CATALYST FUND
Powered by BFAGLOBAL

Cambridge
Centre
for Alternative
Finance

UNIVERSITY OF
CAMBRIDGE
Judge Business School

Digital Savings
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. Banking
2. Data protection
3. Consumer protection
4. AML / KYC
5. Cybersecurity
6. Competition
7. Taxation
8. Other regulations

This deck provides **an overview of an overview of South Africa's regulation of digital savings, agent banking,** and **financial institutions**

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

Banking

Banking: **General overview & licensing**

Main regulator:

Per amendments to the Banks Act, 1990 by the Financial Sector Regulation Act, 2017 (FSR Act), the Prudential Authority (PA) has the responsibility for supervision of banks

Key regulation:

The Banks Act is a historical piece of legislation which provides for the regulation and supervision of deposit-taking institutions.

Scope:

The Banks Act defines a bank as a business that accepts monetary deposits from the general public as a regular feature of its business.

Licensing process:

Firms seeking to undertake banking must be registered under the Banks Act (Section 11). To register, firms are required to (i) apply to the PA for authorization to set up a bank and (ii) apply for registration (Chap. III of the Banks Act for detailed requirements).

Application requirements:

- Complete PA's authorization forms
- Provide copies of incorporation documents & details of the proposed business and how it will be conducted
- List names and addresses of key personnel and shareholders
- Pay application fees.

Capital requirements:

Revised capital requirements were introduced by SARB in 2013 to align with the Basel III framework. These are stipulated in the Banks Act and accompanying regulations. The roll-out of Basel III requirements is still underway. There has been some flexibility in implementing these requirements, and a phased approach has been adopted to allow for smooth transition by banks. A detailed timeline for compliance has been set out by the PA, running from October 1, 2020 to January 1, 2023.

Sources: Financial Sector Regulation Act 2017, The Banks Act, 1990, Guidance Note 6 issued in terms of Section 6(5) of the Banks Act

Banking: **Agent Banking & Digital Banks**

Agents:

- The Banks Act permits the use of agents by banks for certain activities.
- Permitted activities that an agent can undertake on behalf of a bank include:
  - receiving client deposits and other money payable,
  - collection of applications for loans or advances, and
  - making payments due to clients.

Digital Banks:

- Digital banks are described as "deposit-taking institutions that are members of a deposit insurance scheme and deliver banking services primarily through electronic channels instead of physical branches".
- In accordance with the 2009 e-money position paper issued by the SARB (the "E-Money Paper"), providers of digital wallets and e-money solutions may fall within the definition of deposit-taking and may be subject to the requirements of the Banks Act.
- The 2009 E-Money Paper states that only banks can issue e-money.
- Providers who consider themselves to be "digital banks" would therefore be required to have a banking licence and comply with obligations concerning capital and liquidity ratios and reserve requirements
- Fintech firms seeking to establish digital banks should refer to the application requirements in the previous slide applicable to banks.
- Additional provisions relating to e-money are considered in section 5.2 Payments.

Sources: The Banks Act, 1990, SARB Position Paper on E-Money, Regulating fintech financing: digital banks and fintech platforms

Banking: **Deposit insurance**

- There are no stipulated requirements for deposit insurance.
- However, the government has previously compensated consumers for losses in the event of a bank's collapse on a case-by-case basis.
- To address the current gap, the SARB and National Treasury are seeking to create a regulatory framework that will introduce a deposit insurance scheme (DIS). See section 6 on the regulatory pipeline for further details.

Sources: Press Release South African Government, Discussion paper: Establishment of the Corporation for Deposit Insurance: using the deposit insurance fund to reimburse covered depositors, Press Release SARB; MEDIA STATEMENT TABLING OF THE FINANCIAL SECTOR LAWS AMENDMENT BILL,2020

02

Data protection

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

REPUBLIC OF SOUTH AFRICA

Vol. 469 Cape Town 11 March 2008 No. 28919

THE PRESIDENCY

No. 230 11 March 2008

It is hereby notified that the President has assented to the following Act, which is hereby published for general information:—

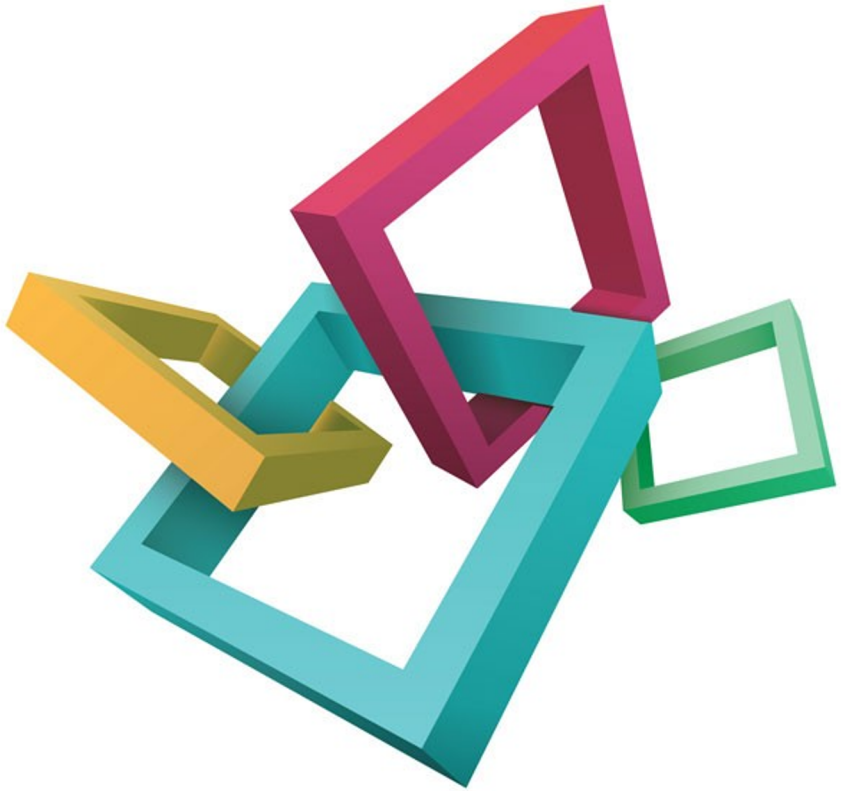
No. 34 of 2005: National Credit Act Aa, 2005

AIDS HELPLINE: 0800-123-22 Prevention is the cure

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,

Cambridge Centre for Alternative Finance

UNIVERSITY OF CAMBRIDGE Judge Business School

03

Consumer protection

Consumer protection: **National provisions**

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

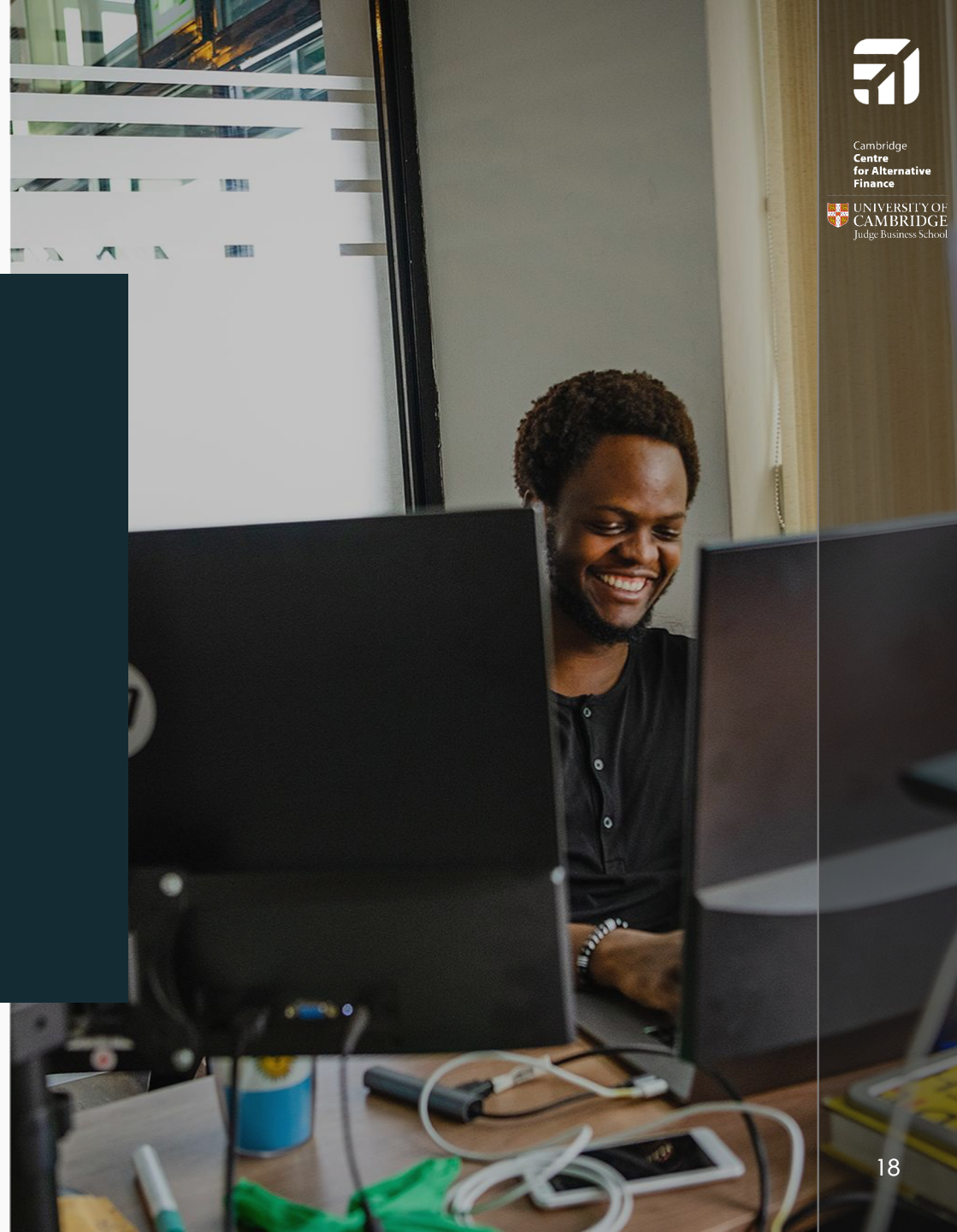
AML/KYC: **Other related requirements**

- **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**

Cambridge Centre for Alternative Finance
UNIVERSITY OF CAMBRIDGE Judge Business School

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).

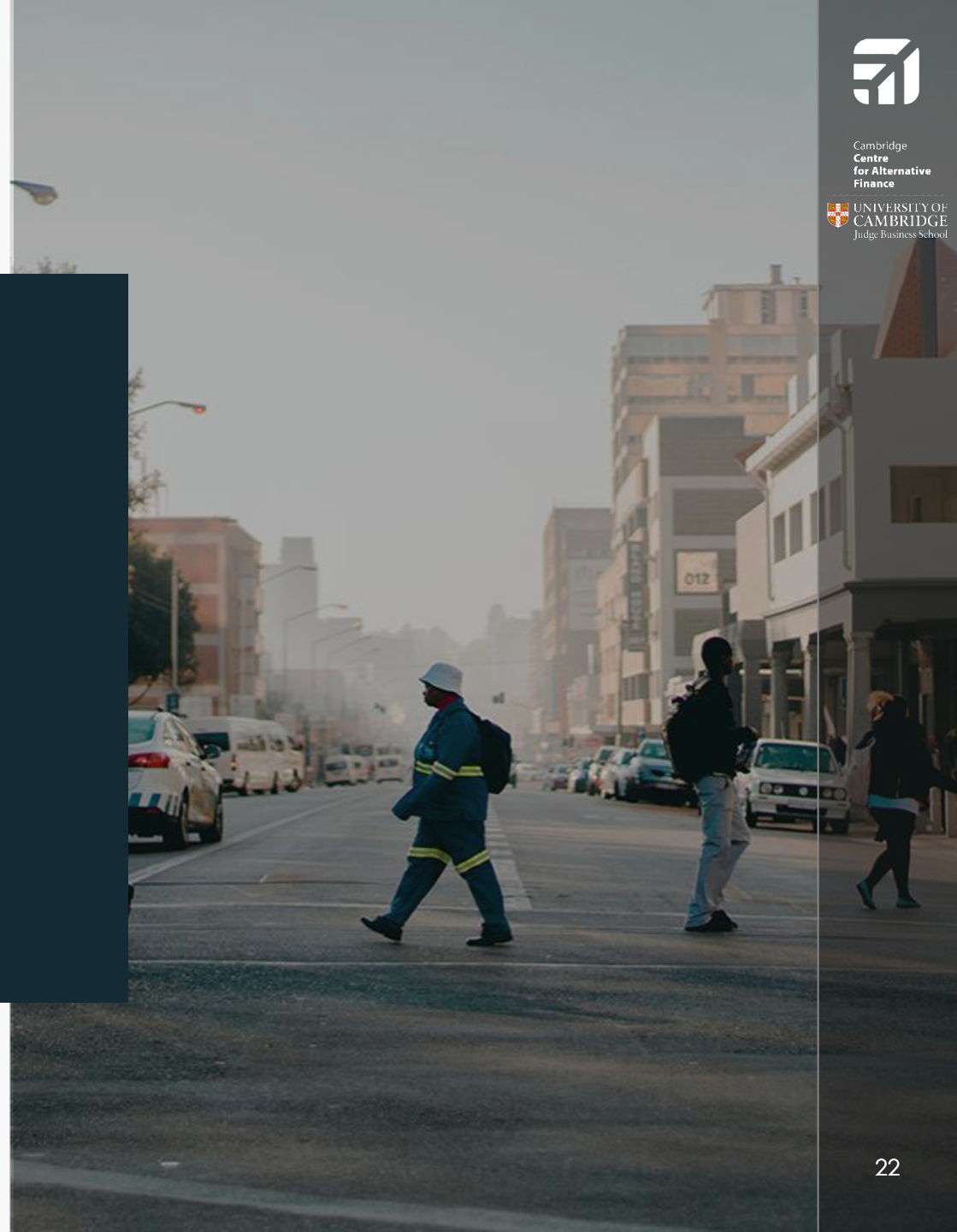
Competition issues in mobile financial services:

- 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