SOUTH AFRICAN RESERVE BANK

National Payment System Department

Consultation paper on open-banking activities in the national payment system

November 2020

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 and/or settlement systems. Furthermore, the National Payment System Act 78 of 1998 (NPS Act) provides for the management, administration, operation, regulation and supervision of payment, clearing and settlement systems in the Republic of South Africa, and provides for connected matters.

1.2 The national payment system (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/or laws applied or utilised to effect payment. The NPS enables the circulation of money, that is, it enables transacting parties to exchange value. The NPS further contributes to the economy and financial stability in South Africa.

1.3 The global payments landscape is constantly changing due to rapid technological developments, with widespread use of digital payment services. As digital payments grow in pace and scope, companies that use financial technology (fintech) develop innovative products and services that aim to increase convenience and improve customer experience. The participation of fintech companies in the financial sector is increasing competition for traditional service providers, which could potentially benefit consumers but might also introduce new risks. This trend is reinforced by the emerging trend of growing demand for access to customer financial information by third parties to enable these parties to provide innovative financial products and services.

1.4 Online banking has streamlined the practice of sharing customer financial information with third-party providers in many countries around the globe, including South Africa. Significant growth in e-commerce and mobile

applications (apps) as the use of smartphones becomes more widespread, has underpinned the increase in online banking over the past two decades.

1.5 Third-party providers are predominantly fintech companies that leverage technology to offer innovative financial products and services. These products and services have also been offered in the domestic NPS, particularly in the e-commerce environment with minimal regulatory oversight. One such service is payment initiation using screen scraping. Screen scraping is the technology that reads and extracts data from a target website using computer software that impersonates a web browser to extract data or perform actions that users would usually perform manually on the website.

1.6 In the payments industry, screen scraping involves a third party developing an app to get direct access to a consumer's online banking profile and subsequently taking over the Internet banking session and automating a payment on behalf of the consumer. For screen scraping to work, a customer should share his/her online banking credentials with the fintech firms practising screen scraping, namely his/her login names, personal identification numbers (PINs) and passwords.

Stylised facts about screen scraping

1.7 Fintech firms practising screen scraping to initiate payments offer confirmation of payment in real time when purchasing goods and services online. Under the traditional interbank electronic funds transfer (EFT) credit push into the merchant's bank account, the payment will only reflect after several hours (sometimes only in a day or two), resulting in delays, as merchants require a trusted confirmation or notification of payment before the goods or services purchased online can be dispatched. Although online banking platforms provide proof-of-payment notifications that can be generated from traditional EFT transactions, they are sometimes not trusted by merchants as these can be subject to fraud.

1.8 In the European Union (EU), following the publication of the revised Payment Services Directive (PSD2), major screen-scraping businesses have been classified on the activity conducted. These are payment initiation service providers (PISPs) and account information service providers (AISPs), collectively referred to as ‘third-party providers’.

1.9 PISPs initiate a payment transaction on behalf of the customer, meaning that they are able to push money directly from a customer’s bank account by requesting the online banking credentials from the customer. When using a PISP, a customer does not need to access his/her online banking to make a payment for products and/or services they choose.

1.10 AISPs, on the other hand, help customers to gain an overview of their financial position by aggregating and analysing transaction information from one or more of their payment accounts and presenting it to customers to base their decisions on. Similarly to PISPs, AISPs require customer credentials to provide the service. Some AISPs claim that they do not store customer credentials and that their systems do not allow movements of funds, but rather gather and aggregate account information and present it to the customer and third parties. AISPs provide a service for customers to see their account information from different bank accounts in one place, either on the online banking platform or on a mobile app. For example, when a customer applies for a new loan, the customer will need to check his/her creditworthiness by checking earnings and expenses from multiple sources. With an AISP, the customer can retrieve the entire transactions history in one view, with an analysis of his/her earnings and expenses, and make a decision far more quickly and conveniently.

1.11 A typical example of screen scraping in payments is when a customer buys goods online. In this case, the merchant’s website gives the customer options to pay with a debit or credit card (Mastercard or Visa) or through an EFT (sometimes termed an ‘instant EFT’) using a third-party payment provider (i.e. a fintech firm practising screen scraping). When choosing the ‘instant EFT’ option, the merchant’s website will request the customer to select the bank that

he/she banks with. After selecting the bank, a screen will pop out (which may look like the customer's online banking website) requesting the customer to populate their online banking login credentials. The consumer is then prompted to select his/her account from which to pay, after which the third party automatically populates the required payment information (destination bank account number, reference number, amount, bank name, branch code etc.) and initiates the payment. Depending on the bank, the consumer may be prompted to authenticate the payment via the short message service (SMS), via Unstructured Supplementary Service Data (USSD) or within their banking app. The payment may be made either to the merchant's bank account or the bank account of the third party, depending on the third party's business model.[1] The fintech firm practising screen scraping will then, in the background, notify the merchant in real time that the customer has paid for the goods, and that they can therefore dispatch the goods. When using this service, it is most likely that some customers do not know that they are not logging on to their online banking directly but rather sharing their login credentials with the fintech firm practising screen scraping, who 'pushes' the funds on their behalf.

1.12 Graph 1 (below) illustrates the process and the payment chain when a customer chooses to make a payment through a fintech firm practising screen scraping:

- **Step 1:** A customer orders goods from an online merchant via the Internet or a mobile app.

- **Step 2:** The merchant provides the customer with an option to pay for the goods using a third party (a fintech firm practising screen scraping).

- **Step 3:** The customer chooses to use the fintech firm's payment service as a method of payment, and provides their online banking credentials to the fintech firm practising screen scraping.

[1] In the case of fintech firms practising screen scraping that facilitate push payments, merchants will benefit from the removal of liquidity risk and improvement of supply chain management as 'trusted proofs of payment' are provided by the fintech firms in real time.

- **Step 4:** The fintech firm practising screen scraping initiates a payment by 'pushing' funds from the customer's bank account using his/her online banking credentials.

- **Step 5:** Once the funds are 'pushed' from the customer's bank account, the fintech firm practising screen scraping notifies the merchant that the customer has made a payment for the goods, and the merchant is expected to dispense of the goods purchased.

- **Step 6:** The customer's bank credits the merchant's bank account.

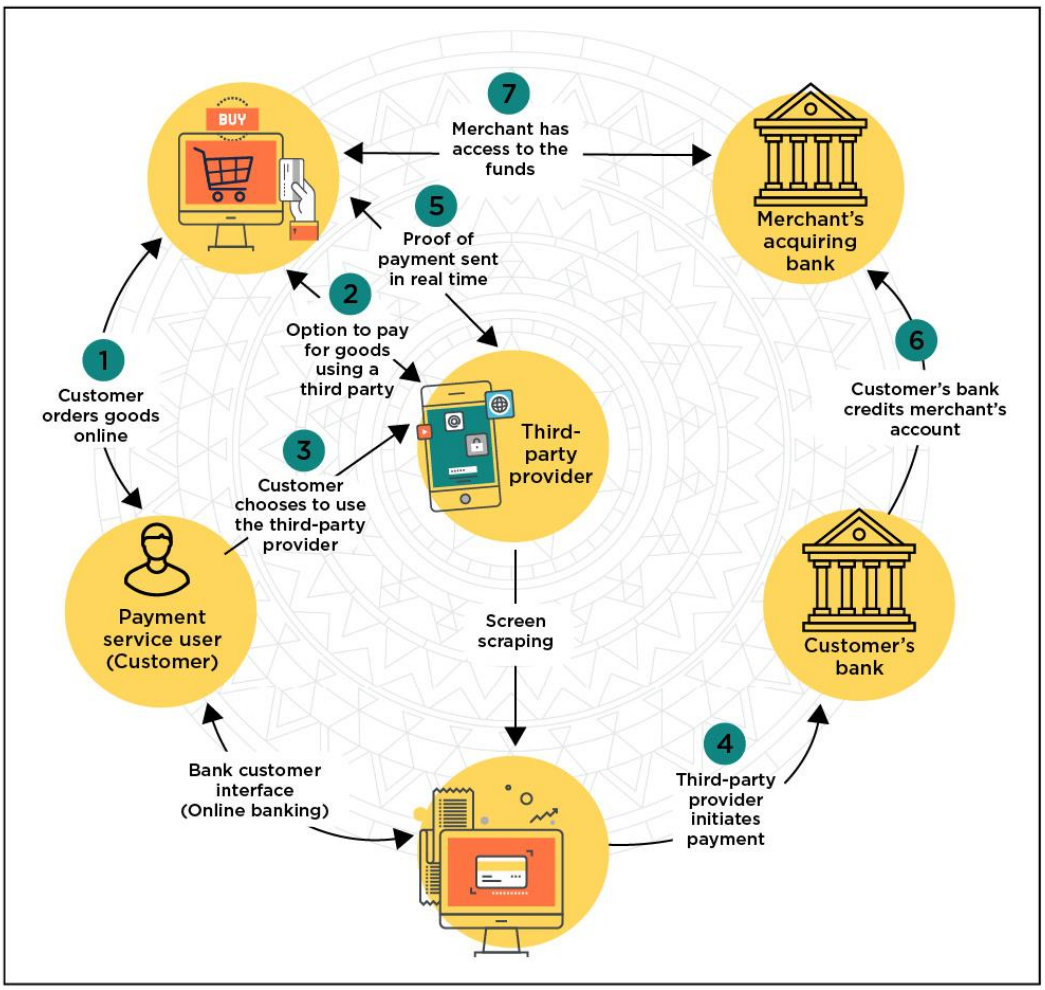
- **Step 7:** The merchant has access to the funds through their own bank.

1.13 Accessing customers' financial information using screen scraping has generally been found to be less secure from data privacy and consumer protection perspectives, among others, and there have been growing interventions by regulators[2] to combat this practice, as it poses risks to the integrity, safety and efficiency of payment systems as well as to the consumer. Furthermore, some third parties practising screen scraping also engage in sort-at-source in the NPS[3], which is an activity that bypasses the clearing system, where a person submits payment instructions directly to a member holding a destination account. In particular, screen scraping has been popularised in the world of fintech because of a lack of legal frameworks and policies in the banking sector that allow the sharing of customers' financial information securely with third parties for payment and/or account information purposes.

[2] In Europe, the European Commission has issued the revised Payment Services Directive (PSD2) directing banks to open up their systems to allow third-party access to certain customer account information, subject to customer consent. The Hong Kong Monetary Authority introduced the Open Application Programming Interface (API) Framework in July 2018, which aims to facilitate the development and wider adoption of APIs by the banking sector.

[3] See the SARB's notice on sort-at-source on its website, at http://www.resbank.co.za/RegulationAndSupervision/NationalPaymentSystem(NPS)/Legal/Documents/Information%20Papers/Sort-at-Source%20Notice%20Ref%2018-2-1-10-C.pdf.

Graph 1: The screen-scraping process flow in payments



Application Programming Interface

1.14 As screen scraping has been found to be generally unsecure, banks and other non-bank financial institutions are exploring the adoption of Application Programming Interfaces (APIs) as an alternative to share customers' financial information to support the provision of innovative payment solutions and improve customer experience.

1.15 APIs are software tools that enable different systems and apps to talk to one another and share data. In the early days, APIs were largely internally focused, proprietary and non-standardised, meaning that they were inaccessible to the outside world and that substantial customisation work was needed to link to

them. These internally focused APIs are known as ‘closed APIs’. They are used by developers in an organisation for internal use only, and are designed to reduce costs, increase efficiency and enhance security.

1.16 Recently, there has been an emergence of open APIs, which are used by third parties for creating innovative apps and products that may bring convenience to existing customers and/or increase customer reach. For example, Google Maps uses open APIs that allow customers to sign into other online accounts using a separate account such as Uber to share their location with the Uber driver for a pickup.

1.17 In banking, APIs may be used to share customer data or information within the organisation or with third parties, in a secure manner (without sharing login credentials), and with consent from the customer. APIs enable consumers and businesses to obtain account information and initiate and track payments using third-party apps that connect directly into the banks’ systems via public domain.

1.18 However, there might be concerns that APIs could give banks too much power as they are mostly owned by banks as custodians of customer data and they have control over what data to share or not to share. This could result in banks playing a ‘gatekeeping’ role, which could be anti-competitive and inhibit innovation.

The emergence of open-banking

1.19 The concept of ‘open-banking’ emerged as a way for third-party providers to securely gain access to customers’ financial information from banks using open APIs in order to leverage innovative technologies and improve customer experience.

1.20 ‘Open-banking’ is a term used in the global financial industry with several definitions, as the concept is still evolving. The Euro Banking Association defines ‘open-banking’ as ‘a movement “bridging two worlds”, i.e. making it

possible for customers to use their banking service in the context of other fintech services, thereby combining innovative functionalities from banks and non-banks with reach through infrastructure'.[4] The Bank for International Settlements (BIS) defines 'open-banking' as 'the sharing and leveraging of customer-permissioned data by banks with third-party developers and firms to build applications and services, such as those that provide real-time payments, greater financial transparency options for account holders, and marketing and cross-selling opportunities'.[5]

1.21 Both screen scraping and open APIs enable open-banking, but it is the latter that is widely embraced by regulators and banks given that it allows customers' financial information to be shared in a secure manner.

Regulatory opportunities in the ever-changing payments landscape

1.22 Fintech companies have brought innovative offerings to the financial sector, including alternative financial products and services to those provided by conventional financial institutions. As the fintech activities in the financial sector grow in scope, there are both opportunities and risks for policymakers, regulators, supervisors and overseers to consider.

1.23 Regulators and policymakers around the globe are currently assessing the adequacy of their regulatory frameworks as the adoption of digital payment solutions offered by fintech companies increases, with the objective of harnessing the benefits while mitigating the risks. For example, in Europe, PSD2 directs banks to open up their systems to allow third-party access to certain customer financial information (subject to the customer's consent) to enable the offering of either payment initiation or account information services.

[4] Euro Banking Association, 2016, *Understanding the business relevance of open APIs and open banking for banks*, available at https://www.abe-eba.eu/media/azure/production/1380/understanding-the-business-relevance-of-open-apis-and-open-banking-for-banks.pdf
[5] Bank for International Settlements, 2019, *Report on open banking and application programming interfaces, a*vailable at https://www.bis.org/bcbs/publ/d486.pdf

2. Purpose and scope

2.1 The purpose of this paper is to develop an NPS policy position on open-banking.

2.2 The scope of this paper covers open-banking activities as they relate to payments.

3. Problem statements

3.1 **The SARB does not have a policy or regulatory framework for open-banking.** More specifically, the NPS Act does not have provisions that deal with open-banking, screen scraping or APIs. However, there have been increasing concerns regarding screen scraping and its impact on the safety and integrity of the NPS, consumer data protection, and other risks it may pose to customers. Although some NPS participants embrace the use of APIs and open-banking, the absence of a firm policy and a regulatory framework is negatively impacting on the progression of open-banking initiatives.

3.2 **There is a lack of accurate information about screen-scraping activities.** Given the unregulated state of screen scraping and APIs, and the nascent stage of open-banking, accurate data and information regarding the domestic landscape is very limited. This makes it difficult to calculate or at least estimate the industry volumes and values of transactions from these activities with absolute certainty. There is also no official record on the number of companies conducting screen-scraping activities in the domestic payments industry.

3.3 **In South Africa, data protection legislation was only implemented fully in July 2020.** The Protection of Personal Information Act 4 of 2013 (POPI Act) gives effect to the constitutional right to privacy by introducing measures that ensure that the way in which personal information is processed by organisations is fair, responsible, and conducted in a secure manner. However, the POPI Act was only fully enacted in July 2020, as some parts of

it could not be enforced given that regulations to the POPI Act regarding personal data processing protection had not been issued. Furthermore, the implementation allows for a one-year grace period for full compliance.

3.4 **Screen scraping presents safety and integrity challenges in the NPS.** Screen-scraping activity exposes customers to the risk of loss of data and money due to uncertain liability and protection mechanisms. It is unclear how consumers would exercise control over the scope or the duration of access to their credentials that they gave to a third party until they changed their passwords. A key threat is cybersecurity risk, whereby consumer data could be breached, leaked or used inappropriately, which could undermine the confidence in the entire payment ecosystem.

3.5 **Merchants are exposed to counterparty risk as they rely on notifications from third parties to dispense their goods and assume that paid funds will be made available.** Possible loose arrangements between merchants and fintech firms practising screen scraping, as well as a lack of oversight and regulation on third parties, may result in risks which may be particularly acute in the specific case of fintech firms practising screen scraping that 'push' funds from the customers' bank accounts for onward payment to merchants.

3.6 **Banks may face reputational risk as third parties do not carry liability and are not subjected to the regulations applicable to banks.** Currently, many consumers assume that if their online banking credentials are compromised, the bank is accountable, but this is not necessarily the case, and may result in the affected bank erroneously suffering reputational damage.

3.7 **Operational risk is one of the key risks in the use of digital solutions, including screen scraping and APIs.** This can manifest in the form of system malfunction, human error and misconduct. A system malfunction may seem manageable, but when customer information is largely digitalised, technology can be vulnerable to compromise that is caused by weak controls and may expose the system to cyberattacks.

3.8 **Screen scraping exposes customers' financial information to fraud.** Since fintech firms practising screen scraping take control of the transaction or session by impersonating the consumer, they may act beyond the expectations of the consumer in relation to the payment account. This can include the actions of a rogue fintech firm practising screen scraping or employees of a screen-scraping entity that fraudulently use consumer data for various unauthorised reasons.

3.9 **There is legal uncertainty in respect of liability, and a lack of dispute resolution mechanisms for customers.** Customers who choose to utilise screen-scraping services do so at their own risk. There is no clarity on the accountability for liability and dispute resolution mechanisms, especially as screen scraping requires consumers to pass on their online banking login credentials, leading to potentially major complications should these end up in the wrong hands. This could result in serious reputational damage to innocent entities in the value chain should funds be stolen or data be breached, as some of them are custodians of customers' deposits and personal data. It should be noted that a customer who shares login credentials with a third party could be in contravention of the terms and conditions of using banking products and services, although banks have indicated that this might not be enough to manage uncertainty with regard to liability risk.

3.10 **Different regulatory approaches exist.** While open-banking could have benefits for end users and foster innovation and competition for banks and non-banks alike, support from regulators might be uneven due to their different mandates. Therefore, this calls for a review of financial sector regulation (including of payments), competition and data privacy laws, all of which may need alignment. This explains why, globally, regulators and policymakers are currently reviewing their approaches to data sharing and open-banking, contributing to progress in fostering innovation.

4. Drivers of screen scraping, APIs and open-banking

Screen scraping

4.1 Ever-changing consumer habits and technology advancements, including the rise in fintech companies offering alternative payment solutions, are driving changes in the payment landscape. These developments are delivering a stream of innovations focused on meeting consumers' financial services needs more effectively. Consumers are also becoming indifferent about whether these solutions are provided by their bank or a non-bank third party such as fintech companies, and tend to gravitate towards solutions where the experience is as seamless as possible. In the case of payments initiated through screen scraping, the user experience delivered by a fintech firm is not cumbersome for consumers who do not have to worry about carrying a card or remembering a card number.

4.2 Screen-scraping activities have gained traction in South Africa due to a lack of effective and attractive real-time retail electronic payments that offer merchants immediate confirmation of payment for e-commerce transactions. It should also be noted that screen scraping is seen as having the potential to reduce the card acquiring costs for merchants as it provides customers with an alternative payment mechanism linked directly to their bank accounts.

4.3 The traditional model of creating batch files of transactions and sharing them via a file transfer protocol network on a deferred basis is regarded as no longer fit for purpose by consumers who need payment providers to offer real-time or immediate payments. Financial customers, including major corporations, are now demanding payments as well as cash management and treasury service experiences that mirror the speed, ease and convenience provided by new technologies.

4.4 Screen scraping may be attractive to criminals, where criminals can set up an illicit third-party payment provider business with the purpose of harvesting personal information and/or stealing customer funds. This practice is highly

probable in an environment where there is still a lack of understanding of screen scraping due to the absence of a clear legal and regulatory framework, which leads criminals to take advantage of weak regulatory regimes.

APIs and open-banking

4.5 As mentioned above, there has been a global demand for access to customers' financial information by third-party providers in order for them to provide payment services that would meet, or be tailored to, the needs of the customer. Unlike screen scraping, open APIs are considered a secure way of giving third-party providers access to customers' financial information to enable the provision of enhanced services, as they do not involve sharing sensitive information like login credentials. This should, however, involve banks getting permission from their customers to share certain of their account information with third-party APIs in a secure and seamless manner.

4.6 Open-banking has the potential to transform financial services (including payments), increase competition, broaden service offerings, support innovation, and improve convenience and customer experience. Furthermore, open-banking aims to leverage recent digital developments in the financial sector by creating data-driven financial services, and also has the potential to provide consumers with greater transparency on the products and services offered by financial institutions, thus allowing them to make more informed decisions. It also makes it easier for consumers to move and manage their money. When it is implemented with appropriate regulatory frameworks in place, it can strengthen collaboration between the banking sector and fintech companies.

5. Policy objectives

5.1 This paper outlines a review of the practices of screen scraping, APIs and open-banking, and their possible contribution to the achievement of the goals and strategies contained in the *Vision 2025* document and ultimately the

mandate and objectives of the SARB, which is to ensure the safety and efficiency of the NPS. Efforts to address the issues or problems associated with screen scraping, as outlined in Section 3, will positively contribute to the achievement of *Vision 2025* objectives. For the purposes of this paper, focus is given to the following *Vision 2025* objectives:

5.1.1 **Financial stability and security.** The sharing of sensitive personal customer data across platforms increases security and privacy risks. A key threat is the risk of misuse of consumer information and loss of funds, which would undermine confidence in the entire payment ecosystem and ultimately have a negative impact on financial stability and security. Therefore, a clear policy position regarding this matter should mitigate such risks to the industry.

5.1.2 **Transparency and public accountability.** Currently, it is not clear to what extent consumers understand the risks involved with the various uses of their banking credentials, including the limited liability accepted by many third-party providers relative to their bank or credit card issuer. This may be compounded by the fact that some third-party providers may in turn share those credentials with other parties in the value chain. Furthermore, should a screen-scraping service provider's system be breached in any way, it may not be clear who would bear responsibility for the losses that may be suffered.

5.1.3 **A clear and transparent regulatory framework and governance.** To date, the SARB has not given direct focus to the practice of screen scraping. This policy paper aims to address this matter and develop a regulatory framework that will introduce standards for open-banking in order to maintain the safety, integrity and efficiency of the NPS.

5.1.4 **The promotion of financial inclusion, competition and innovation, and cost-effectiveness.** Open-banking may help create a level playing field for both banks and non-banks in offering payment services and solutions that will improve customer experience without compromising the integrity of transactions, financial stability or financial inclusion. This will contribute to an increase in the speed of payments and the reduction of costs to consumers.

6. The benefits and risks of open-banking

Participants	Benefits	Risks
Consumers	**Convenience** • When buying goods online, consumers may not have to log on to both the banking and the merchant websites to make online payments. • Consumers do not have to email proofs of payment for online purchases. • Open-banking creates infrastructures to facilitate the efficient offering of payment services to consumers. • The retail customer experience is improved, particularly on e-commerce. • There is easier account comparison and switching. • It is safer to share transactional data with third-party providers. **Alternative payment options** • Open-banking provides alternative payment methods to traditional card and transactional account payments. **Increased competition** • Consumers benefit from increased competition as greater access to the payment system by third parties will potentially lower fees on payment products and services.	**Exclusion** • Although digital payments are growing, many consumers still have low digital capabilities and may not take advantage of some digital solutions. • Some consumers with access to the Internet or smartphones may not have the confidence or trust in open-banking. **Fraud** • Customers' financial account data could be used for purposes that are not mandated by the customer. **Data security and privacy** • Open-banking exposes customers to the risk of data theft and inappropriate use. **Loss of funds** • Weak security measures could expose bank customers to a loss of their funds to criminal activity. **Conduct risk** • Consumers may not understand the risks involved when sharing their banking data, including the limited liability accepted by many third-party providers.
Third-party providers	**Business opportunities** • Open-banking creates a level playing field for non-bank third-party providers, which presents an opportunity for them to offer payment solutions that will improve customer experience. • Open-banking may encourage greater usage and offering of innovative solutions by third parties.	**Reputational risk** • If third-party providers are not subject to the same regulations as banks, they may expose banks and merchants to reputational risks through data misuse. **Fraud** • Unethical employees of third-party providers could use or sell consumer data to unscrupulous parties. **Operational risk** • System malfunction, human error and cyberattacks are some of the risks in digitalised solutions.

Participants	Benefits	Risks
Banks	**New business opportunities** • Open-banking provides banks with the ability to introduce new offerings and enhance their current service offering on payment accounts to other services as well as other markets. • It allows banks to create new partnerships and access new revenue streams through an API-based economy.	**Reputational risk** • Potentially fraudulent or rouge third parties, and unauthorised use of consumer data, can have a negative impact on consumer trust in the bank. **Disintermediation** • Third-party providers may reduce banks' role as the main intermediators, potentially leading to partial loss of customer relationships. • Banks could lose revenue from fees. **Change in business model** • The current operational infrastructure, including Know Your Customer (KYC), transactional monitoring and security checks, will need to change to allow for API functionality. This could increase the costs for banks and have competitive challenges for banks.
Merchants	**Convenience** • The customer experience is improved. • Merchants could gain the ability to enhance customer relationships. **Wider market reach** • Open-banking could grow merchants' product offering and reach markets that were previously difficult to reach. **Lower card transaction costs** • Open-banking has the potential to displace various fee elements of card transactions that constitute the merchant service charges from the issuing banks, acquiring banks, processors and schemes, which should be positive for consumers.	**Reputational risk** • Merchants may also be exposed to reputational risks if consumers lose their data or payments are intercepted. **Counterparty risk** • Third parties may go bust and fail to honour their obligations to merchants. **Operational risk** • System challenges, data breaches and human error could affect the dispatch of products and negatively affect consumer confidence. **Fraud** • Merchants may be exposed to accepting payments that originate from illicit activities, whereby consumer data has been breached or accessed fraudulently.
Payment system	**Competition and innovation** • The payment system benefits from increased competition as the levelled playing field will potentially bring innovative payment solutions.	**Operational risk** • System malfunction, human error and cyberattacks may negatively affect integrity and confidence in the payment system.

Participants	Benefits	Risks
	Transparency • Open-banking can enhance the transparency of payment flows by eliminating fake and rouge third-party providers and building technical and data-sharing standards. **Efficiency** • Open-banking may create infrastructures that underpin payment instruments and mechanisms that are efficient for clearing and settling transactions.	• More third parties could practise sort-at-source should they have access to all banks' APIs. **Settlement risk** • Third-party providers that acquire transactions may fail to honour their obligations to merchants as a result of liquidity challenges.

7. The domestic landscape

7.1 During the development of this paper, the SARB conducted a survey of screen-scraping practices and open-banking activities in the payments industry. The aim of the survey was to assess the prevalence of these practices and activities in the market.

7.2 The results of the survey indicate that the market is still in its nascent stage, and banks reported divergent experiences with these practices and activities. The majority of banks could not report on the magnitude of transactions that involve screen scraping, as they could not reliably detect screen scraping and were not aware of screen-scraping activities embedding their websites. In addition, banks have not received disputes or complaints about these practices from their customers. However, banks generally raised concerns about the unsafe nature of screen scraping, which may pose a liability to them and data security risks for customers. Banks that offer traditional transactional accounts foresee the risk of disintermediation by third parties as a result of the growing emergence of open-banking, while banks that operate largely in the corporate environment do not expect their business model to change significantly.

Screen scraping

7.3 The survey results indicate that there are about five major or dominant service providers in the industry, most of which are PISPs. Among these five parties, only two are registered with the Payment System Management Body (PSMB) or the Payments Association of South Africa (PASA). Of the two registered parties, one is registered both as a System Operator (SO) and as a Third Party Payment Provider (TPPP), while the other party is only registered as an SO.

7.4 Over and above the five major service providers identified, the prevailing view of the market is that there are other operators that screen-scrape bank websites in South Africa, with some of these operators domiciled in other jurisdictions. Anecdotal evidence suggests that some financial institutions use screen scraping to access customer information in order to offer multi-banked customers data analytics of accounts held at multiple banks. In addition, it appears that some organisations may be screen scraping banks' websites to access their own accounts. However, in this case, data security risks would be limited as these organisations do not use a third party but their own systems to access their information.

7.5 The majority of the banks indicates that they do not endorse or support third-party use of screen scraping to access customer information, but do and would allow approved vendors to access customers' financial information using APIs. A minority of the banks, however, does allow third parties to gain access to customers' financial information using screen scraping to render services to their clients. When on-boarding third-party vendors, banks conduct due diligence and enter into service level agreements. Although most of the banks indicate that they do not allow screen scraping, they do not have mechanisms to block it, as it is difficult to do so. It is expected that the POPI Act will address some of the data privacy challenges emanating from screen-scraping activities. The POPI Act will ensure that information capturing, storage and usage through systems is aligned with its requirements and objectives.

7.6 The customer protection approach adopted by banks differs across banks. For banks that allow screen scraping and have contractual relationships with fintech firms practising screen scraping, there should be a liability clause in their agreements that would enable customers to claim for loss of data and/or funds for various reasons. Further, contractual agreements between banks and third parties generally make provision for the prohibition of the reselling of customer-permissioned data to be shared beyond the scope of the agreement. Banks without contractual relationships rely mainly on the existing data privacy and consumer protection laws, for example the POPI Act and the Consumer Protection Act 68 of 2008.

7.7 The results of the SARB's survey further indicate the extent to which some of the banks would not be in a position to understand the risks involved with screen scraping as they cannot detect all the activities conducted through screen scraping on their websites. The existing cybersecurity policies as well as terms and conditions of using banking products and services also appear to be inadequate to manage the risks, and banks propose stringent standards for third-party access to consumer data through APIs. Most of the banks seem to be concerned about data privacy risks, which involve the scraping of credentials and account holder information, as these could be used for unintended purposes.

7.8 PASA is managing the adherence to international standards by SOs and TPPPs to ensure that the data they are storing in their systems is secured through the adoption of standards such as the Payment Card Industry Data Security Standard (PCI-DSS)[6] that can be applied to electronic payment systems.

7.9 The PASA strategy team is also engaging on screen-scraping matters, and options are being explored on how to address various issues. The following options have been proposed:

[6] The Payment Card Industry Data Security Standard (PCI-DSS) is an information security standard for merchants of all sizes, financial institutions, point-of-sale vendors, and hardware and software developers that handle branded credit cards from the major card schemes.

- banks will develop an effective EFT industry solution for e-commerce purchases;

- banks will follow the European PSD2 approach; or

- regulation will be ensured through enforcement standards similar to the PCI-DSS and liability shifts for third parties practising screen scraping. The banking industry has also established a working group that will develop and agree on a common standard for open-banking.

Open APIs and open-banking

7.10 The majority of the banks is in support of open-banking where open APIs are used, given that they are more secure than screen scraping. However, banks have raised concerns about the lack of uniformity in a standard for open-banking APIs. Some banks have indicated that they have APIs which allow approved merchants to integrate their online transactions through e-commerce platforms.

7.11 The key pillar for open-banking is customer consent. All parties accessing data need to sign a non-disclosure agreement that adheres to data privacy standards. Third parties should only have access to data that they require to perform the services that they offer, and they should ensure that there is requisite consent where required.

8. International experiences

8.1 Globally, there is a growing drive for real-time payment capabilities and a levelled playing field to enable bank and non-bank offerings in the financial system. Fintech companies are fast becoming integrated in the payment ecosystems through screen-scraping and open-banking activities, creating

both opportunities and risks that policymakers, regulators, supervisors and overseers are grappling with.

8.2 Regulatory and oversight developments show heterogeneity across jurisdictions. Some countries have taken the approach of mandating banks to share customer-permissioned data. Others issue guidance, notices and recommended API standards. Others still have opted for a flexible approach, with no regulations or standards (see Table 1 below). The common pillars of open-banking across countries include consent, data privacy expectations, and data security requirements.[7] Most jurisdictions embrace the use of APIs to share customer data, and there is currently no widespread ban on screen-scraping practices.

Table 1: Open-banking developments around the globe

Jurisdiction	Initiatives
Australia	• In 2018, the Australian government approved a framework for open-banking. • Open-banking in Australia is being implemented in a phased approach, with the four big banks legally required to make consumer usage data available to consumers on credit and debit cards as well as deposit and transaction accounts from July 2020, followed by mortgage and personal loan data from November 2020. • Other banks will be allowed to start sharing data from February 2021.
China	• Open-banking is not being promoted by regulators but rather by fintech companies. For example, fintech companies allow the connection of Alipay and the use of third-party data through APIs.
European Union	• In the EU, PSD2 directs banks to open up their systems to allow third-party access to certain customer account information, in order to make payments on their behalf (via credit transfers) and to provide them with an overview of their various payment accounts, subject to customer consent. The aim of this is to increase competition and promote innovation through data sharing.

[7] Bank for International Settlements, 2019, *Report on open banking and application programming interfaces*, available at https://www.bis.org/bcbs/publ/d486.pdf

Jurisdiction	Initiatives
Hong Kong	• The Hong Kong Monetary Authority introduced the Open API Framework in July 2018. It aims to facilitate the development and wider adoption of APIs by the banking sector. • Phase I of the Framework was launched in January 2019. • So far, 20 participating retail banks have made available more than 500 open APIs, offering access to information of a wide range of banking products and services.
India	• The Indian government has mandated an open API policy. • In 2016, IndiaStack was introduced as a set of APIs. • The Aadhaar biometric digital system facilitates open API banking through government proprietary software dealing with a centralised database for authentication.
Japan	• The Banking Act was amended in 2018 to require financial institutions to develop APIs for use by third parties.
Malaysia	• The central bank of Malaysia has established open API implementation groups to encourage the use of APIs. • These groups, comprising banks, fintech companies and other key stakeholders, are in the process of identifying and developing standardised open APIs for high-impact use cases.
Nigeria	• Open Banking Nigeria, a non-governmental organisation backed by a group of industry experts across the banking, fintech and risk management industries, is working with industry players to build API standards for the Nigerian financial services sector. • The central bank of Nigeria is currently exploring an open-banking framework, which could result in the development of regulatory requirements for both banks and non-banks.
Singapore	• Singapore is attempting to implement a different type of regulatory framework, with a less aggressive and more organic approach. It is not planning to force regulations onto financial institutions. • The Monetary Authority of Singapore will be working towards guidelines for the ethical usage of data and artificial intelligence that will work for all players within the ecosystem.
United States	• There is no legal requirement for open-banking, and the decision on how data sharing occurs is up to financial institutions. • Entities still use screen scraping rather than open APIs. This includes web-based financial management tools that aggregate customers' financial data.

9. Policy proposals

9.1 **A new class of third-party providers should be introduced, and its access to customers' financial information should be promoted, in order to improve product and service offerings for customers, increase competition, and promote innovation.** There is acknowledgement that third-party providers operating in a controlled environment can offer customers alternative and innovative payment mechanisms and enhance other service offerings that may improve customer experience. It is therefore important to separate the 'good' open-banking practices, which may be allowed, from the 'bad' practices, which may include unsecure screen-scraping activities[8] that should be prohibited. However, opening access for regulated third-party providers to customers' transactional account information should only be allowed subject to customer consent. Opening access to consumer data may also benefit banks by enhancing innovation and customer experience and improving both the competitive and the collaborative relationships between banks and fintech companies.

9.2 **All third-party providers in the NPS should be regulated.** Third-party providers that provide payment services and infrastructure and have access to customer accounts should be regulated by the relevant authorities, such as the SARB and the Financial Sector Conduct Authority (FSCA), in accordance with their respective mandates. Importantly, regulation should include:

- data security standards;
- entry and participation criteria into the NPS;
- insistence on specific minimum requirements that may include a common API standard to allow for open and controlled access to shared data;
- insurance cover to protect consumers in the event of failures; and

[8] This refers to traditional screen-scraping activities whereby the third party has no relationship with the banks they screen-scrape and/or there are no strong authentication mechanisms.

- the implementation of an identification layer that authenticates a third-party provider (a fintech firm practising screen scraping) for accessing customer information from banks.

9.3 **Prior to being granted access to customer information, a third party practising screen scraping must identify itself and provide the requisite credentials to the bank.** This will result in facilitated access to service providers for value-added services from the current form to a model similar to the one adopted under PSD2, whereby screen scraping is offered as a fallback mechanism when open APIs cannot be accessed. However, this could result in fragmentation, complexity and additional costs, as different systems would have to be developed to allow for interface between banks and third parties.

9.4 Graph 2 below depicts the transaction flows with the adoption of open APIs and the implementation of a layer that authenticates a third-party provider (a fintech firm practising screen scraping) for accessing customer information. Graph 2 can be explained in the following steps:

- **Step 1:** A customer orders goods from an online merchant via the Internet or a mobile app.

- **Step 2:** The merchant provides the customer with an option to pay for the goods using a third party (a fintech firm practising screen scraping).

- **Step 3:** The customer chooses to use the fintech firm's payment service as a method of payment, and provides their online banking credentials to the fintech firm practising screen scraping.

- **Step 4(a):** The fintech firm practising screen scraping initiates a payment by 'pushing' funds from the customer's bank account using his/her online banking credentials.

- **Step 4(b):** The API user initiates a payment by pushing funds from the customer without sharing online banking credentials.

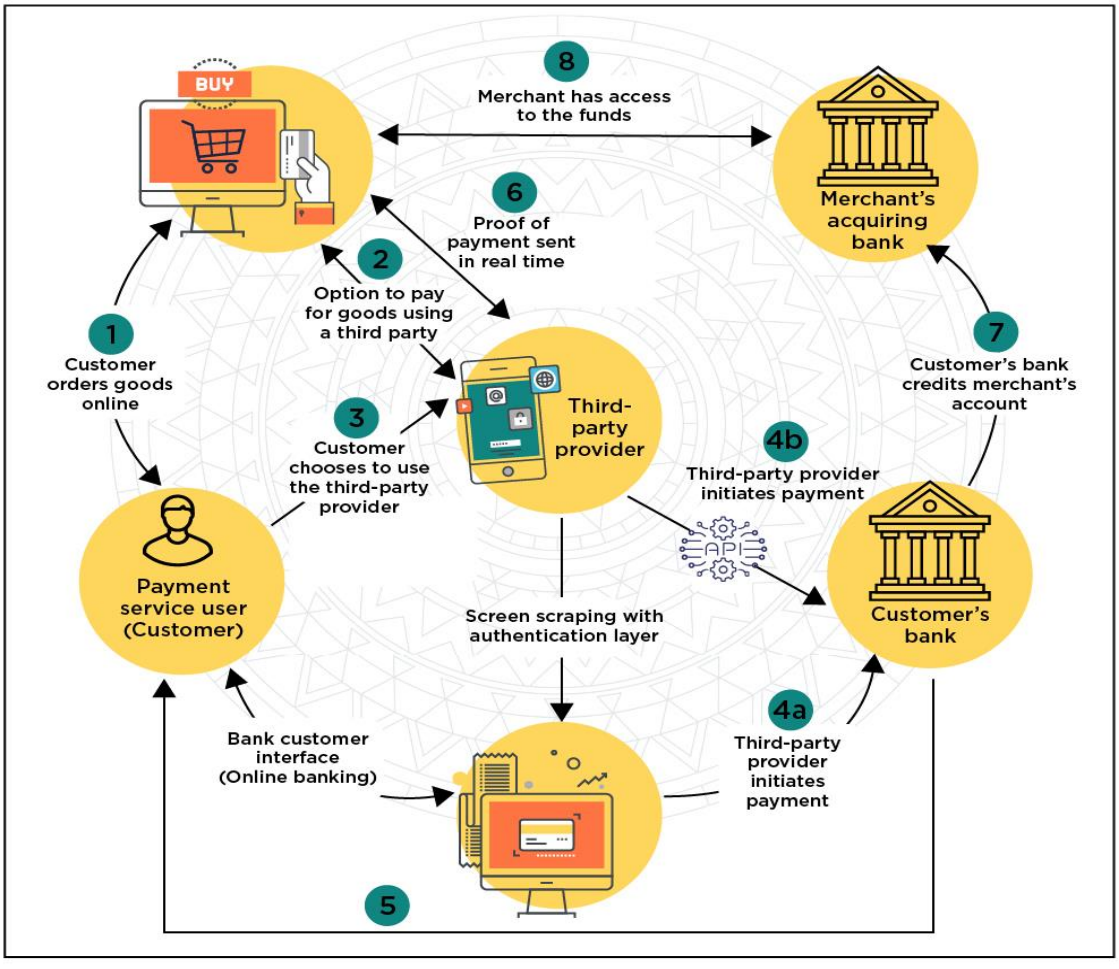
- **Step 5:** Customer's bank notifies the customer about the successful payment.

- **Step 6:** Once the funds are 'pushed' from the customer's bank account, the fintech firm practising screen scraping/API user notifies the merchant that the customer has made a payment for the goods, and the merchant is expected to dispense of the goods purchased.

- **Step 7:** The customer's bank credits the merchant's bank account.

- **Step 8:** The merchant has access to the funds through their own bank.

Graph 2: Authenticated screen scraping and the API process flow in payments



9.5 **Banks should provide access to customers' financial information, subject to customer consent, to regulated third-party payment providers.** Banks should grant non-bank payment providers access to their systems for the development of APIs as a safe mechanism to enable the sharing of customer data. Fintech companies that develop and provide APIs should also be regulated and subjected to open-banking technical standards. Reciprocity of sharing customers' financial information should apply to ensure fairness.

9.6 **Technical standards for open-banking should be developed and implemented.** This could include the establishment of open-banking working groups that should include NPS participants, regulators (such as the FSCA, the Information Regulator, the Prudential Authority, and the SARB), and other relevant authorities (such as the Competition Commission and National Treasury) and stakeholders to identify and develop standards for open-banking.

9.7 **Third-party providers must not store customer information and must only use the information for its intended purpose.** PISPs and AISPs should only access the data that is necessary to provide the service(s) selected by the consumer, and there should be no storage of customers' login credentials or data (for security and data protection reasons). Third-party providers must be prohibited from the on-selling or distributing of data.

9.8 **Third-party providers should bear the risks and costs that they introduce to consumers.** They should also make the necessary efforts to prevent, detect and resolve any unauthorised access and/or data sharing. In addition, they must have put in place requisite insurance or guarantee mechanisms against possible losses, and they must always protect the integrity of the NPS.

9.9 **Third-party providers should implement effective processes to mitigate operational risks.** Third-party providers should implement mechanisms to promptly respond to, resolve and remedy any data breaches, transmission errors, unauthorised access and fraud. In addition, the management of customer credentials should be in place to prevent interception or compromise.

Operational risk could be mitigated when the technologies and systems used for open-banking are subject to prudent regulation and oversight.

9.10 **Consumers should have practical means at their disposal to dispute and resolve instances of unauthorised access, the failure by merchants to honour purchase orders, and possible data breaches.** Such dispute resolution mechanisms will benefit consumers, banks and third-party providers alike, as they will curb the loss and reputational risks that providers may face.

9.11 **Consumer education or awareness should be conducted.** As indicated throughout this paper, many consumers may not be aware of the potential risks when using third parties to effect payments or the services of data aggregators. In this regard, educating consumers will be important in building trust on open-banking products and services, and ultimately the success of open-banking. Banks, third parties and regulators should play a key role in educating consumers about open-banking; this could be achieved by issuing safety notices and guidelines.

9.12 **Consumers should be educated about their right to withdraw consent at any time, provided that the withdrawal does not violate other legitimate obligations.** Custodians of consumers' financial information should ensure that the withdrawal of consent is made as easy as possible.

10. Conclusions

10.1 Currently, the SARB does not regulate, supervise or oversee open-banking activities such as screen scraping and open APIs, including their effectiveness, soundness, integrity or robustness. Consequently, the consumers and entities involved in open-banking activities have no recourse to the SARB.

10.2 The SARB is of the view that open-banking activities should be regulated and reformed, risks should be managed, and safety considerations should be

embedded, all the while ensuring that customer convenience is ensured and enhanced. The banking industry should develop secure control systems and protocols that require third-party providers to be identified and authenticated by banks as they access customer data.

10.3 The information currently available indicates that the screen-scraping practice poses no significant risk to financial stability at this stage. However, consumers are exposed to data protection and cybersecurity risks, and are cautioned about the possibilities of loss or theft of data shared with third parties that use screen scraping to offer alternative payment solutions and account information services.

10.4 Regulations relating to data sharing and open-banking should strike a balance between risk management and incentives for promoting innovation. Regulatory frameworks should set clear roles and responsibilities in line with market changes.

10.5 By collaborating and sharing information on this matter, regulators and industry stakeholders will be able to identify relevant opportunities and weaknesses in the NPS and address them proactively. Encouraging collaboration within the industry will go a long way in improving the understanding of the regulatory requirements of the practice of data sharing and the emergence of open-banking.

11. The way forward

11.1 The planned consultation process and timelines going forward are as follows:

- Comments on this consultation paper should be received by 31 January 2021.

- An industry workshop will be arranged in January 2021.

12. Comments and contact details

12.1 Stakeholders and other interested parties are invited to forward their comments on this consultation paper by 31 January 2021. Comments should be addressed to npsdirectives@resbank.co.za.