment. *Reduced systemic effects of cyber-attacks on other participants in the NPS* • As some payment institutions are participants in the NPS, the inability to recover from a cyber-attack may have a spill-over effect in the broader NPS.
Merchants	*Ability to offer e-commerce products and services using secure digital payment platforms* • Cyber-resilience improves the security and safety of e-commerce payment platforms and gateways, resulting in a reduced financial loss for merchants.
End user	*Confidence in the NPS* • A cyber-resilient NPS reduces the possibility of systemic effects that may affect end users. End users will retain confidence in the system knowing that their data and funds will not be compromised

	when facilitating payments using secure digital payment channels within the NPS. *Data protection* • Cyber-resilience includes adequate data security controls wherein end-user data is protected in the event of data breaches, thus reducing the risk of identity theft and financial losses.

8. Domestic interventions to promote cyber-resilience

8.1 Concerns relating to cyber-risks have led to the acknowledgement that both government and regulatory authorities have an important role to play in an effort to direct the actions of regulated entities. In this regard, cyber-resilience ranks as a priority area of focus to government departments such as the Department of Communication and Digital Technologies (DCDT) and the Department of Justice (DOJ) as well as regulatory authorities in ensuring that their respective sectors are resilient to the potential cyber-incidents that they may experience and have developed and implemented measures to combat cyber-threats and promote cyber-resilience. In respect to the financial sector specifically, cybersecurity and cyber-resilience are particularly important in the maintenance of financial stability.

8.2 Table 3 indicates the key interventions taken by government, regulatory authorities and financial sector participants.

Table 3: Key interventions that have been taken by various authorities

Authority	Interventions	Affected stakeholders
DCDT	*The establishment of the National Cybersecurity Hub (Hub)* • The Hub serves as the National Computer Security Incident Response Team of South Africa. • The Hub collaborates with various stakeholders such as government, the private sector, civil society and the public. • The Hub coordinates cybersecurity response activities and facilitates information and technology sharing.	South African government, the private sector, civil society and the general public

DOJ	*Cybercrimes Act 19 of 2020 (Cybercrimes Act)* • The Cybercrimes Act sets out cybercrime offences and penalties. The Act provides a cybersecurity legislative framework. • The Cybercrimes Act imposes an obligation on electronic communications service providers (ECSPs) and financial institutions, such as banks, to report cyber-offences within 72 hours of becoming aware of them.	All ECSPs, financial institutions, government departments, all users of computers and the Internet
Prudential Authority (PA)	*Directive 2 of 2019* • The PA has issued a directive in respect of banks which sets out cyber-resilience requirements, including reporting requirements in respect of IT and cyber-incidents. *Draft joint standard on IT risk management* • The PA and the Financial Sector Conduct Authority (FSCA) have published a draft standard that outlines IT risk management that financial institutions must comply with. *Draft joint standard on cybersecurity and cyber-resilience requirements* • The PA and the FSCA have published a draft standard that outlines the requirements for cyber-resilience.	Banks Banks, insurers, market infrastructures, financial services providers and collective investment schemes Banks, insurers and market infrastructures
SARB	*Position paper adopting the Principles for Financial Market Infrastructures (PFMIs)* • The SARB has issued a position paper in respect of the adoption and implementation of the PFMIs for payment system FMIs. • The PFMIs recognise operational risk, which includes cyber-risk, as a specific key risk faced by FMIs, and stipulates that an FMI should have governance arrangements and objectives in place to manage these risks within a comprehensive risk management framework. *Establishment of the Cyber-Resilience Subcommittee (CRS)*	FMIs Participants include the financial sector supervisors

	• The main objective of the CRS is to guide, evaluate and monitor cybersecurity efforts within the financial sector. *The SARB's Cyber and Information Security Unit (CISU)* • The CISU is responsible for the protection of the SARB through the detection and efficient response to cyber-attacks and cyber-incidents.	and regulators, national financial structures, associations, commercial banks and insurers. SARB departments
Information Regulator of South Africa	• The Information Regulator was established in terms of section 39 of the Protection of Personal Information Act 4 of 2013 (POPI Act) and became effective in 2021. • The Information Regulator is responsible for monitoring and enforcing public and private bodies' compliance with the POPI Act as well as its promotion thereof. • The POPI Act will have a positive impact on the promotion of cybersecurity in respect of holding public and private entities accountable for the personal information and data stored on their information systems as well as holding them accountable in the event of data breaches. • The POPI Act has compelled entities to assess their current IT security measures and enhance them to ensure that personal data is not compromised.	Public and private entities
SABRIC	• SABRIC was created by South African banks with the objective of combating banking and financial crime as well as promoting security and safety within the banking sector. • SABRIC facilitates the exchange of information between members and launches various campaigns on its website to educate the public about cybercrime and other risks inherent in the banking environment.	Banking industry

9. Jurisdictional analysis

9.1 Building resilience to cyber-risks in the financial sector is a priority in many jurisdictions around the globe. Regulatory authorities are actively involved in developing interventions to promote cyber-resilience within the financial sectors of their respective jurisdictions. Interventions across many jurisdictions are channelled towards developing regulatory and supervisory

frameworks, including risk management guidance, legally binding standards as well as information gathering and sharing initiatives that will require regulated entities to be more proactive in pursuing cyber-resilience.

9.2 Table 4 provides examples of initiatives that various jurisdictions have undertaken to promote cyber-resilience.

Table 4: Initiatives by various jurisdictions

Jurisdiction	Initiatives
Reserve Bank of New Zealand (RBNZ)	• In April 2021, the RBNZ released a guidance on what regulated entities should consider when managing cyber-resilience. The guidance applies to all entities regulated by the RBNZ. • The objective of the guidance is to raise awareness amongst board members and senior management to promote accountability for managing cyber-risk within institutions, and it focuses on the following four elements: a) governance; b) capability building; c) information gathering; and d) third-party management.
European Central Bank (ECB)	• The ECB has set best practice and rules in order to ensure that FMIs have a high level of cyber-resilience. • The ECB has developed a European framework for ethical hacking, wherein an organisation can request an ethical hacker to attempt to hack its system in line with the guidance stipulated in the framework. • The goals of this framework are to assist entities in gaining insight about their protection, detection and response capabilities.
Bank of Canada (BoC)	• The BoC published a Cybersecurity Strategy for 2019-2021, which aims to reduce risk and promote resilience. • In 2018, the BoC entered into a formal partnership with Payments Canada, which is the entity responsible for Canada's payment clearing and settlement infrastructure, and the six largest Canadian banks. The intention of the partnership is to improve domestic coordination and make wholesale payment systems resilient to cyber-attacks. This includes improved cyber-detection as well as joint resiliency and recovery alternatives.

	• In October 2021, the BoC issued Expectations for Cyber-Resilience of FMIs, which outlines to FMIs the BoC's expectations for cyber-resilience.
Bank of England (BoE)	• The BoE has developed the CBEST framework for testing firms' cyber-resilience. The CBEST provides direction on how to conduct a safe but realistic simulated attack on the people, processes and technology that comprise a firm's cybersecurity controls. • The BoE conducts cyber-resilience assessments that assess firms' cyber-resilience capabilities. • The BoE has established a strategic cyber-forum which brings together cyber-resilience experts to share best practice and develop guidance for organisations.
Monetary Authority of Singapore (MAS)	• In December 2019, MAS published a notice under the Payment Services Act to licensees and operators of designated payment systems. The purpose of the notice was to set out cyber-hygiene requirements. These include cybersecurity requirements on applying security patching, deploying network security devices, implementing anti-malware measures and establishing security standards. • In March 2021, MAS issued a joint paper with the Association of Banks of Singapore on risk management and operational resilience in a remote working environment. This is amid the increase in remote working by financial institutions. The good practices to mitigate risk such as cybersecurity risk were also shared.
Banco Central do Brasil (Central Bank of Brazil)	• In February 2021, the Banco Central do Brasil issued Resolution CMN 4 893, which provides for the cyber-security policy and requirements for contracting services of data processing, data storage and cloud computing by financial institutions and other institutions licensed by the Central Bank of Brazil. • The resolution includes, among other requirements, that institutions must implement and maintain a cybersecurity policy formulated according to guidelines and principles that seek to ensure confidentiality, integrity and availability of data and information systems used. Institutions are also required to disclose their cybersecurity policies to employees and third-party service providers, and to disclose a summary of the cybersecurity policy to the public.
Reserve Bank of Australia (RBA)	• The RBA is a member of the Council of Financial Regulators (CFR), which was established with the objective of promoting the stability of

and Australian Prudential Regulation Authority (APRA)	the Australian financial system. The CFR has classified cyber-risk as a top risk and has developed a framework for improving cyber-resilience within the Australian financial services industry. • The CFR has developed the Cyber Operational Resilience Intelligent Led Exercises Scheme (CORIE). CORIE is a pilot programme of exercises aiming to assess financial institutions' cyber-resilience. • The RBA published a media release in February 2021 in respect of its Payment System Board update meeting. Discussions focused on how the RBA can best support cyber-resilience in the payments system in the context of the Australian Government Cybersecurity Strategy. • The RBA has adopted the CPMI/IOSCO guidance on the cyber-resilience for FMIs and assesses FMIs against the guidance. • APRA has issued Prudential Standard CPS 234 on Information Security as well as Prudential Practice Guide CPG 234. The prudential standard is intended at ensuring that APRA-regulated entities take measures to be resilient against information security incidents, which include cyber-attacks.
Reserve Bank of India (RBI)	• In December 2019, the RBI issued two circulars titled 'Comprehensive Cybersecurity Framework for Primary (Urban) Cooperative Banks – a Graded Approach' and 'Cybersecurity Controls for Third-Party ATM Switch Application Service Providers' to all regulated entities, including primary urban cooperative banks (UCBs). The objective was to ensure that UCBs with high IT penetration and offering all payment services were in line with other banks with mature cybersecurity infrastructure and practices.
Hong Kong Monetary Authority (HKMA)	• The HKMA introduced the Cybersecurity Fortification Initiative (CFI) in 2016. The CFI was aimed at raising the cyber-resilience of Hong Kong's banking system. The CFI is underpinned by three pillars: a) Cyber-Resilience Assessment Framework (C-RAF) b) Professional Development Programme c) Cyber Intelligence Sharing Platform

10. Policy recommendations

10.1 *The SARB should use regulatory tools to drive cyber-resilience in the NPS.* Such tools should, at a minimum, drive actions that will address the following:

10.1.1 *Cyber-resilience frameworks:* Payment institutions should be required to develop and maintain cyber-resilience frameworks. The Committee on Payments and Market Infrastructure (CPMI) and the International Organization of Securities Commissions (IOSCO) issued a guidance on cyber-resilience for FMIs in 2016.[17] The SARB is of the view that the guidance is also relevant for payment institutions. The guidance emphasises the importance of FMIs embarking on the establishment of cyber-resilience frameworks that should cover the following five primary risk management categories:

a) governance;
b) identification;
c) protection;
d) detection; and
e) response and recovery.

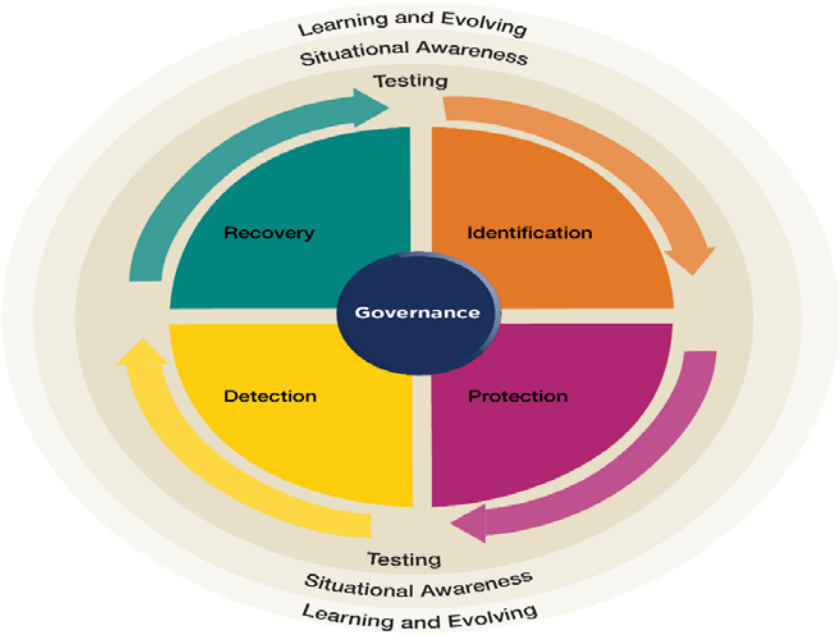
The CPMI/IOSCO guidance further highlights the following three overarching general components that should be addressed in FMIs' cyber-resilience frameworks:

f) testing;
g) situational awareness; and
h) learning and evolving.

Figure 3 depicts the relationship amongst the risk management categories and overarching components.

[17] Committee on Payments and Market Infrastructures Board of the International Organization of Securities Commissions, Guidance on cyber resilience for financial market infrastructures, June 2016
Guidance on cyber resilience for financial market infrastructures (bis.org)

Figure 3: Cyber-risillience guidance on overarching components and risk management categories



Source: CPMI/IOSCO Guidance, 2016

10.1.1.1 *Cyber-governance:* Payment institutions should have effective cyber-governance arrangements in place as part of their comprehensive cyber-resilience frameworks. The frameworks should define how cyber-resilience objectives are determined and should outline the people, processes and technology requirements for managing cyber-risks and for timely communication, all in order to enable payment institutions to effectively respond to and recover from cyber-attacks. The board of directors (board) and/or senior management of the payment institution should play an important role in respect of cyber-governance and should specifically have the following responsibilities:

a) Determine the entity's cyber-risk tolerance levels and oversee the development and implementation of a cyber-resilience framework.

b) Approve the cyber-resilience framework and policies.

c) Ensure the appointment of a senior executive and technical experts with the relevant skills, expertise and experience accountable for cyber-resilience.

d) The senior management of the payment institution should regularly keep the board informed and updated on the cyber-resilience status of the entity and on any developments relating to cyber-threats within the payment system environment, as it may affect them.

10.1.1.2 *Identification of critical operations and information assets:* Payment institutions should, in order of priority, identify which of their critical technology, operations and supporting information assets should be protected against cyber-compromise. Furthermore, payment institutions should identify internal processes, procedures, information assets and external dependencies that will strengthen their overall resiliency to cyber-threats. This process should make provision for the following:

a) the identification and ranking of technology, processes and functions in a risk-based approach to ensure that protective, detective, response and recovery efforts are facilitated in a priority order;

b) the identification of technology, information assets, system configurations and access rights to information assets, and keeping records that will assist in the detection of anomalies;

c) the regular review and updating of critical business processes that will ensure that information remains current and accurate; and

d) the identification of cyber-risk interconnections within the payment ecosystem.

10.1.1.3 *Cyber-protection measures:* Cyber-resilience frameworks should include security controls, processes and systems that effectively protect and safeguard the confidentiality, integrity and availability of services provided

and information handled by a payment institution. These measures should, however, be proportionate to the threat landscape, risk tolerance and systemic role of the payment institution in the NPS. The protection measures should make provision for the following:

a) the embedding of protective controls that minimise the likelihood and impact of a successful cyber-attack on identified critical business functions and information assets;

b) the development and implementation of protective measures to mitigate risks arising from the interconnected entities within the payment ecosystem;

c) the development and implementation of measures that mitigate cyber-risk and address anomalous behaviour by staff with access to the system; and

d) the continuous investment in the training of all relevant staff to develop and maintain awareness and ensuring that staff are knowledgeable in detecting and addressing cyber-risk.

10.1.1.4 *Detection:* Cyber-resilience frameworks should include cyber-attack trigger points and detection measures. This will ensure that payment institutions have the capabilities to continuously monitor and detect anomalous events and activities. The relevant cyber-attack detection measures should make provision for the following:

a) *continual and comprehensive arrangements for monitoring:* the development and implementation of measures that enable continuous monitoring and detection of anomalous activities and events;

b) *the development and implementation of layered detection controls:* the development of multi-layered trigger indicators and detection controls

that accommodate processes, people and technology, ensuring that each layer serves as a safety net;

c) *incident response:* the facilitation of incident response processes to ensure that there is efficient recovery from incidents that could not be prevented; and

d) *analysis of security measures:* the development and implementation of security measures that help to identify and facilitate the analysis of irregular behaviour by persons with access to the entity's information assets and network.

10.1.1.5 *Response and recovery:* Payment institutions should have arrangements in place designed to enable them to resume critical operations rapidly and safely to mitigate potential systemic risk. In this regard, cyber-resilience frameworks should include the following*:*

a) *incident response and planning:* Payment institutions should have incident response plans and measures in place to enable the early detection of cyber-attack attempts as well as successful cyber-attacks. The measures should further enable institutions to immediately initiate recovery efforts to restore operations*.*

b) *the resumption of critical operations within two hours:* Payment institutions should design and test their systems to enable them to resume critical operations within two hours in the event of a cyber-incident and under extreme cyber-attack scenarios or as per the payments industry-specified timeline provided, which shall not exceed two hours of recovery/resumption time*.*

c) *contingency planning:* Payment institutions should plan for extreme scenarios wherein the resumption of critical operations may not be possible within two hours. This should include an analysis of critical functions and interdependencies to prioritise resumption and

recovery actions in a contingency mode while remedial efforts are in progress.

d) *planning and preparation:* Payment institutions should develop and regularly test response, resumption and recovery plans. Plans should be updated on a continuous basis based on information sharing, current cyber-threat intelligence and lessons learned from previous cyber-events.

e) *third-party management:* Payment institutions should include relevant third-party management plans in their cyber-resilience frameworks. Third-party management plans should make provision for the following:

   i. extensive due diligence to evaluate the cyber-resilience measures that relevant third parties *have in place;*

   ii. an assessment of the criticality of processes that may be outsourced prior to entering into envisaged outsourcing contracts;

   iii. obtaining independent security attestation reports from third parties as an additional layer of assurance of the security posture of the third-party service providers;

   iv. ensuring that the business continuity plans of critical third-party service providers align with the objectives and policies of the payment institution; and

   v. in the event of outsourcing to a CSP, ensuring that the following principles are adhered to:

- The payment institution should conduct due diligence on the CSP and should be comfortable with the CSP's cyber-resilience measures.

- The payment institution should be comfortable with the jurisdiction risk in relation to the data transmitted, stored and processed in the cloud.

- The payment institution should share responsibility and remain accountable for the data stored and processed as well as for the overall security of the solutions developed on the cloud.

10.1.1.6 Testing : Payment institutions should develop and implement cyber resilience testing programmes and methodologies which make provision for the following :

a) *comprehensive scenario based testing*: Payment institutions should ensure that tests address different scenarios and simulations of various cyber attacks that challenge the resumption and recovery plans and practices.

b) *penetration testing*: Payment institutions should conduct penetration testing on their systems and processes through simulation of cyber attacks on their systems in order to identify the vulnerabilities in their systems. Payment institutions should include relevant stakeholders in their tests , such as critical service providers and other stakeholders.

c) *cyber resilience testing after significant system changes :* Payment institutions should test their systems after implementation of significant changes to their systems to identify any security vulnerabilities due to system change.

10.1.1.7 *Information sharing*

a) Cyber-resilience frameworks should include arrangements that address how payment institutions may access and share information with external stakeholders within the payment industry and financial sector. The collection and exchange of information should assist payment institutions in facilitating learnings relating to the detection, response and recovery of their systems from cyber-incidents experienced in the broader ecosystem.

b) Payment institutions should plan arrangements for information sharing and should ensure that it is effected through trusted channels. Actively participating in information-sharing groups and organisations such as the Cyber Hub and Cybersecurity Incident Response Teams will assist institutions in gathering, distributing and assessing information about cyber-practices, cyber-threats and early warning indicators relating to cyber-threats.

10.2 Cyber-incident reporting requirements

10.2.1 The SARB, as regulator of the NPS, should establish requirements for cyber-incident reporting for all payment institutions. This will address the importance of cyber-event reporting within the NPS that will accommodate all payment institutions in order to enable the relevant regulators to observe emerging trends and entry points of cyber-events within the NPS to induce relevant change. The cyber-incident reporting requirements may include the following:

a) Payment institutions may be required to report material cyber-incidents to the SARB within 24 hours, including in particular:

- the date and time of the incident;
- the cause and source of the incident;
- the type and nature of the incident;

- the impact on the provision of services;
- the expected recovery period;
- the impact on stakeholders;
- the improvement action plan; and
- the possible systemic effect of the incident on other participants.

10.3. The SARB should develop and implement a cyber-resilience threat intelligence assessment for the NPS.

10.3.1. This is a measure that has been adopted by a number of jurisdictions, including Australia and the United Kingdom (UK), in a collaborative manner by regulators within those jurisdictions. It is essential that the SARB has its own toolkit to continuously monitor the cyber-resilience of payment institutions and to identify any trends and threats that may adversely impact on the soundness and efficiency of the NPS. Furthermore, the NPS landscape has grown substantially, and such a toolkit should apply to all participants in the system.

10.4. The SARB should develop and apply cyber-resilience assessment standards for FMIs.

10.4.1. The CPMI/IOSCO highlights the role of overseers in ensuring that FMIs have extensive cyber-resilience frameworks. FMIs are currently assessed against the Principles for Financial Market Infrastructures (PFMIs). However, it is imperative that cybersecurity risk is recognised as a risk theme that needs to be assessed on its own due to its disruptive nature. It is therefore vital that the SARB develops standards which are aligned to international standards and which should be utilised in the assessment of FMIs' cyber-resilience.

10.4.2. The assessment standards should provide for the following:

a) *expectations of the level of cyber-resilience:* The assessment standards will set out levels of expectation which provides a benchmark

against which the FMIs' level of cyber resilience may be evaluated. This will measure progression and establish priority areas for improvement.

b) *an assessment of cyber-resilience frameworks against the minimum requirements stated in 10.1 above.*

c) *the minimum requirements and risk categories* mentioned in 10.1 above that set out a benchmark against which FMIs' framework will be assessed.

10.5. *Consumer education on cyber-risk*

10.5.1. Financial sector regulators such as the SARB, the Prudential Authority (PA) and the Financial Sector Conduct Authority (FSCA) should collaborate to promote consumer awareness and education in relation to cyber-risk and its impact on consumers. Consumer education empowers consumers to be alert for different types of cyber-threats and related fraud indicated in paragraph 5.1. Furthermore, the SARB and FSCA should develop requirements for payment institutions, including banks, to develop and implement consumer awareness programmes on cyber-threats and related fraud, particularly in relation to the products and services that they provide to consumers.

11. Conclusions

11.1. Currently, the SARB does not have a cyber-resilience framework for the NPS. Cyber-risk presents a significant opportunity for systemic disruption to the NPS. A framework to mitigate this potential risk should therefore be developed, specifically for the NPS, to ensure that all payment institutions implement resiliency measures to contribute to the overall cyber-resilience of the broader NPS.

11.2. It is evident that the evolution of digital payments has made the payment experience for end users more convenient but not without increased risk. Sophisticated digital payment methods are exposed to sophisticated cyber-

threats. The safety and efficiency of the NPS may be compromised through attacks on new entrants in the payment system that introduce new digital payment methods. It is thus important that the regulation of the NPS strikes a balance and does not hinder the entrance of new payment institutions but equally promotes innovation in a secure payment environment. A secure payment environment will be achieved through robust cybersecurity measures that need to be applied by all payment institutions. The SARB should, in its supervisory role in the NPS, implement interventions that address the cyber-resilience of all participants in the NPS.

11.3. Cyber-threats and cyber-attacks have a significant potential to disrupt the efficiency and effectiveness of the NPS. In this regard, it is essential that cyber-risk is not addressed as a subset of operational risk but rather that it be addressed as a risk theme on its own. This requires payment institutions to develop frameworks or, if these are already in existence, to improve such cyber-resilience frameworks that are in place. However, for these interventions to be effective, cyber-resilience guidelines should be developed by the SARB and should be used to monitor and oversee the levels of cyber-resilience within the NPS.

11.4. To enable the SARB to effectively ensure the safety, efficiency and resiliency of the NPS, a robust cyber-resilience regulatory framework needs to be developed in order to ensure that the facilitation of innovation in the payment environment and the support for financial inclusion is promoted without compromising the security and efficiency of the NPS.

12. Comments and contact details

12.1. Stakeholders and other interested parties are invited to submit their comments on this consultation paper by 31 January 2023.

12.2. Comments should be addressed to npsdirectives@resbank.co.za

Abbreviations

AI	Artificial Intelligence
APP	Authorised Push Payment
APRA	Australian Prudential Regulation Authority
ATM	Automated Teller Machine
BIS	Bank of International Settlements
board	board of directors
BoC	Bank of Canada
BoE	Bank of England
CFI	Cybersecurity Fortification Initiative
CFR	Council of Financial Regulators
CISU	Cyber and Information Security Unit
CORIE	Cyber Operational Resilience Intelligent Led Exercises Scheme
CPMI	Committee on Payments and Market Infrastructure
C-RAF	Cyber-Resilience Assessment Framework
CRS	Cyber-Resilience Subcommittee
CSP	cloud service providers
DCDT	Department of Communication and Digital Technologies
DDoS	distributed denial of service
DOJ	Department of Justice
ECB	European Central Bank
ECSP	electronic communications service providers
EMV	Europay, Mastercard and Visa
fintech	financial technology
FMI	financial market infrastructure
FSB	Financial Stability Board
FSCA	Financial Sector Conduct Authority
HKMA	Hong Kong Monetary Authority
Hub	National Cybersecurity Hub
INTERPOL	International Criminal Police Organization
IOSCO	International Organization of Securities Commissions
IT	Information Technology
MAS	Monetary Authority of Singapore

NPS	national payment system
NPS Act	National Payment System Act 78 of 1998
PA	Prudential Authority
PFMI	Principles for Financial Market Infrastructures
PIN	personal identification number
POPI Act	Protection of Personal Information Act 4 of 2013
PSP	payment service provider
RBA	Reserve Bank of Australia
RBI	Reserve Bank of India
RBNZ	Reserve Bank of New Zealand
SABRIC	South African Banking Risk Information Centre
SAMOS (system)	South African Multiple Options Settlement system
SARB	South African Reserve Bank
SARB Act	South African Reserve Bank Act 90 of 1989
SWIFT	Society for Worldwide Interbank Financial Telecommunications
UCB	urban cooperative banks
UK	United Kingdom
US	United States
VPN	virtual private network