Digital Payments & Remittances

(mobile wallets/e-money, payment initiation, mobile point-of-sale)

South Africa

www.bfaglobal.com | @bfaglobal

UPDATED 28 JUNE 2021

Funded by
UKaid
from the British people

Cambridge Centre for Alternative Finance
UNIVERSITY OF CAMBRIDGE Judge Business School

Disclaimer

To the best of our knowledge, the information contained herein is accurate and reliable as of the date of publication.

However, **BFA Global** and the **Cambridge Centre for Alternative Finance** do not assume any liability whatsoever for the accuracy and completeness of the deck, and we provide no warranty, expressed or implied, in respect thereof. The provision of the information contained in this deck does not constitute legal or financial advice or opinions of any kind. No advisory, fiduciary, or other relationship is created between us and any person accessing or otherwise using any of the information provided herein. **BFA Global**, the **Cambridge Centre for Alternative Finance**, any of their directors, officers, employees, agents, or contributors will not be liable for any damages, losses, or causes of action of any nature arising from any use of the said information.

How to use this deck

Relevant regulations

1. Payments
2. Data protection
3. Consumer protection
4. AML / KYC
5. Cybersecurity
6. Competition
7. Taxation
8. Other

This deck provides **an overview of the various regulations relevant to digital payments and remittances in South Africa,** including product areas like **mobile wallets/e-money, payment initiation, and mobile point of sale**.

Each slide in this deck provides high-level facts about each of the relevant regulations as well as a link to the original source.

The Cambridge Centre for Alternative Finance (CCAF) and BFA Global's Catalyst Fund have developed this deck to help fintech startups working in South Africa and those seeking to enter the South African fintech market navigate the regulatory environment.

Cambridge Centre for Alternative Finance

UNIVERSITY OF CAMBRIDGE Judge Business School

01 — Payments

Payments: **General overview**

Cambridge Centre for Alternative Finance
UNIVERSITY OF CAMBRIDGE Judge Business School

Main regulators:

SARB has a mandate to conduct, monitor, regulate, and supervise the payments sector in South Africa.

Payments Association of South Africa (PASA) is the governing body for payment systems. It is responsible for organizing, managing, and regulating its members' participation in the payment system.

Key regulation:

The South African Reserve Bank Act, 1989, the National Payment System Act, 1998, the Financial Services Laws General Amendment Act 22, 2008, and the Banks Act, 1990

Main provisions:

- Providers of Payment Services must register as a System Operator (SO) or third-party payment provider (TPPP) with PASA.
  - SOs provide the electronic means for parties to receive or send funds.
  - TPPPs accept money or the proceeds of payment instructions from two or more payers for payment to third persons to whom the money is due.
- Providers of Payment Services cannot issue e-money; only registered South African banks can.
- For members of PASA to clear payment instructions, there must be an understanding of the business rules, requirements, and technical agreements that make clearing possible.

Sources: South African Reserve Bank Act, 1989, the National Payment System Act, 1998, the Financial Services Laws General Amendment Act 22 of 2008, The Banks Act, 1990,

Payments: **Registering as a provider of payment services**

Who:

SOs are non-bank providers of services in relation to payment instructions.

TPPPs are non-bank providers and can either be a Beneficiary Service Provider (BSP) and Payer Service Provider (PSP).

How much:

PASA's Constitution provides a formula for the calculation of fees in Clause 33.

Permitted activities:

- An SO provides the electronic means (including the delivery to and/or receipt of payment instructions) to two or more persons to allow such persons to make payments and/or to receive the proceeds of payment instructions.
- A TPPP accepts money or proceeds of payment instructions from two or more payers for on-payment to third persons to whom the money is due.
- A TPPP is generally enabled by an SO, and may hold funds for payment due in its own bank account for a short time. An SO only provides the technology but does not accept the funds into its own bank account for on-payment to another party.

How:

SO entry and participation criteria are prescribed by PASA. The application is required to be made in prescribed form, which is accessible via the PASA website, alongside supporting documentation. Applicants are required to different types of criteria as detailed in Section 3 of the PASA document. This includes:

- Be a registered company.
- Financial criteria includings providing a certified copy of the report of the external auditors in respect of the latest financial year end; on request, providing to the SARB certified copies of its audited annual financial statements.
- Operational criteria including having tested its systems to ensure it is operationally and technically capable of providing the service.
- Legal and contractual requirements requiring the SO to enter into a written service level agreement with each person to whom services are provided, that obliges the parties to comply with all the appropriate requirements and rules for providing a service as contemplated in the authorization criteria, the NPS Act and any other applicable law.
- Applicants are required to pay "a non-refundable application fee, determined by PASA from time to time".
- PASA is empowered to exempt persons from authorization after consultation with SARB and the applicant.

All TPPP's are required to be registered by a clearing participant who may be banks or designated clearing system participants (who may be non-banks)

Sources: the National Payment System Act, 1998 SARB Directive for Third Party Payments Providers PASA Constitution , SARB Directive 2 of 2007 for System Operators NPS Key Role Players

Payments: **Legislative reform & fintech firms**

Legislative reform:

SARB has launched an evaluation of current payment systems legislation, which could have implications for payment systems and fintech providers in years to come.

SARB's Policy Paper on the Review of the National Payment System (NPS) Act highlights several reasons to examine the robustness and resilience of the NPS legislative and regulatory framework in the rapidly evolving, technologically advanced, and highly innovative payments landscape. The target date for legislative reform is 2022.

Fintech firms in payments:

A potential barrier for fintech firms is that all businesses must have prior approval and authorization from PASA to engage in any payment activity. These authorizations may be very difficult to obtain.

Due to the restrictive licensing process, a number of fintech firms have partnered with 'traditional' financial services providers, such as banks. However, the Banks Act requires SARB approval for contractual engagements between a bank and a non-bank entity where the parties undertake an economic activity that is subject to their joint control.

Sources: Policy Paper on the Review of the NPS Act, The Banks Act, 1990,

Payments: **E-money**

Although the SARB investigated the feasibility of allowing non-banks to issue e-money in its 2009 E-Money Paper, it decided to only allow registered South African banks to issue e-money to reduce risk in the national payment system. Thus fintech firms interested in issuing e-money must partner with a bank or earn authorized as a bank pursuant to the Banks Act.

Due to this decision, the use of mobile money and related services, including remittance and mobile payments, are quite limited in South Africa, especially compared to other sub-Saharan Africa countries.

Sources: The Banks Act, 1990, SARB Updated Position Paper on E-Money

Payments: **Remittances & Exchange Control**

Regulator:

SARB controls and oversees all capital inflows and outflows, designating power to authorized dealers (banks) who oversee and regulate the market on their behalf.

Key regulation:

Currency and Exchanges Act No. 9, 1933 and Regulations (Exchange Control Regulations, 1961)

Currency and Exchanges Manuals for Authorized Dealers in foreign exchange with limited authority

Scope:

- Authorized Dealer - a legal person authorized by the Financial Surveillance Department (FSD) of the SARB to deal in gold and/or foreign exchange.
- Authorized Dealer in foreign exchange with limited authority (ADLA) includes bureaus de change, independent money transfer operators, and value transfer service providers, who are authorized by the FSD to deal in foreign exchange transactions.

How:

- The exchange control system, subject to exemptions, requires anyone undertaking cross-border money remittance, i.e. ADLAs, to apply for prior permission from SARB or authorized dealers in foreign exchange (typically banks)
- The Currency and Exchanges Manual for ADLAs contains the permissions and conditions applicable to transactions in foreign exchange that may be undertaken by ADLAs and/or on behalf of their customers.
- SARB's E-Money Paper is silent on whether electronic money customers can send and/or receive international money transfers.
- The Exchange Control Department of the SARB issues Exchange Control Rulings, which lay out administrative measures, permissions, transaction limits, and conditions for Authorized Dealers.

Sources: SARB Updated Position Paper on E-Money, Currency and Exchanges Act No. 9 of 1933 and Regulations (Exchange Control Regulations, 1961, Currency and Exchanges Manuals for Authorized Dealers in foreign exchange with limited authority, SARB FAQ on Foreign Exchange

02

Data protection

Cambridge Centre for Alternative Finance

UNIVERSITY OF CAMBRIDGE Judge Business School

Data protection: **National provisions**

Key laws: Constitution of the Republic of South Africa & The Protection of Personal Information Act, 2013 (POPIA)

Main provisions:

- **The Constitution of the Republic of South Africa** guarantees the right to privacy for every citizen. This right includes the right not to have the privacy of their communications infringed.
- **The Protection of Personal Information Act, 2013** promotes the protection of personal information processed by public and private bodies. It stipulates minimum requirements, creates the role of Information Regulator, and codifies the way organizations can source and use individuals' and entities' personal information, including digital information. Any direct marketing to customers in South Africa is regulated by POPIA.

On cross-border transfers:

- POPIA sets out provisions regarding cross-border information transfers under Chapter 9.
- The transfer of personal information about a data subject by a responsible party to a third party in a foreign country is contingent on meeting certain conditions:
  - The data subject has consented.
  - The third party is subject to laws or binding corporate rules or agreement that provides similar protection to POPIA.
  - The transfer is necessary for the performance of a contract between the data subject and responsible party.

Sources: Constitution of the Republic of South Africa, The Protection of Personal Information Act, 2013

Data protection: **Sectoral provisions**

There are also data protection provisions in sector-specific legislation and regulation:

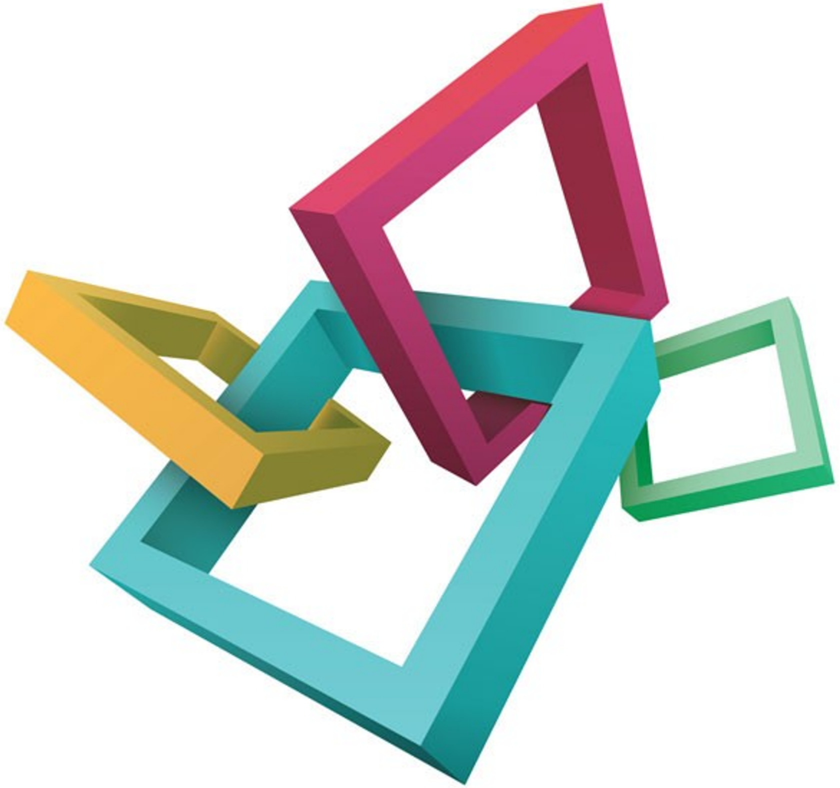
- The South African Reserve Bank Act provides for the preservation of secrecy (Section 33).
- The Code of Banking Practice is a non-binding code that all banks agree to follow. In the code, banks agree to treat all customer personal information as private and confidential (Section 6.1)
- The National Credit Act sets out requirements related to confidentiality, personal information, and consumer credit records (Chapter 4, part B). Persons who receive, compile, retain, or report confidential customer information are obligated to keep this confidential (Section 68).


Government Gazette

Sources: National Credit Act, South African Reserve Bank Act, 1989, Code of Banking Practice,

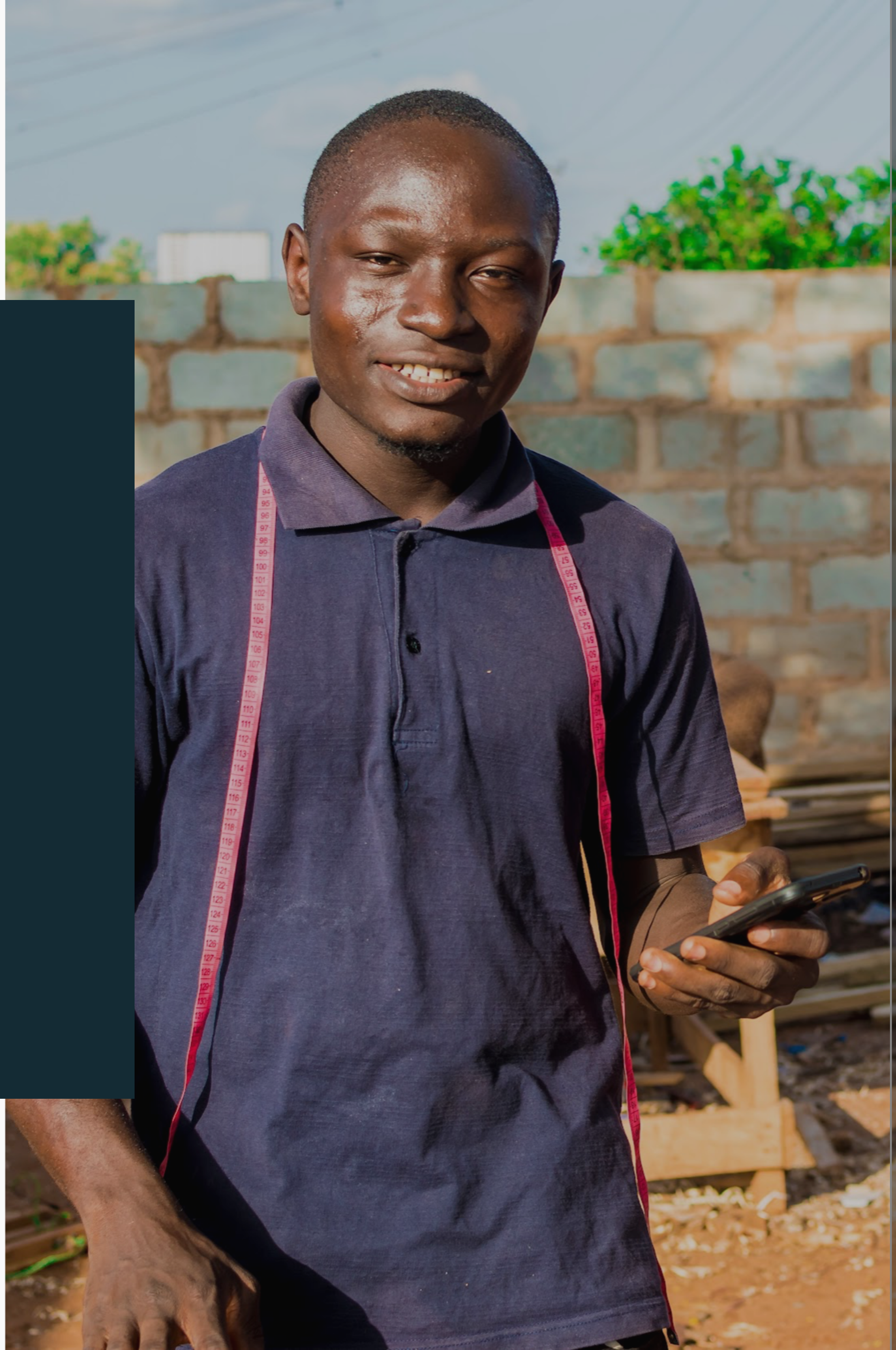
Data sharing: **Open banking**

- There are currently no prescribed requirements for open banking.
- The SARB released a Consultation Paper on "Open-banking activities in the national payment system" in November 2020 for stakeholder comment (not public).
- The IFWG also recently released a paper on "Non Traditional Data Research."
- Firms interested in introducing initiatives in this area should check with SARB, IFWG, and other relevant regulators.



Sources: Non Traditional Data Research,

03 — Consumer protection



Consumer protection: **National provisions**

Cambridge Centre for Alternative Finance
UNIVERSITY OF CAMBRIDGE Judge Business School

Key Laws: Constitution of the Republic of South Africa, the Consumer Protection Act, 2008

Main provisions:

- Schedule 4, Part A of the **Constitution of South Africa** provides that consumer protection is an area of concurrent legislative jurisdiction, which means both the national and provincial governments in South Africa are permitted to pass legislation on consumer protection.

- The **Consumer Protection Act** sets out consumer rights and the responsibilities of product and service providers to protect these rights (see Chapter 2). This includes:
  - the right to privacy, disclosure, and information; and
  - rights related to marketing, fair and reasonable terms and conditions.

  The Act also prescribes how these rights can be enforced and mechanisms for dispute resolution (Chapter 3A and Chapter 6).

Sources: Constitution of the Republic of South Africa, Consumer Protection Act,

Consumer protection: **Sectoral provisions**

There are some piecemeal consumer protection regulations that apply to specific financial service providers including:

- The FSCA introduced the Conduct Standard for Banks (the Standard) on 3 July 2020 to supervise the banking sector's conduct. The Standard sets out high-level requirements for the banking sector aimed at ensuring the fair treatment of financial customers.
- The National Credit Act also sets out consumer protection provisions related to credit marketing practices (Chapter 4 Part C), forms of disclosure in credit agreements (chapter 5 Part B), and on dispute settlement (Chapter 7), among others.

Sources: Conduct Standard for Banks; National Credit Act

04

Anti-money laundering (AML)/know your customer (KYC)

AML/KYC: **Key laws & main provisions**

Key Laws:

The Financial Intelligence Centre Act, 2001 (FICA) and Amendment Act, 2017 regulate money laundering in South Africa

Main provisions:

- Accountable Institutions include banks, financial instrument traders, long-term insurance providers, dealers in foreign exchange, lenders, and investment advisers, as set out in Schedule 1 of the FICA. Not all fintech firms are in scope.
- Accountable Institutions are subject to compliance requirements when accepting new customers, which vary depending on the entity. Each decision-making member of the customer is required to be compliant and the business entity verified by the accountable institution.
- Accountable Institutions must report any unusual or suspicious transactions, include those that have no apparent business or lawful purpose as well as those that appear to be an evasion or attempted evasion of paying a tax, duty, or levy.
- The Amendment Act introduced a risk-based approach to customer due diligence. Accountable Institutions are required to document, maintain and implement a Risk Management and Compliance Programme (RMCP) with respect to anti-money laundering/ combatting the financing of terrorism (AFL/CFT). A copy of this document must be made available to the Financial Intelligence Centre. The Amendment Act changes replace previous prescriptive onboarding requirements and allow entities to choose how to establish and verify customer identity. The documented approach must take into account AML/CFT risks connected with customer onboarding, and the occasional nature of one-off/ ingle transactions (see Chapter 3 of the Act for detailed provisions on CDD).

Sources: The Financial Intelligence Centre Act, 2001, Financial Intelligence Centre Amendment Act, 2017

AML/KYC: **Customer due diligence requirements**

- The Financial Intelligence Centre (FIC), in collaboration with the National Treasury, the South African Reserve Bank, and the Financial Services Board, published Guidance Note 7 on the implementation of a risk-based approach to Customer Due Diligence (CDD). Guidance on CDD measures for various types of customers are set out in Chapter 2 e.g., for natural persons, legal persons, trusts and partnerships.
- For natural persons, identity can be determined by reference to a number of attributes. At a minimum these attributes are the person's full names, date of birth and, in most cases, a unique identifying number issued by a government source (e.g. in the case of a South African citizen or resident, his/her identity number or, in the case of other natural persons, a passport number or numbers contained in asylum seeker or refugee permits, work permits, visitors' visas etc.)
- Previously, banks verified customer identity on the basis of a visual inspection of the barcoded green ID book and visual comparison of the photo in it to the appearance of the (prospective) customer.
- The 'manual' method of identity verification had flaws. To address them, the South African Banking Risk Information Centre (SABRIC) and the Department of Home Affairs (DHA) collaborated to enable the verification of customers' identities by matching their fingerprints directly against the DHA's biometric HANIS database, which sends back a 'verified' or 'not verified' response.

Sources: Guidance on the Implementation of Aspects of the Financial Intelligence Centre Act; Guidance on Digital ID

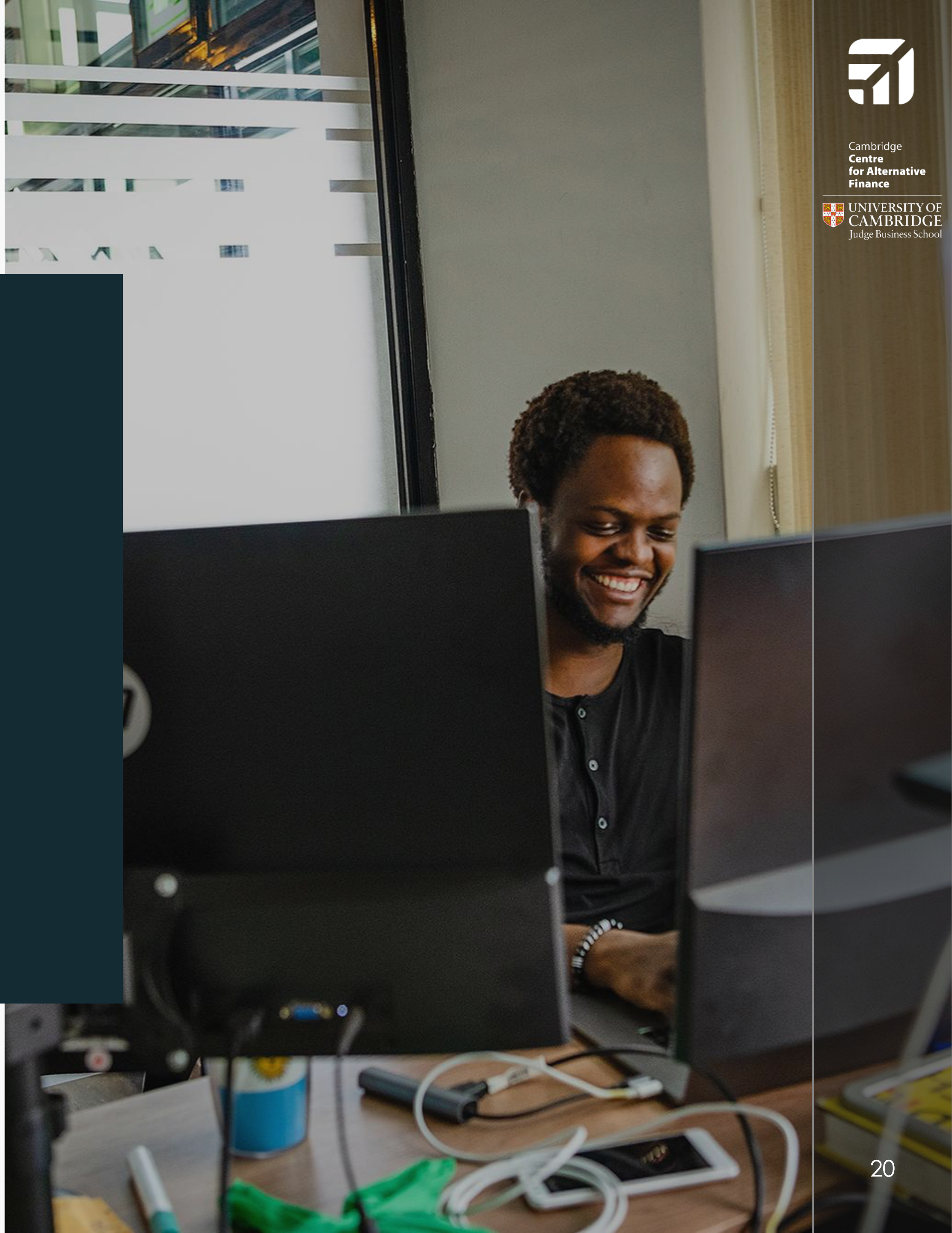
AML/KYC: **Other related requirements**

- **The Prevention and Combating of Corrupt Activities Act, 2004** was introduced to strengthen measures to prevent and combat corruption and corrupt activities, to provide for the offence of corruption and related offences, to create measures to investigate corruption, and to establish and endorse a Register that places certain restrictions on persons and enterprises convicted of corrupt activities relating to tenders and contracts.
- **The Protection of Constitutional Democracy Against Terrorist and Related Activities Act 2004** includes measures to prevent and combat the financing of terrorism and related activities.

Sources: The Prevention and Combating of Corrupt Activities Act, 2004, The Protection of Constitutional Democracy Against Terrorist and Related Activities Act 2004

05 —

Cybersecurity



Cybersecurity: **Relevant legislation**

- A National Cybersecurity Policy Framework (NCPF) was adopted by the Government in 2012, with the objective of providing a coherent approach to and strategies for coordination across government on cybersecurity.
- A CyberSecurity Hub was established under NCPF as a decision-making body responsible for identifying and combating cybersecurity threats.
- The Cybercrime Act was passed on May 27, 2021 as a single, overarching legal and regulatory framework governing cybersecurity, which was previously dealt with in various pieces of legislation. Provisions include:
    - Creation of cybercrime offences, including unlawful access, unlawful interception of data, unlawful acts respecting software/hardware, unlawful interference with data/computer program, cyber fraud, and cyber extortion.
    - Criminalization of the disclosure of harmful data messages.
    - Obligation of service providers and financial institutions to report cybercrime offences to the police within 72 hours, and to retain evidence connected to the offence.

Sources: National Cybersecurity Policy Framework, Cybercrime Act, Cybersecurity Hub Website

06 — Competition

Competition: **Relevant legislation & issues**

Relevant legislation:

- The Competition Act, 1998 established the Competition Commission (Chapter 4) which is responsible investigating anti-competitive activity, such as abuse of a dominant position (Chapter 2 Part B).

- The Act bars dominant firms from charging excessive prices and denying competitors access to an essential facility, where economically feasible (Section 8).

Competition issues in mobile financial services:

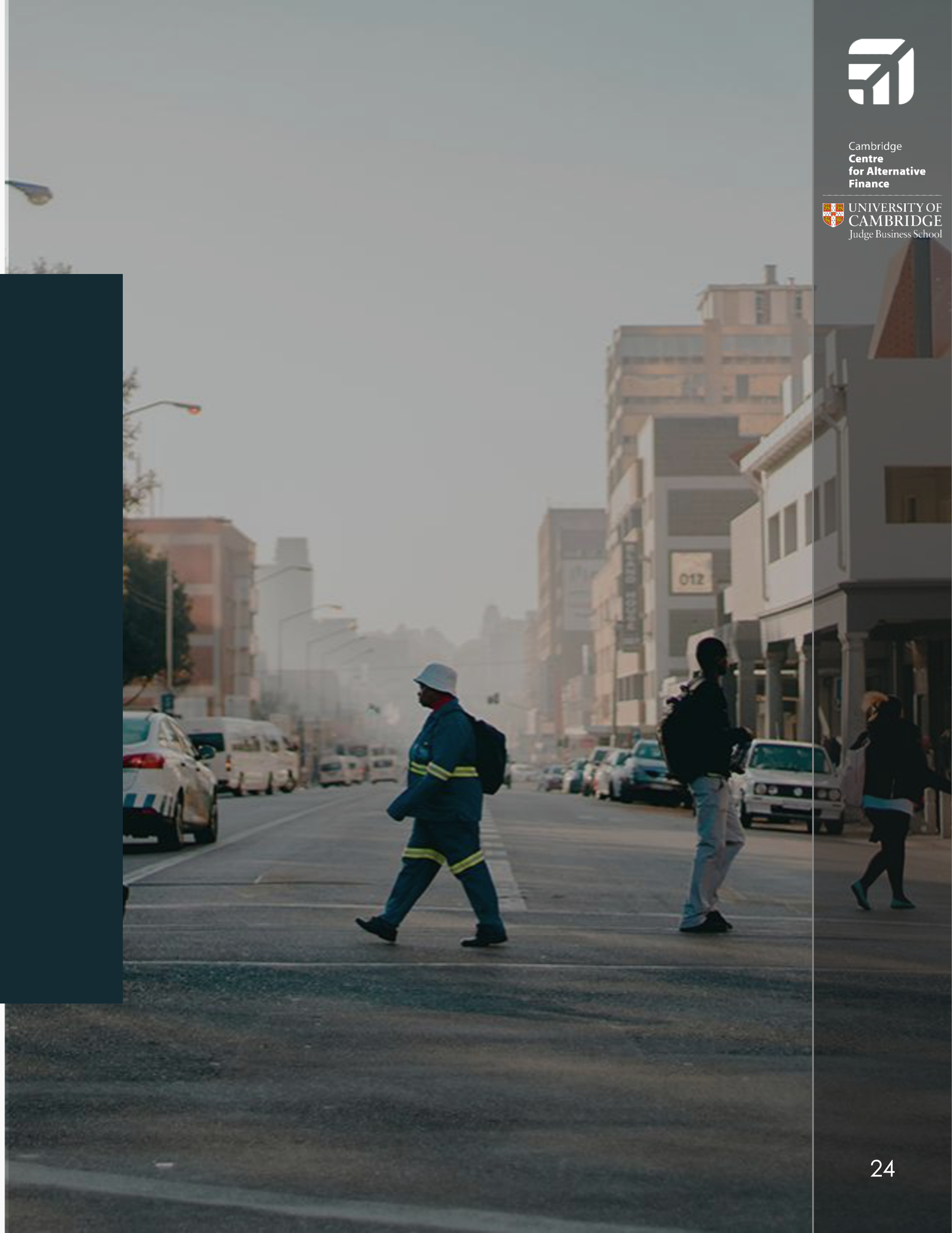
- Include issues with channel access, transparency, interoperability, regulatory coordination, and data sharing — these may also be present across other fintech sectors

- The Competition Commission has recently published a report on competition in the digital economy, which highlights specific competition issues that affect digital markets, including platforms and digital financial services.

Sources: The Competition Act, 1998, Report on Competition in the Digital Economy

07

Taxation of financial services



Taxation: **Financial services**

Relevant taxes:

- In June 2014, South Africa expanded the scope of its VAT rules by include cross-border digital financial services. The VAT rate is 15%. The provisions require registration for foreign suppliers which exceed the R50,000 ($3,434) limit.

Application to fintech:

- These taxes may impact fintech businesses involved in cross-border payments or other cross-border financial services. Fintech firms are encouraged to consult the South African Revenue Services regarding the implications of the VAT and other requirements that may be relevant for their business.

Sources: The Value-Added Tax Act 89 of 1991, South African Revenue Service Website

08

Other regulatory requirements

Other Regulatory Requirements: **Financial advisory/ intermediaries & company registration**

Advisory & intermediaries:

- Financial Advisory and Intermediary Services Act, 2002 (FAIS) relates to financial advisory and intermediary services, including debt rehabilitation.
- Financial services providers that provide any of the following services are regulated by FAIS: furnishing of advice; buying, selling, or otherwise dealing, managing, administering or servicing a financial product; collecting or accounting of premiums or other monies payable by a client to a product supplier; and the receiving, submitting, or processing of claims.

Company registration:

- The Companies Act, 2008 requires all businesses to register as an external company within 20 business days after they first begin conducting business within South Africa.

Sources: The Financial Advisory and Intermediary Services Act, 2002 , The Companies Act, 2008

For more information and further guidance on engaging with regulators see [Fintech Regulation in South Africa]

www.bfaglobal.com
info@bfaglobal.com
@bfaglobal