



Cambridge
**Centre
for Alternative
Finance**



UNIVERSITY OF
CAMBRIDGE
Judge Business School

Digital Payments & Remittances

(mobile wallets/e-money, payment initiation, mobile POS)

Kenya

www.bfaglobal.com | [@bfaglobal](https://twitter.com/bfaglobal) **UPDATED 31 JANUARY 2021**

Funded by





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 any of the said information.

How to use this deck

Relevant regulations

1. Payments
2. Data protection
3. Consumer protection
4. AML / KYC
5. Economic crimes
6. Cybersecurity
7. Competition
8. Telecom regulation
9. Taxation
10. Foreign exchange

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

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 Kenya and those seeking to enter the Kenyan fintech market navigate the regulatory environment.





01 Payments



Cambridge
Centre
for Alternative
Finance



UNIVERSITY OF
CAMBRIDGE
Judge Business School

Payments: General overview

Main regulator:

Central Bank of Kenya (CBK) has a mandate to oversee all payment systems and payment service providers (PSPs) with the aim of ensuring the safety and efficiency of the National Payment System.

Key regulation:

The National Payment System Act (NPSA 2011) and Regulations (NPSR 2014), which set out licensing requirements

Scope:

The services in scope include...

- sending, receiving, storing or processing payments, or provision of other services in relation to payment services through any electronic system;
- ownership, possession operation, management or control of a public switched network for the provision of payment services; or
- the processing or storage of data on behalf of such payment service providers or users of such payment services.

Payments: Acquiring a payments license

Who: Applies to all providers of services in scope set out in the slide “Payments: general overview”

How much: Different application requirements, depending on the license acquired. For electronic retail PSPs:

- Application fee: KES 5,000 (\$45)
- Authorization fee: KES 100,000 (\$910)

Capital requirements: Core capital is KES 5,000,000 (\$45,496) for electronic retail PSPs (depends on license acquired)

How: An application for authorization is required to be sent to the CBK, accompanied by:

- Registration documents, details of services to be provided
- A business plan, including an indicative budget for the first three years
- A description of governance and control structures, including any use of agents
- A current tax compliance certificate

If the applicant is a mobile PSP, application also requires certified copies of:

- Their license from the Communications Authority
- Their management agreement where a custodial trust relationship exists with the mobile payment service provider

If authorized, a firm is required to commence business within six months.

Payments: Licensing for small e-money issuers

Who: PSPs who are authorized to issue e-money (“EMIs”). The NPSR provides for a category of EMI called “small EMI” for those who issue e-money on a small scale, which have special application criteria.

How much - for small EMIs:

- Application fee: KES 5,000 (\$45)
- Authorization fee: KES 100,000 (\$910)

Capital requirements:

Core capital is KES 1,000,000 (\$9,098) for small EMI

Differences with other PSPs:

- Small EMI applicants may be exempted from complying with several provisions detailed under NPSR regulation 46(2)
- EMIs who do not fall into the definition of “Institutions”* are prohibited from engaging in lending or investment activities



*NPSA section 2 defines an “institution” as a bank, mortgage finance company or a financial institution as defined in the Banking Act (Cap. 488) or a microfinance bank business as defined in the Microfinance Act, 2006 (No. 19 of 2006) or any other body which the Minister may, in consultation with the Central Bank, declare, by notice in the Gazette, to be an institution for the purposes of this Act.”

Payments: PSPs and appointing agents

PSPs are permitted to appoint agents to act on their behalf through an agency agreement, however agents remain liable to their customers for the conduct of their agents (NPSR, Regulation 14).

Agent services in scope:

Sending, receiving, and processing payments

Requirements:

PSPs who appoint agents are required to maintain records pertaining to the agents (Section 19), exercise due diligence and undertake a suitability assessment (Section 20)

Exclusivity:

Agent exclusivity is not permitted



Payments: Safeguarding customer funds

Trust Fund:

- The NPSR (2014) requires PSPs to establish a trust and ensure all customer monies are held in a trust fund.
- These monies are required to be placed in multiple trust accounts with commercial banks or Government of Kenya securities.

Deposit Insurance:

- The Kenya Deposit Insurance Act (2012) provides that the deposits that are held in trust by a trustee for beneficiaries (e-money customers) are considered separate from a deposit by that trustee with the “Institution” on the customers’ own behalf, and separate from any deposit held in trust by another trustee for the beneficiaries in the Institution. Deposit insurers are permitted to insure these trust accounts.
- As with bank deposits, the e-customer deposit placed with an Institution are insured by KDIC, and the maximum amount payable to a customer is a protected deposit up to KES100,000 (\$910).

Small EMIs:

- Small EMI may be exempted from complying with provisions on setting up of a Trust. See the NPSR Regulation 46(2) for a list of the exempt clauses, including section 25 which stipulates the requirements regarding trusts for PSPs.

Sources: [The National Payment System Regulations \(2014\)](#), [Kenya Deposit Insurance Act \(2012\)](#)

Payments: **Becoming a money remittance operator**

— **Key regulation:**

Money Remittance Regulations (2013) provide for the licensing and regulation of a money remittance operator (MRO) to deal in inbound and outbound international money transfer transactions

— **Scope:**

- Companies who are permitted to provide inward & outbound international remittances
- "A money remittance business shall not engage in any other business other than as authorized by the Bank" - thus PSPs must set up a separate subsidiary
- Permitted and prohibited activities are set out in Part IV

— **How:**

- The regulations detail provisions relating to the establishment and licensing of MROs (Part II)
- To provide money remittance services, a firm must be incorporated as a limited liability company and obtain business name approval prior to incorporation*
- The firm must obtain an MRO license
- The guidelines prescribe license application fees (Regulation 5) and core capital (Regulation 10)
- Banks and MFIs are exempt from getting a MRO license
- MROs can provide services via an agent (Regulation 25)

*This name is required to include either the words "money-remittance" or "money transfer" as a brand (trading) name.

Sources: [Money Remittance Regulations \(2013\)](#)



Cambridge
Centre
for Alternative
Finance

UNIVERSITY OF
CAMBRIDGE
Judge Business School

Payments: Becoming a money remittance operator (cont.)



Obligations

- As part of the customer protection requirements, MROs are required to make specified written disclosures to customers including that they are not a deposit taking or lending institution, and that customers are not subject to deposit protection (Regulation 38).
- All Forex inflows and outflows must be done through bank accounts so no wallet to wallet remittances



Payments: Other requirements of PSPs

Customer disclosures:

PSPs are required to make the following specified disclosures to customers (as set out in NPSR Regulation 35):

- A clear description of services, prominently displayed at points of services (“POS” - the definition of POS encompasses head office and branches, agent outlets, and websites)
- Give prior notice to customers in the event of material changes to terms, conditions and charges
Display PSP’s name together with telephone number or other contact details at POS
- Information on how customers can access the PSP’s customer care system

Interoperability

- The NPSR (Regulation 21) requires PSPs to use systems that are capable of becoming interoperable with both national and international payment systems



02

Data protection



Data protection: National provisions



Key Laws: Constitution of Kenya & The Data Protection Act (2019) – modelled on the EU's GDPR

Main provisions:

- **Constitution of Kenya** guarantees the right to privacy for every citizen. This right includes the right not to have information relating to a person's private life unnecessarily revealed or required, or the privacy of one's communications infringed.
- **Data Protection Act** sets out restrictions on how personally identifiable data obtained by firms and government entities can be handled, stored and shared, as well as details of the role of the Data Commissioner. Data controllers and processors must be registered, but implementation details of the Act have yet to be released (as of Jan 2021). The first Data Commissioner was appointed and took office on 16 November 2020.

On cross border transfers:

- Part VI of the Data Protection Act stipulates provisions on cross border transfers and data localization requirements.
- Cross border transfers are contingent on data controllers and processors evidencing to the Data Commissioner that appropriate safeguards are in place to ensure the security and protection of personal data. Safeguards include providing proof that jurisdictions where data is to be transferred have commensurate data protection laws, and the transfer is necessary e.g., as part of a contractual performance.
- The Cabinet Secretary may specify that certain types of data processing can only be done through a server or data centre located in Kenya.

Data protection: Sectoral provisions

There are also data protection provisions in sector specific financial service regulation that apply to specific types of financial service providers

PSPs:

- National Payment System Regulations requires that PSPs, their agents, and cash merchants, keep customer data collected in connection with the services they provide confidential (Regulation 42).
- The CBK is empowered to suspend or revoke a PSPs license where it fails to protect confidentiality of the data that it collects.

Institutions:

- CBK's Prudential Guidelines on Consumer Protection requires "Institutions" to protect consumer's personal and financial information through the establishment of appropriate control and protection mechanisms. These mechanisms must define the purpose of data collection, processing, and disclosure to third parties, as well as customer rights, such as informed data sharing.

Telecom licensees:

- The Kenya Information and Communications (Consumer Protection) Regulations 2010 provides for a customer's right to personal privacy and protection against unauthorized use of personal information (Regulation 3(1)(d)).
- Licensees are required to keep subscriber information confidential and are prohibited from monitoring/disclosing this information or allowing others to do so (Regulation 15).

Central depositories:

- The Central Depositories Act (2000) prescribes secrecy obligations (Part VI).

Sources: [National Payment System Regulations 2014](#), [CBK's Prudential Guidelines on Consumer Protection](#), [The Kenya Information and Communications \(Consumer Protection\) Regulations 2010](#), [The Central Depositories Act \(2000\)](#).

Data sharing: Open banking

- There are currently no prescribed requirements for open banking.
- The recent released draft of “Kenya National Payments System Vision and Strategy, 2021 – 2025” contains some provisions on open API frameworks, and suggests that CBK may mandate data portability in financial services as well as facilitate the development of an industry wide standard for open APIs (sections 5.4.3 and 5.5.1). However, this draft is up for public consultation and the final version may be substantially different.
- Firms interested in introducing initiatives in this area should check with their regulator.





03 Consumer protection



Cambridge
Centre
for Alternative
Finance



Consumer protection: National provisions

Key Laws: Constitution of Kenya, Consumer Protection Act (2012), The Access to Information Act (2016)

Main provisions:

- Article 46 of the **Constitution of Kenya** specifies consumers right to:
 - Goods and services of reasonable quality
 - The information necessary for them to gain full benefit from such goods and services
 - Compensation in case of loss or injury emerging from defects with goods or services
- The **Consumer Protection Act** contains further obligations on providers, including:
 - Confidentiality
 - Provisions relating to the performance of credit agreements* and agreements executed over the Internet
 - Disclosures to be made for remote agreements
- The **Access to Information Act** (2016) was enacted to implement Article 35 of the Constitution. It provides that every citizen has the right to access information held by public entities and private bodies (Section 3 and 4, and Part II more generally). Fintechs will need to ensure they provide information requested pursuant to the Act.

* Not all credit agreements are covered by the Consumer Protection Act. Part VII of CP Act applies only to supplier credit arrangements where a supplier extends fixed credit to a consumer to assist the consumer in obtaining goods or services, other than credit or a loan of money from the supplier.

Consumer protection: Sectoral provisions

There are consumer protection provisions in sectoral regulation that apply to specific financial service providers:

PSPs:

- National Payment System Act & Regulations include consumer protection provisions, such as on misleading advertisements (Sec. 29 NPS Act)

Institutions:

- CBK's Prudential Guidelines on Consumer Protection
- Banking Act contains consumer protection provisions, including a restriction on the imposition of charges on savings, seven day call, or fixed deposit accounts (Section 16A), and limits on interest recoverable in the event of customer default (Sec. 44A)

Telecom licensees:

- The Kenya Information and Communications (Consumer Protection) Regulations 2010 include consumer protection provisions, i.e., customers have the right to receive clear and complete information about rates, terms, and conditions for products and services from telecom providers (Reg 3)

Insurers:

- The Insurance Act contains consumer protection provisions i.e., a dispute resolution for consumers (Sec. 204A) and establishes a fund to compensate policyholders for insurance firm collapse (Sec 179)

Capital Markets Authority (CMA) licensees:

- The Capital Markets Authority Act stipulates the protection of investor interests (Sec 11) and establishes a fund to compensate investors where a CMA licensee fails (Sec 18)

Sources: [National Payment Systems Act 2011](#), [National Payment System Regulations 2014](#), [CBK's Prudential Guidelines on Consumer Protection](#), [The Kenya Information and Communications \(Consumer Protection\) Regulations 2010](#), [the Banking Act](#), [The Insurance Act, 1987 \(as amended\)](#), [The Capital Markets Authority Act](#)



04

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

AML/KYC: Key laws & main provisions



Key Laws: The Proceeds of Crime and Anti Money Laundering Act (2009, as amended) (POCAMLA), Proceeds of Crime and Anti Money Laundering Regulations (2013), Prevention of Terrorism Act (2012), & The National Payments Systems Regulations (2014)

Main provisions:

- The **Terrorism Act** stipulates that entities must monitor products and services for possible use in aiding and supporting terrorist activities
- The **POCAMLA** and **related Regulations:**
 - Categorize financial Institutions as reporting Institutions, who are obligated to put measures in place to combat money laundering and register with the Financial Reporting Centre (FRC)
 - Impose AML obligations such as monitoring and reporting to the FRC (Section 44), verification of customer identity (Section 45), maintaining customer records (Section 46), and the maintenance of internal reporting procedures (Section 47)
- The **National Payments Systems Regulations** provides for AML measures for PSPs and their agents, including cash merchants, who are also required to comply with the Proceeds of Crime and Anti-Money Laundering Act (2009) and the Prevention of Terrorism Act (2012)
- The CMA has also issued **Guidelines on the Prevention of Money Laundering and Terrorism Financing in the Capital Markets**

Sources: [The Proceeds of Crime and Anti Money Laundering Act \(2009, as amended\)](#), [Proceeds of Crime and Anti Money Laundering Regulations, 2013](#), [Prevention of Terrorism Act, 2012](#), [National Payment System Regulations 2014](#), [Guidelines on the Prevention of Money Laundering and Terrorism Financing in the Capital Markets](#)

AML/KYC: Customer due diligence requirements

- Customer Due Diligence (CDD) requirements for institutions licensed under the Banking Act are contained in the **CBK Prudential Guidelines on AML/CFT** (Part V).
- The Guidelines prescribe Know Your Customer (KYC) requirements, processes for customer identification and verification, situations that call for enhanced due diligence and applicable measures, transactions monitoring and reporting, and record keeping.
- **At a minimum the mandatory KYC requirements for an individual are:**
 - A birth certificate
 - Passport
 - National identity card
 - Drivers license
- Additional due diligence measures that may be used to verify the identity of the customer include: a) Address of current residence verified by a referee, a utility bill; b) Verified employment and/or source(s) of income; and c) Where applicable, written confirmation from customer's prior bank attesting to customer's identity and history of account relationship (bank referee).
- The **POCAMLA and Regulations** do not provide for simplified CDD nor overtly provide a tiered approach to KYC. However, given that firms such as mobile money providers are permitted to incorporate additional KYC information incrementally, a risk-based approach may be inferred.
- A number of providers employ remote (i.e., non face-to-face) CDD by mobile phone like M-Shwari




05

Other economic crimes

Other economic crimes: Relevant legislation

- The Anti-Corruption and Economic Crimes Act (2003, as amended) provides for the prevention, investigation, and punishment of corruption, economic crime, and related offences. See particularly Part IV on investigation, and Part V on offences and penalties.
- The Bribery Act (2016) stipulates provisions relating to prevention, investigation, and penalties for bribery. The applicability of the Act includes both public and private entities and is therefore relevant to fintech providers and are obliged to take steps to prevent bribery by establishing procedures proportionate to their size, scale, and operations (Section 9).




The Anti-Corruption Division

In order to effectively and efficiently execute its mandate, the ODPP is divided into thematic divisions so as to be responsive to emerging and complex crimes.

The Anti-Corruption is one such division that was established in realization of its complex nature and notoriety. Its establishment was also in recognition of the public interest in the fight against corruption.



■ LIKE ■ FOLLOW ■ SUBSCRIBE:

 ODPPKenya  ODPP_KE  Office of the Director of Public Prosecutions Kenya

Sources: [Anti-corruption and Economic Crimes Act \(2003, as amended\)](#), [Bribery Act \(2016\)](#),



06

Cybersecurity



Cambridge
Centre
for Alternative
Finance



UNIVERSITY OF
CAMBRIDGE
Judge Business School

Cybersecurity: Relevant legislation

National legislation:

- The Computer Misuse and Cybercrimes Act (2018) stipulates several key objectives including protecting the confidentiality, integrity, and availability of computer systems, programs, and data (Section 3(c)), and facilitating the prevention, detection, investigation, prosecution, and punishment of cybercrimes (Section 3(e)).
- The Act also prescribes several offences, and penalties for non-compliance under Part III. Examples of offences include unauthorized access, interference, disclosure of passwords and access codes, and interception of electronic messages or money transfers. Firms are obliged to put in place adequate cybersecurity measures to ensure adherence.

Banking sector:

- CBK's note on Cybersecurity for Banking Sector sets out minimum standards with respect to cybersecurity risks for the banking sector.

PSPs:

- Pursuant to the National Payments Systems Act, the CBK has issued guidelines on cybersecurity for PSPs. These detail the minimum requirements to be adopted in the development of effective frameworks for cybersecurity governance and risk management.
- All PSPs are required to review their cybersecurity strategy, policy, and framework annually based on a threat and vulnerability assessment (Part IV).



07 Competition



Cambridge
Centre
for Alternative
Finance



Competition: Relevant legislation & competition issues



Relevant legislation:

- The Competition Act (2010) established the Competition Authority of Kenya (CAK), which is mandated to provide oversight over market conduct aspects such as price transparency and consumer recourse
- The Competition Act prohibits restrictive practices and “unconscionable business conduct”
- The Communications Authority of Kenya (CA) also has a mandate to ensure “fair competition and equal treatment” and this jurisdiction applies to payment providers who use communication channels to deploy products and services
- The Competition Act prevails in areas of concurrent jurisdiction, and there is a non-statutory MoU between CBK and Competition Authority

Competition issues in mobile financial services:

- These include issues with channel access, transparency, interoperability, regulatory coordination, and data sharing — these may also be present across other fintech sectors
- Several regulatory interventions have been introduced to address competition issues, including a ban on agent exclusivity, and requirements for disclosure of mobile money transaction costs at point of usage

Sources: [The Competition Act \(2010\)](#), [CGAP Competition in Mobile Financial Services Lessons from Kenya and Tanzania](#), [National Payment System Regulations 2014](#), [Kenya Ends Hidden Costs for Digital Financial Services](#), [The Kenya Information and Communications Act, 1998](#), [The Kenya Information And Communications \(Fair Competition And Equality Of Treatment\) Regulations, 2010](#)



08

Telecommunications regulation



Telecommunication regulation: Licensing



Key regulations:

- The Kenya Information and Communications Act (KICA, 1998, as amended) empowers the Communications Authority of Kenya (CA) to license and regulate information and communications services (Section 5)
- The KICA Regulations (2001) also apply
- The Competition Authority has a Unified Licensing Framework (ULF), which is technology and service neutral

Main provisions:

- The Act regulates respective sub-sectors, including telecommunications (Part III), radio communication (Part IV), and broadcasting services (Part IVA)
- The ULF provides the licensing procedures for Network Facilities Providers, Application Service Providers, and Content Service Providers

Application to fintech:

- The Competition Authority may license a fintech where its operating model incorporates a technological aspect and the implementation of the innovation requires the fintech business to establish its own telecommunications infrastructure or results in content generation
- In such a cases, the Competition Authority will issue (i) an approval or license, (ii) a letter of no objection, or (iii) confirmation that a firm does not require a telecommunications license



09

Taxation of financial services



Cambridge
Centre
for Alternative
Finance



UNIVERSITY OF
CAMBRIDGE
Judge Business School

Taxation: Financial services



Relevant taxes:

- In 2013, taxes on financial transactions, mobile and computer hardware, and software were introduced in Kenya as well as the wider East Africa region
- For example, the VAT Act of 2013 imposes 16% VAT tax on phone sales
- The Finance Act of 2018 increased excise duties to 15% on airtime, 20% for money transfer by banks /MTOs/ other financial institutions, and to 12% on mobile phone based financial transactions
- The Finance Act of 2018 also introduced a 15% tax on internet data services and fixed-line telephone services, while removing a 2009 exemption on mobile phones

Application to fintech:

- These taxes may impact fintech businesses, and fintechs are encouraged to consult the Kenya Revenue Authority regarding the implications of the measures cited, as well as other requirements that may be relevant for their business model



Cambridge
Centre
for Alternative
Finance

UNIVERSITY OF
CAMBRIDGE
Judge Business School

SOKOWATCH



10

Foreign exchange



Forex: Key regulations & main provisions

Key regulations:

- Part VI A of the Central Bank of Kenya Act
- Foreign Exchange Guidelines issued by CBK

Main provisions:

- All foreign exchange transactions must be carried out through authorized forex dealers
- Dealers are required to obtain and retain appropriate documents for all transactions above the equivalent of US\$ 10,000 — these transactions are required to be reported to the CBK



For more information and further guidance on engaging with regulators see [Fintech Regulation in Kenya](#)

www.bfaglobal.com

info@bfaglobal.com

[@bfaglobal](https://twitter.com/bfaglobal)



Cambridge
**Centre
for Alternative
Finance**



**UNIVERSITY OF
CAMBRIDGE**
Judge Business School