INTERPOL

enact
Enhancing Africa's response to transnational organised crime

Mobile money and organized crime in Africa

June 2020

This project is funded by the European Union

This analytical report was compiled in the framework of the European Union (EU) funded Project ENACT (Enhancing Africa's response to transnational organized crime). The contents of this INTERPOL report can in no way be taken to reflect the views of the EU or the ENACT partnership.

ENACT is implemented by the Institute for Security Studies and INTERPOL,
in association with the Global Initiative Against Transnational Organized Crime

Table of Contents

List of acronyms....4

Executive summary....5

Introduction....6

1. Structure of the report....7

1.1. Scope & objectives....7

1.2. Methodology....7

2. What is mobile money and how does it work?....8

2.1. Concept definition and key players....8

2.1.1. Definition....8

2.1.2. Key players involved in the mobile money ecosystem....9

2.2. How does mobile money work?....10

2.2.1. Mobile money transaction types and transaction flows....11

2.2.2. Mobile money access channels....14

2.2.3. Mobile money consumer protection....15

3. Landscape of mobile money services in Africa....16

3.1. Mobile money deployment and adoption....16

3.1.1. Operators....17

3.1.2. Users....17

3.1.3. Value of mobile money transactions....18

3.1.4. Future developments....19

3.2. Regulations governing mobile money systems in Africa....20

3.2.1. Regulating mobile money in Africa?....21

3.2.2. Mobile money regulatory frameworks in Africa....22

3.2.3. Analysis of regulatory frameworks....22

4. Mobile money and crime....31

4.1. Vulnerabilities and impact....31

4.2. Key vulnerabilities....31

4.3. Illicit goods trafficking and mobile money....34

4.4. Other illicit commodities....37

4.5. Corruption....38

4.6. Money laundering....38

4.7. Trafficking in human beings and people smuggling....39

4.8. Extortion....40
4.9. Enabling factor....40
5. Mobile money and terrorism....41
6. Law enforcement capacity to investigate and fight mobile money abuses....42
Conclusion....43
APPENDIX 1 - Analysis of mobile money transactions and balance limits regulations per region....44
APPENDIX 2 - Financial action task force on money laundering country consolidated assessment ratings published in February 2020:....46
References....47

List of Acronyms

BEAC	Banque des Etats d'Afrique Centrale
CAPCCO	Central African Police Chiefs Coordination Organization
DRSP	Digital Remittance Service Providers
EAPCCO	East African Police Chiefs Coordination Organization
GSM	Global System for Mobile Communications
GSMA	GSM Association
MENA	Middle East and North Africa
MMO	Mobile Money Operator
MMS	Mobile Money Services
MNO	Mobile Network Operator
MTO	Money Transfer Operator
SARPCCO	Southern African Regional Police Chiefs Coordination Organization
WAPCCO	Western African Police Chiefs Coordination Organization
Existing access channels	IVR: Interactive Voice Response is a technology that allows a computer to interact with humans through the use of voice and Dual-tone multi-frequency (DTMF) signalling input via a keypad. In telecommunications, IVR allows customers to interact with a company's host system via a telephone keypad or by speech recognition, after which services can be inquired about through the IVR dialogue. IVR systems can respond with pre-recorded or dynamically generated audio to further direct users on how to proceed. SMS: Short Message Service is a text messaging service component of most telephone, Internet, and mobile device systems. It uses standardized communication protocols to enable mobile devices to exchange short text messages USSD: Unstructured Supplementary Service Data, sometimes referred to as "Quick Codes" or "Feature codes", is a communications protocol used by GSM cellular telephones to communicate with the mobile network operator's computers. WAP: Wireless Application Protocol is a technical standard for accessing information over a mobile wireless network. STK: SIM Tool Kit is a standard of the GSM system which enables the subscriber identity module (SIM card) to initiate actions which can be used for various value-added services.
Know Your Customer (KYC)	Regulatory requirements for financial industry to establish credentials of customers and identify legitimate business activity in order to highlight suspicious activity regarding money laundering.

Executive summary

The development of mobile money services in Africa offer criminals a substantial opportunity to utilize these services to target victims in a variety of crimes as well as to further enable other forms of criminality. This rapid service development combined with criminal opportunities represents a security issue of interest to all member countries in Africa and poses a significant challenge to law enforcement agencies in member countries. As a result, INTERPOL, under the European Union funded ENACT Project, has assessed this issue in order to help drive a more strategic law enforcement response.

Criminals and criminal organizations will most probably continue to utilize mobile money services following the recent increase in their popularity and the prominent role such services now play in society across Africa. This prominent role in society has enabled criminals to exploit weaknesses in regulations and identification systems, further enabled by a lack of experience and resources in law enforcement.

Crime types have been identified that exploit mobile money services across Africa. These primarily include various types of fraud that target the distinct stages of deployment for mobile money services. Whilst acquisitive crimes significantly impact the lives of victims, criminals have also identified further opportunities to exploit mobile money services to assist other criminal activities. These 'mobile money enabled crimes' include illicit commodities purchases, terrorism financing and firearm enabled crime. Such significant crimes pose a threat to stability and security across Africa if not addressed by member countries.

The threat from criminality facilitated by mobile money services in Africa is substantial, yet there is sometimes limited capacity amongst law enforcement to manage this complex issue, especially concerning the technical expertise required to utilise relevant evidence in the criminal justice system. As mobile money services develop interoperability across Africa, stronger partnerships amongst all law enforcement agencies, greater awareness of the overall issue at a regional level and identification of best practice responses from such agencies will be required. INTERPOL is in a position to support member countries through coordinated, intelligence led support to law enforcement using a range of police databases and operational support techniques.

The following are the key findings found through an analysis of a range of data sources available on mobile money in Africa:

- Peer-to-peer (P2P) transfers are the most common use of mobile payment services. They accounted for 91.4 per cent of the 21 billion total mobile payment transactions processed in 2019. As a result, this form of transaction represents the most significant vulnerability for exploitation in the form of fraud.
- Cross-border mobile money remittances are the fastest growing segment of the peer-to-peer transfer mobile money market in Africa, where 120 million people received international remittances worth USD 60 billion in 2015. This tendency shows no sign of slowing down with the total value of P2P transfers having more than doubled between 2017 and 2019. This has resulted in transnational criminal syndicates exploiting mobile money services to enable low risk money laundering and purchases of illicit commodities with an international dimension, whilst benefitting from the anonymity offered by poorly applied regulatory standards.

- Eastern Africa is by far the leading region in Africa in terms of value of transactions, of which it represented close to 70 per cent in 2018. The share of Western Africa in terms of the total value of transactions is in strong progression since 2013. Mobile money will continue expanding across Africa. There is still significant growth potential for mobile money services in countries such as Nigeria, Ethiopia and Egypt which so far have low rates of financial inclusion and limited availability of mobile money services. The rapidly expanding nature of the industry has provided organised crime the opportunity to capitalize on the lack of regulatory adherence in the industry. This has particularly provided opportunities for illicit finances to be laundered in Africa by African and global criminal syndicates.
- Mobile money crime facilitating factors include: the weakness of individual identification systems; the lack of consumer awareness, the lack of resources and training of law enforcement concerning the collection and use of technical evidence in the criminal justice system. These factors have resulted in difficulties in prosecuting offenders and tackling established organized crime groups.
- There are strong indications that mobile money enabled criminality represents a significant threat to society in Africa. Such threats include: terrorist financing, illicit goods purchases, money laundering and extortion payments all of which offer criminal incentive to participate in or associate to violent activities that serve to destabilize public order and citizen safety. In addition to this, mobile money service exploitation by criminals benefits from poorly applied regulations and expertise in the criminal justice system. If this is not addressed, there is a significant risk of further criminal proliferation due to perceived risks versus rewards.
- The criminal exploitation of mobile money services is evident in a range of crime types that include; fraud, money laundering, extortion, human trafficking and people smuggling, the illegal wildlife trade, firearms availability, the drugs trade, stolen motor vehicle trade and terrorism.

Introduction

Mobile money was introduced in Africa in 2007 with the launch of the M-PESA (M for mobile, PESA for money in Swahili) service by Safaricom and Vodafone. M-PESA was started as a public/private sector initiative after the United Kingdom (UK) based telephone company Vodafone won funds from the Financial Deepening Challenge Fund competition established by the UK Government's Department for International Development to encourage private sector companies to engage in innovative projects so as to deepen the provision of financial services in emerging economies.

Originally, M-PESA was designed as a system to allow microfinance-loan repayments to be made by phone, reducing the costs associated with handling cash. After the pilot testing, it was broadened to become a general money-transfer scheme. The service then quickly gained popularity, initially with urban populations as a mean of sending money to family members in remote and underserved rural areas. Once the ability to buy airtime using M-PESA was introduced, the transaction volume increased rapidly as well as the adoption of the service by all population demographics.

Today, mobile money has grown in popularity across the whole African continent where some 153 mobile money services were active by the end of 2018 in 45 African countries. In sub-Saharan Africa alone more than 350 million

mobile money accounts were registered in December 2018 and the value of transactions exchanged through these accounts exceeded USD 301 billion.

The sheer volume and value of mobile money transactions raises questions about abuses of this payment system by criminal and terrorist elements. Indeed, every payment system has some vulnerability that could facilitate fraud, money laundering and terrorism financing.

Open source information indicates that such abuses exist. Therefore, the EU funded ENACT Project has undertaken this assessment on mobile money in Africa to inform law enforcement at a strategic level.

This report is divided into four main parts. The first part sets the boundaries of the report by presenting its scope and objectives as well as the methodology employed. The second part aims at explaining what mobile money is and how it works. The third part presents the landscape of mobile money in Africa with the objective to enable grasping the magnitude of the implantation of this new financial tool on the continent. This section will also examine the regulations governing mobile money and assess some of these regulations bearing in mind the law enforcement perspective. The fourth part of the report is dedicated to mobile money and crime. It will examine the main mobile money abuse typologies and report on the principal abuses associated to mobile money noted by African member countries. This section will also examine the difficulties encountered by law enforcement on the continent in investigating mobile money crime as well as identified intelligence gaps.

**** Two versions of this report exist. This report is the public version of the completed analysis, which included police information; where specific police information was used, this information has subsequently been sanitized for public distribution ****

1. Structure of the report

1.1. Scope & objectives

The primary objective of this report is to consider the situation regarding mobile money in Africa as a whole, accurate to the level of available data.

This assessment will draw upon data from available open sources and present, on the one hand, conclusions about the current level of adoption of mobile money by the African population and, on the other hand, provide an assessment of its abuses by criminal and terrorist elements. This is done so that stakeholders become aware of the criminality that surrounds this particular financial instrument and how the criminality pertaining to mobile money fits into a regional and possibly global context.

1.2. Methodology

This assessment follows an all source intelligence analysis methodology. It is the result of integrating multiple data sources.

Open sources used in the framework of this report include news articles and reports from various international organizations and think tanks.

Information from the aforementioned sources was all aggregated together in order to identify consistencies across all data, patterns and trends, and any identifiable convergences.

A regional approach was retained when drafting this report. Therefore, when national examples are quoted, it is done for illustrative purposes, in order to put forward regional dynamics.

INTERPOL African regions are defined on the basis of countries' participation in regional chiefs of police organizations. Some countries participate in more than one regional chiefs of police organization. In such cases, they are counted in each of the regional organizations in which they participate. North African countries are member of the INTERPOL Middle East and

North Africa (MENA) region. For the purpose of this report which only covers the African continent, they were regrouped in a category named North Africa. This category includes the following countries: Algeria, Egypt, Libya, Morocco and Tunisia. The other INTERPOL African regions and their member countries are grouped as follows:

CAPCCO: Cameroon, Central African Republic, Chad, Democratic Republic of Congo, Equatorial Guinea, Gabon, Republic of Congo, Sao Tome and Principe.

EAPCCO: Burundi, Comoros, Djibouti, Democratic Republic of Congo, Eritrea, Ethiopia, Kenya, Rwanda, Seychelles, Somalia, South Sudan, Sudan, Tanzania, Uganda.

SARPCCO: Angola, Botswana, Democratic Republic of Congo, Eswatini, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Tanzania, Zambia, Zimbabwe.

WAPCCO: Benin, Burkina Faso, Cape Verde, Ivory Coast, Gambia, Ghana, Guinea Bissau, Liberia, Mali, Mauritania, Niger, Nigeria, Senegal, Sierra Leone, Togo and Guinea.

2. What is mobile money and how does it work?

2.1. Concept definition and key players

2.1.1. Definition

Mobile money is defined as a digital financial service in which an individual uses a mobile phone handset to access a financial service or initiate a financial transaction. Mobile Money Services (MMS) may hence include, consulting balance, storing, transferring money and making payments using the mobile phone.

The perimeter of what is considered mobile money may vary depending on institutions. In its 2017 Financial Inclusion Index, the World Bank's definition of a mobile money account is limited to services that can be used without an account at a financial institution. People using a mobile money account linked to their financial institution are considered to have an account at a financial institution, hence resorting to mobile banking.[1] Conversely, the Global System for Mobile Communications Association (GSMA) representing the interests of mobile network operators worldwide, considers that mobile banking is a subsection of mobile money as it is mobile payment offered by nonbank actors such as Mobile Network Operators (MNO). Therefore, the term mobile money merely refers to using the mobile phone to access financial services, notwithstanding any specific deployment model, or any particular transaction type.[2]

These differences in the understanding of the scope of mobile money may result from the fact that, depending on national regulations, mobile money can be offered by different operators such as banks (or other financial institutions) in a bank based model or new market entrants, typically MNO in a MNO based model, or third parties. When mobile money services are offered by non-bank actors such as MNOs, they have, since they cannot issue electronic money themselves, to partner with a bank. Alternatively, they can obtain an electronic money issuer license from relevant national regulators.

Each model presents strengths and weaknesses. One of the advantages of the MNO led model is for instance the proven ability of MNOs to develop and manage extensive agent networks including in remote and poorly served areas. MNO also benefit from a larger customer base and robust brand developed through service provision and strong marketing. The bank-led model on the other hand presents more guaranties for financial regulators, given their adherence to financial discipline, proven processes, attention to security, etc.

Another model also exists in the form of associating a government provider, banks and cell phone companies. In this model the cell phone company, if involved, provides communications services while a government sponsored interbank clearing system operates the payment switch between banks and between accounts within banks.[3]

Currently, most mobile money services increasingly associate bank and nonbank operators. In such a scheme, MNOs conduct cash in/out payments through their agent networks but they are also linked to regulated financial institutions such as banks, insurance companies or remittances companies etc. in order to offer additional added value services to their customers, such as transnational remittances, saving plans, insurances, microcredit etc. Bank based mobile money providers on the other hand may use, through partnerships, MNOs technical infrastructures (for example Unstructured Supplementary Service Data [USSD] channels) as its carrier and propose mobile phone services in order to attract a new category of customers, unbanked up to that time.

In Africa, the deployment of mobile money was driven initially by MNOs who, on the model of the M-PESA service launched in 2007 in Kenya, saw in mobile money services an opportunity to capitalize on their mobile phone networks and subscribers' base in order to diversify and increase their revenue. Furthermore, national authorities saw in mobile money services offered by MNOs an opportunity to increase the financial inclusion of large sections of society, previously deprived from access to financial services. Today, bank-led, MNO-led and hybrid models are functioning across the continent.

2.1.2. Key players involved in the mobile money ecosystem

There are various models of mobile money service delivery. However, a typical mobile money platform always involves several stakeholders who play different roles and derive various benefits from the whole mobile money ecosystem, as presented in Table 1 below.

Actor	Role(s)	Incentive(s)
Mobile money user	They use the mobile money services fitting their needs	Users derive benefits by getting cheaper and more efficient means of transferring or paying money to other people or businesses.
Mobile Network Operator (MNO)	In a MNO based mobile money model, MNOs provide mobile money services in partnership with banks or through obtaining e-money issuer licences. They use their existing mobile phone service customer base and communication infrastructure as a competitive advantage. In a bank led mobile money model, MNOs provide the mobile infrastructure and communication services. A MNO ensures compliance with telecommunication regulations and policy within the country.	MNOs benefit from mobile money by increasing and retaining the number of customers, reducing the cost of airtime distribution and by generating new revenue.

Bank/financial institution with banking license and infrastructure	In a MNO based mobile money model they may act as segregated/trust accounts for MNOs. They enable the exchange of money between different parties. In a bank led model, they deliver mobile money services in partnership with MNOs of which they use the technical infrastructure. They also provide oversight and ensure compliance with national financial regulations and policy.	Banks or other financial institution can leverage mobile money platforms to reach new customers in traditionally underserved areas at much lower cost.
Regulatory institutions across different sectors	Key regulators usually include Central banks for the financial sector and telecommunication regulators for the communications sector. They set up the regulatory framework under which mobile money service providers operate.	Driven by the need for national development, regulators would like to see more people served by formal financial and communication services.
Agents	They familiarize customers with products and services, guide and support them in their transactions. They may also enrol new customers. They facilitate cash-in (converting cash into mobile money) and cash-out (issuing cash on demand) hence ensure convertibility between mobile money and cash. The agent activity can be a full time endeavour or a side activity carried out in addition to their main enterprise. An agent may serve several mobile money service providers. MNOs have developed extensive agent networks to sell airtime and other products while those of the banks tend to be limited to urban or highly populated areas.	Agents earn commission on various transactions carried out by mobile money users.
Third parties: Merchandise and service providers	They accept mobile money payments in exchange for different products and services or use mobile money as a means of delivering their services, i.e. merchants, retailers, microfinance institutions, insurance providers, large-scale disbursers and bill issuers.	Mobile money minimizes the need to handle cash and represents an opportunity to develop and deliver new products to previously untapped customers.
Equipment manufacturers and platform providers	These include a wide array of stakeholders like, network equipment providers, mobile phone makers as well as application suppliers.	They benefit from the increased sale of end-user devices like mobile phones, equipment to handle increased network capacity and fees or subscriptions respectively.

Table 1: Key players involved in the Mobile money ecosystem[4]

2.2. How does mobile money work?

Before using mobile money services, each customer has to complete two processes. Registration to comply with Know Your Customer (KYC) requirements from financial regulators and account activation. The registration procedure varies between operators and countries. The speed of activation likewise, from immediate to more or less delayed,

depends on procedures put in place by the operators in accordance with national regulations.

To fund their mobile money account, a customer goes to a mobile money operator's point of sale or typically an agent, where they deposit cash to buy e-money to be credited to their mobile money account. The operation is instantaneous, and the user receives a notification confirming the success of the operation and an indication of the new balance. This process is called "cashing-in".

Withdrawal of cash money or "cashing-out" is just as simple. The customer goes to a MMOs point of sale or agent, who gives the customer cash in exchange for a transfer from the customer's mobile money account.

Any credit or debit transaction generates a notification with indication of the new balance. The security of operations is ensured by the use of a Personal Identification Number (PIN) for every transaction. However, this process has some weaknesses. The PIN characters entered by a customer on one's phone are not masked, thus potentially visible to someone who may be watching. Also, the PIN used is only a 4 digit number which can be guessed through social engineering, especially when users have low security awareness and use obvious PINs such as dates of birth.

In the event that a user's mobile phone is stolen and used by fraudsters capable of determining their user PIN, the unique solution for a user is to report the stolen mobile phone or SIM as soon as possible to the MMO in order to have all mobile money transactions blocked. This reporting process can be burdensome for the less savvy or isolated users who engage less with technology, despite efforts made by the MMOs to raise customers' awareness of security and simplify the reporting process through dedicated service lines, email addresses, messaging apps, Frequently Asked Questions (FAQ) sections on websites etc. Besides, a complaint filed with the police is sometimes also necessary in addition to, or as a precondition for, the signalling made to operators.

2.2.1. Mobile money transaction types and transaction flows

The mobile money account holder can perform an increasing number of transactions. The number and variety of operations has grown, as mobile money markets matured and partnerships formed between various players involved in this market. Figure 1 below summarizes the main types of transactions that are currently available to a mobile money account holder:

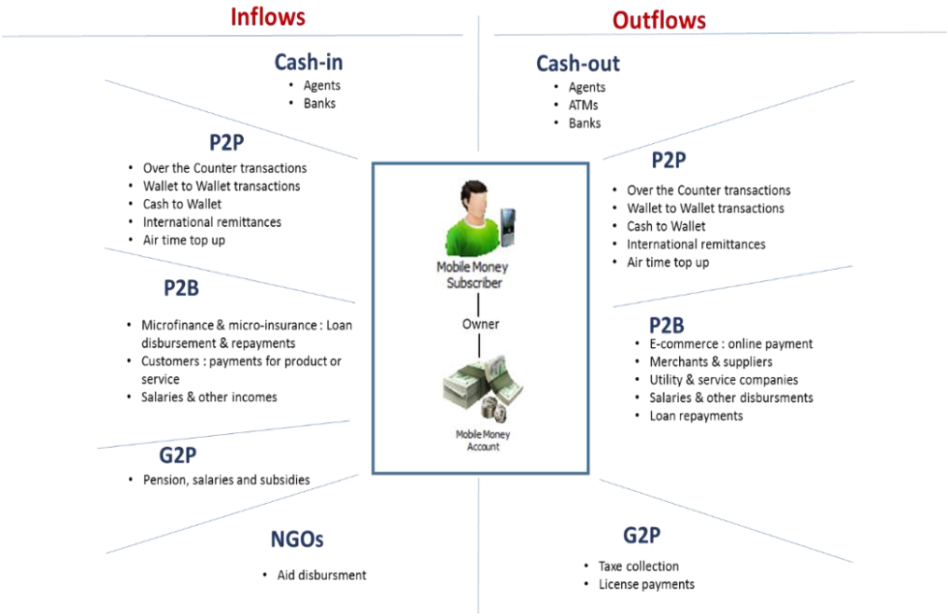


Figure 1: Representative mobile money transactions[5]

Cash-in: The process by which a customer credits his account with cash. This is usually via an agent who takes the cash and credits the customer's mobile money account.

Cash-out: The process by which a customer deducts cash from his mobile money account. This is usually via an agent who gives the customer cash in exchange for a transfer from the customer's mobile money account.

P2B: Person to Business transaction

P2P: Person to Person

G2P: A payment by a Government to a person's mobile money account.

Source: GSMA Mobile Money Definitions

It should be noted that the most common transactions in Sub-Saharan Africa and in the MENA region which include North African countries are cash-in, cash-out and peer to peer (P2P) transactions[6] as per Figure 2 below.

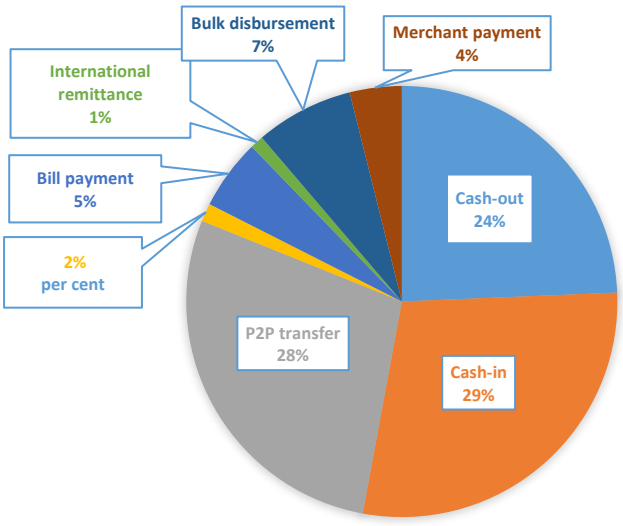
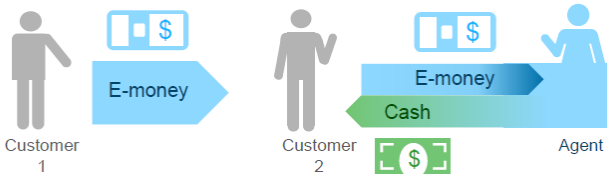


Figure 2: Breakdown of mobile money transactions per type, based on transactions value, in Sub-Saharan Africa in December 2018[7]

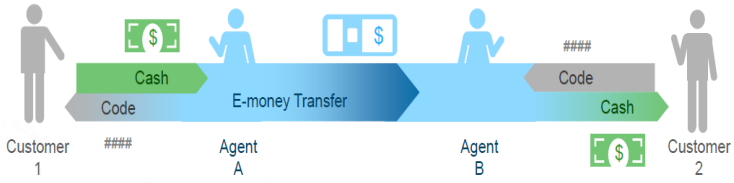
P2P transactions are mostly of two types, Wallet to Wallet transactions (See Figure 3) and Over the Counter Transactions (OTCs). An OTC transaction occurs when the sender or the receiver does not use his own mobile money account but instead transacts in cash with an agent who executes the electronic payment on his/her behalf.



Transfer: Customer 1 sends money via his/her wallet to customer 2, typically paying a fee for the service.	**Cash-out**: Customer 2 receives funds into his/her wallet free of charge. He/she may choose to keep the E-money or cash it out. In such case,the customer pays a fee to withdraw cash from an Agent, who earns a commission

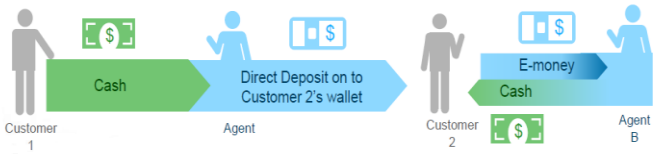
Figure 3: Wallet to Wallet transaction[8]

OTC transactions are useful in the case when the sender or the receiver does not possess a mobile money account. Besides, they may be easier for illiterate customers who do not have the ability to manage the menu interface. Nonetheless, OTC transactions limit the customers' ability to use the full range of mobile money products (e.g. they cannot store value in their E-wallets and are not creating a consumer financial profile that may later be used to assess credit-worthiness and access micro loans and insurance services, etc.). Besides, this type of transaction may expose customers to higher risks of fraud by dishonest agents or third parties.[9] Finally, there are several types of OTC transactions and some variants may not be allowed by national legislations. Figures 4 and 5 below illustrate two out of many possible OTC transaction types.



Cash payment: Customer 1 provides cash to Agent A and pays a transfer fee. He receives a code from Agent A.	**Transfer**: Agent A makes the funds available for "pickup" at any other agent location, and earns commission.	**Disbursement**: Agent B is provided a code from the receiving customer (customer 2), disburses cash, and earns a commission.	**Cash receipt**: Customer 2 picks up cash from the receiving agent, and does not pay a fee.

Figure 4: Cash to cash OTC transaction[10]



Cash Payment: Customer 1 visits an agent with cash, sometimes paying an informal fee for the service.	**Transfer (deposit):** Agent A uses their agent account to deposit directly onto the personal account of the receiving customer (Customer 2).	**Cash-out:** Customer 2 receives funds into their wallet free of charge, but pays a fee to withdraw cash from Agent B, who earns a commission.

Figure 5: Direct deposit OTC[11]

2.2.2. Mobile money access channels

Most mobile money platforms in Africa offer users a menu driven system through which they can perform a variety of operations/transactions. Each platform applies different methods to deliver these commands to its servers via a number of channels.[12] Each channel has its characteristics and advantages but the USSD is dominant in Africa where according to the GSMA, over 90 per cent of mobile money transactions are driven by the USSD.[13] Indeed, USSD appears to be the most appropriate access channel for mobile banking thanks to its compatibility with virtually any mobile phone including the most basic ones (feature phones) owned by the poorest and unbanked customers. It is additionally aided by its ease and speed of use for customers, its limited operation cost for MNOs, and lastly its relative security. USSD is indeed deemed more secure as it is session-based and once the session terminates, no data is left on the phone. Conversely, Short Message Service (SMS) is transaction-based, and SMS data stored on the phone creates a vulnerability if the SMS is not erased and the phone ends up in the wrong hands.

M-PESA in Kenya, which is the best known mobile money system in the world with its 20 million users, does not use the USSD but the SIM Tool Kit (STK) coupled with encrypted SMS. Nevertheless, M-PESA in Tanzania, which was launched a year later in 2008, was developed on USSD technology rather than STK.

STK technology helps break down the transaction into a series of logical steps that can be followed by the customer to accomplish the transaction with the objective to ensure that the user does not have to remember complex keywords or sequences. USSD nonetheless remains faster to use and more suitable for complex transactions. In addition, some MMOs employing USSD channels, such as Airtel Money, support the use of nicknames (created beforehand within a list of favourites) in the place of a mobile number to indicate the recipient of a transaction. Besides privacy and security, nicknames can be similar to a business name, making them more memorable for customers.[14]

Increasingly, mobile money platforms are compatible with a variety of different access channels i.e. Virtual Imaging Platform (VIP), Wireless Application Protocol (WAP), SMS, USSD, STK and mobile apps. This versatility helps broaden how users can interact with mobile money services.

GSM networks are known to have security gaps in their encryption and authentication algorithms, especially in generation prior to 3G.[15] As a result data sent via either USSD or SMS is not encrypted end-to-end and a transaction is therefore vulnerable to interception. Some GSM security flaws have been addressed in generations above 2G systems[16] but 2G technology still represented 59 per cent of mobile connections in Sub-Saharan Africa (and 37 per cent in the MENA region) in 2018,[17] despite a rapid adoption rate of 3G and 4G technologies.[18] Mobile operators have to ensure interaction between networks of different generations (2G, 3G and 4G) which leaves room for possible cross-protocol attacks, exploiting the flaws in signalling channels used by these different generation technologies. Exploitation of these flaws may enable a fraudster to affect mobile network operability, bypass billing, intercept calls and SMS and steal money from mobile accounts.[19]

EXISTING ACCESS CHANNELS:

IVR: Interactive Voice Response is a technology that allows a computer to interact with humans through the use of voice and DTMF tones input via a keypad. In telecommunications, IVR allows customers to interact with a company's host system via a telephone keypad or by speech recognition, after which services can be inquired through the IVR dialogue. IVR systems can respond with pre-recorded or dynamically generated audio to further direct users on how to proceed.

SMS: Short Message Service is a text messaging service component of most telephone, Internet, and mobile device systems. It uses standardized communication protocols to enable mobile devices to exchange short text messages

USSD: Unstructured Supplementary Service Data, sometimes referred to as "Quick Codes" or "Feature codes", is a communications protocol used by GSM cellular telephones to communicate with the mobile network operator's computers.

WAP: Wireless Application Protocol is a technical standard for accessing information over a mobile wireless network.

STK: SIM Tool Kit is a standard of the GSM system which enables the subscriber identity module (SIM card) to initiate actions which can be used for various value-added services.

Source: Wikipedia

2.2.3. Mobile money consumer protection

Consumer protection is defined as the practice of safeguarding buyers of goods and services and the public against unfair practices in the marketplace. These protection measures are often established by law, with the intent to prevent businesses from engaging in fraud or specified unfair practices in order to gain an advantage over competitors or to mislead consumers.[20] There are three dimensions of mobile money consumer protection:

- Basic protection rules
- Safeguarding of consumers' funds
- Consumers' deposit insurance

Basic protection rules pertain to ensuring transparency as regards: a) price of services, b) guaranteeing customers' access to the terms of service and c) granting access to recourse and complaint procedures in order to resolve disputes. Figure 6 below presents the level of protection enjoyed by consumers on the basis of previously listed criteria.

Available data indicates that the situation varies greatly between countries and regions as regards basic consumer protection offered to mobile money users. A majority of SARPCCO region countries appear to be lacking basic protection rules for mobile money users. In other regions, the situation is more favourable to mobile money users.

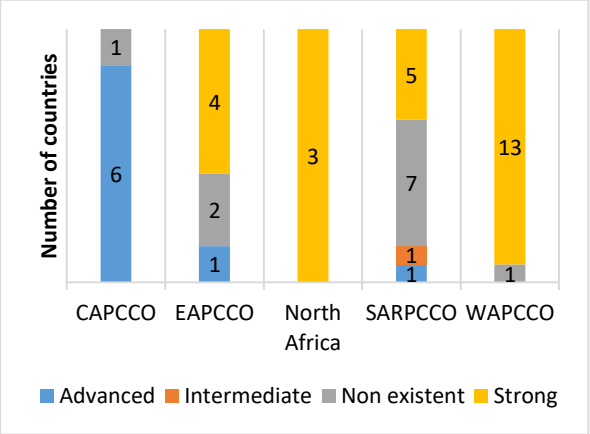


Figure 6: Assessment of consumer protection regulations in different African regions.[21]

The situation with regard to regulations pertaining to the safeguarding of consumers' funds is more homogenous. As per GSMA data, all MMOs in Africa are required by regulation to safeguard consumers' deposits in order to make sure that funds are set aside in safe, liquid investments to meet customer demand for cash. In other words, MMOs must make sure that they can provide in cash, the equivalent of their e-money liabilities. Non-banks providing mobile money have to keep 100 per cent of their e-money liabilities in liquid assets while banks allowed to provide mobile money must be prudently regulated.[22]

In relation to the safeguarding of funds, in the event of default or bankruptcy another mechanism applies, that of the insurance of consumer deposits. Traditionally, a deposit insurance is a measure implemented to protect bank depositors in full or in part from losses caused by a bank's inability to pay its debts when due. Similarly, in the context of mobile money, a deposit insurance regime aims at compensating

individual mobile money account holders in the event of a MMO's insolvency. In the absence of such insurance, mobile money customers are not entitled to priority status with respect to reimbursement in full or part of their funds.[23] According to GSMA data, only five African countries (Gambia, Ghana, Kenya, Nigeria and Rwanda) have a mobile money regulation providing deposit insurance protection for each mobile money account. In the event of an MMO bankruptcy, most African mobile money users would therefore lose the bulk, if not all of their deposits.

3. Landscape of mobile money services in Africa

3.1. Mobile money deployment and adoption

Mobile money started in 2007 in Kenya with the M-PESA service. Since that date mobile money services have spread across Africa and the African continent is the world leader in terms of mobile money services. In September 2019, there were 153 active MMOs operating in 45 African countries.

By the end of December 2018, more than 395 million customers' accounts were registered in sub-Saharan Africa alone, including more than 100 million active on a monthly basis. The estimated total value of transactions generated through these accounts exceeded USD 301 billion in sub-Saharan Africa in 2018.

Eastern Africa is by far the leading African region in terms of the value of transactions, of which it represented close to 70 per cent in 2018. The share of Western Africa in terms of the value of transactions is in strong progression since 2013.

Mobile money will continue expanding in Africa. There is still a significant growth potential for mobile money services in countries such as Nigeria, Ethiopia and Egypt who so far have low rates of financial inclusion and limited availability of mobile money services.

Among significant dynamics affecting the mobile money services in Africa is interoperability. Interoperability increasingly enables customers to transfer money between accounts held with different MMOs, enables them to transfer money between accounts held with MMOs and other financial system players such as banks, and lastly enables them to transfer money across borders, a fact offering increased opportunity to criminals.

Another significant dynamic affecting the mobile money services in Africa is digitalization, particularly development of services aside cash-in, cash-out and P2P transfers. This indicates that the mobile money services offered are getting larger and that institutional actors and private businesses are increasingly adopting mobile money, which became a driving factor of the digitalization of the African economy and a shift away from a massively cash-based financial system.

The third dynamic poised to affect the mobile money services market in Africa is the smartphone adoption. Current smartphone adoption rates in sub-Saharan Africa are reported to be around 39 per cent and around 31 per cent in North Africa. This rate is set to rise to 66 per cent by 2025. Higher smartphone adoption will open access to a larger customer base, broaden the range of available financial products and services and lead to an increase of transactions performed through smartphone apps.

3.1.1. Operators

The adventure of mobile money started in 2007. The number of active mobile money operators then grew steadily across the continent, with a high point in terms of new operators entering the market reached in 2012. That year, 35 service providers launched their mobile money products in five regions[24] of the continent.

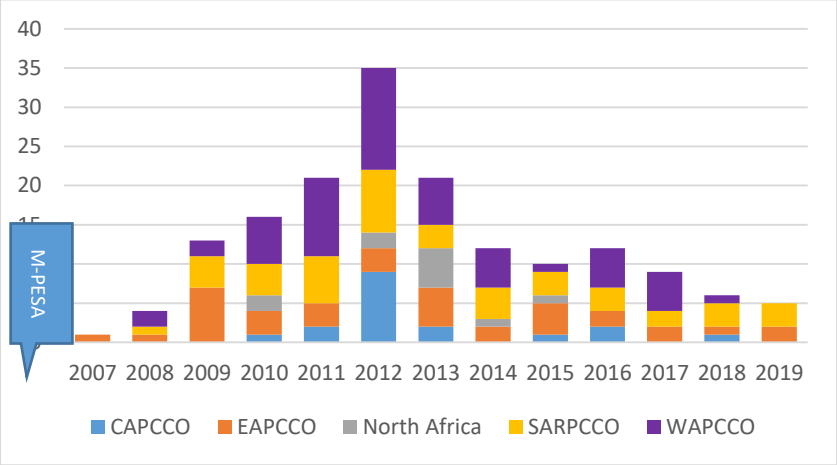


Figure 7: Timeline of MMO deployment in Africa

Today, the African continent is the world leader in terms of mobile money services.[25] As of 3 September 2019, there were 153 active MMOs operating in 45 African countries.

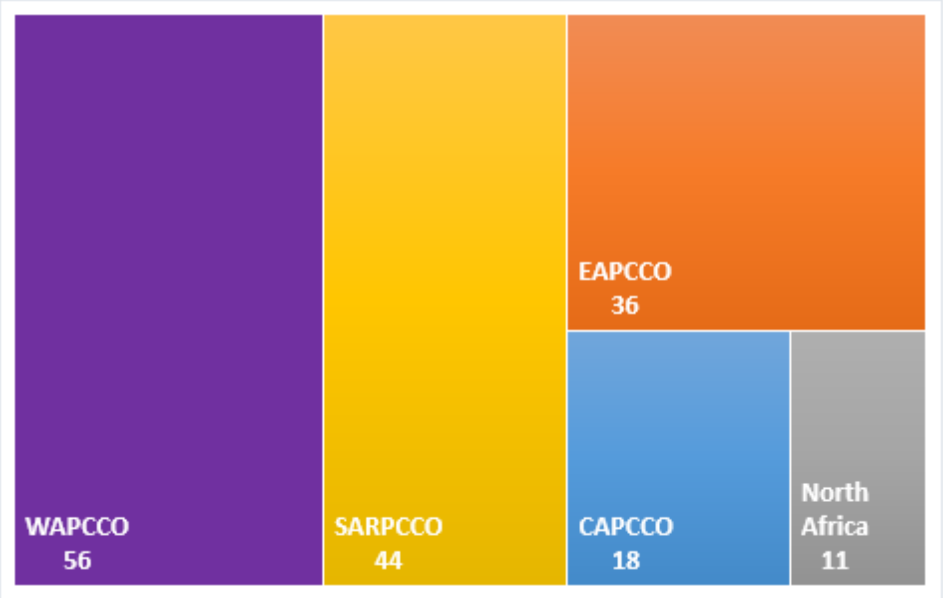


Figure 8: Number of mobile money operators per African region as of September 2019[26]

3.1.2. Users

According to GSMA, over 60 per cent of the sub-Sahara African adult population possess a mobile money account.[27] In this region, MMOs totalled as of December 2018, 395,698,890 registered customers' accounts, including more than 100,000,000 active on a monthly basis.

Whilst the number of registered accounts is a good indicator for the expanding popularity of mobile money, the number of active accounts is a more significant metric to measure the rate at which customers are using mobile money services.

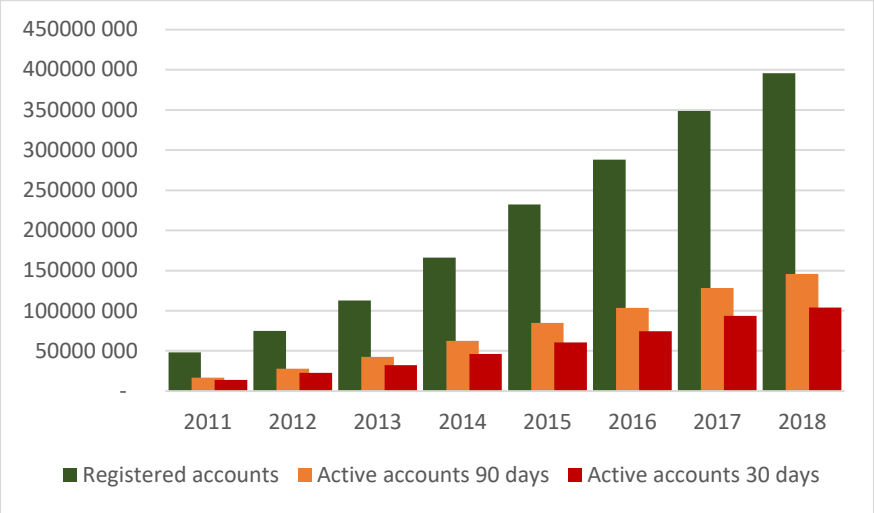


Figure 9: Number of Mobile money registered accounts in sub-Saharan Africa as of December 2018

Notes: Registered accounts refers to the number of customer accounts that have been used to perform at least one P2P payment, bill payment, bulk payment, cash-in to account, cash-out from account, or airtime top up from account during at least 90 days or 30 days prior to the end of a reference period.

3.1.3. Value of mobile money transactions

The estimated total value of transactions generated through these accounts exceeded USD 301 billion[28] for the year 2018. This value has increased by 457.41 per cent between 2012 and 2018, as indicated in Figure 10 below.

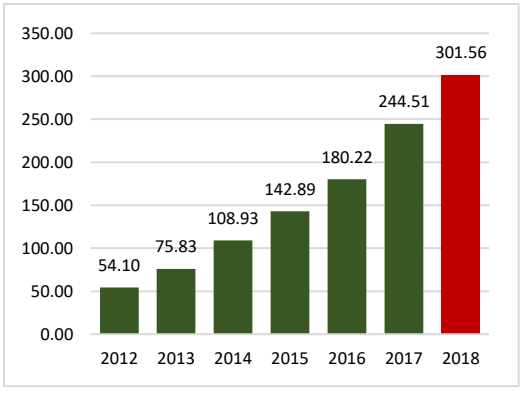


Figure 10: Estimated value of transactions in billion USD in sub Saharan Africa from 2011 to 2018

As previously indicated, analysis of the GSMA data indicates that Eastern Africa is by far the leading African region in terms of the value of transactions as shown in the figure below. Since 2016, the region accounts for 70 per cent of the value of transactions processed by MMO in Sub-Saharan Africa. Western Africa is also in strong progression since 2013[29], as evidenced by Figure 12. Eastern African leadership results from an early adoption of such services by the region's customers, economic and institutional actors and a conducive economical and legal environment.[30] [31]

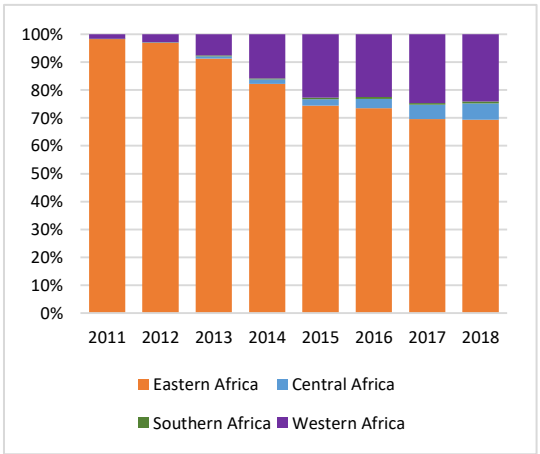


Figure 11: Share of transaction per sub-Saharan African regions, based on transaction value [32]

Analysis of the type of transactions conducted through mobile money services in sub-Saharan Africa indicates that cash-ins to customer accounts, peer to peer (P2P) transfers[33] and cash-outs from customer accounts, represented

the majority of the USD 26.81 billion in transaction value in December 2018. This indicates that mobile money usage in sub-Saharan Africa is centred on individual to individual transactions and is predominantly cash based.

Detailed figures for the five North African countries could not be obtained, as GSMA value and types of transaction datasets incorporate the larger MENA region, which in the GSMA dataset includes: Djibouti, Egypt, Iran, Iraq, Jordan, Morocco, Qatar, Tunisia and the United Arab Emirates. It was hence impossible to extract data specific to North Africa. As a result, trends and patterns affecting North African countries can only be inferred from those affecting the MENA region as a whole, with a substantial margin of error, given the differences that exist between North African and Middle East countries as regards financial inclusion rates, economic structures and growth, social fabric, diasporas, etc.

GSMA data indicates that the MENA market for mobile money services is, in many ways, much smaller than that of sub-Saharan Africa. Indeed, the estimated total value of transactions of mobile money services for the whole MEMA region in 2018 was USD 5.26 billion, compared to the USD 301.56 billion for sub-Saharan Africa, that is to say 57.3 times less. To continue, the total number of registered mobile money accounts in the MENA region is, with 48,891,406 total registered accounts in December 2018, 8 times less than in Sub-Saharan Africa.

Nonetheless, GSMA data indicates that the value of mobile money transactions grew by 30 per cent in the MENA region when comparing December 2017 and 2018 (compared to + 23.33 per cent in sub-Saharan Africa over the same period) and the number of registered accounts grew by 3.43 per cent between December 2017 and December 2018. This is a sign of slow but steady growth.

Regarding the type of transactions conducted through mobile money services in the MENA region, GSMA data indicates that similarly to sub-Saharan Africa, cash-ins to customer accounts, cash-outs from customer accounts and peer-to-peer (P2P) transfers, represented the great majority of the USD 457.81 million in transactions in December 2018.

3.1.4. Future developments

Mobile money services will continue expanding in Africa, both sub-Saharan and Northern, likely at a slower pace as suggested by the relative decline in growth rates of both registered accounts and the value of transactions. This reduction in growth is explained by the fact that the bulk of the adult population in many countries has already gained access to these services. Nevertheless, there is still significant growth potential for mobile money services in Africa. Countries such as Nigeria, Ethiopia and Egypt, with their combined population above 15 years old, exceeding 244 million individuals,[34] have so far had low rates of financial inclusion and a limited availability of mobile money services. In 2018, these three countries have introduced a series of reforms and strategies, which should bolster the development of mobile money services at the national level.[35]

One significant dynamic affecting the mobile money services market in sub-Saharan Africa is interoperability. Interoperability will bolster the diversity of services available to customers, increase their sophistication and enhance their geographical reach, hence positively impacting financial inclusion across the continent.

Another significant dynamic affecting mobile money services in Africa is digitalization. Mobile money services in sub-Saharan Africa are currently largely cash based and centred on transactions carried out between individuals. Data for the MENA region indicates a similar use of mobile money services. Table 2 below indicates that merchant payment, bulk

disbursement, international remittance and bill payment have a growth rate from year to year which is by far exceeding the growth rate of "classical" mobile money services that are cash-ins to customer accounts, P2P transfers and cash-outs. This indicates that mobile money services are getting larger and that institutional actors and private businesses are increasingly adopting mobile money, which became a driving factor of the digitalization of the African economy and shift away from a massively cash based financial system.

Mobile money services	Value in December 2017 in USD billion	Value in December 2018 in USD billion	Growth 2017-2018
Merchant payment	0.57	1.04	84.71 per cent
Bulk disbursement	1.15	1.97	71.67 per cent
International remittance	0.17	0.27	62.08 per cent
Bill payment	0.92	1.42	54.22 per cent
Airtime top-up	0.26	0.36	40.30 per cent
P2P transfer	5.63	7.56	34.24 per cent
Cash-in	6.02	7.66	27.13 per cent
Cash-out	5.21	6.52	25.16 per cent

Table 2: Growth rate, in terms of value, of mobile money services per category between December 2017 and December 2018 in sub-Saharan Africa

Lastly, the third dynamic poised to affect the mobile money services market in Africa is smartphone adoption. Currently, the smartphone adoption rate in sub-Saharan Africa was reported to be around 39 per cent at end of 2018 and it is set to rise to 66 per cent by 2025 according to a GSMA 2018 report on the state of the mobile industry.[36] Available open source data indicates that the average smartphone adoption for three North African countries i.e. Morocco, Egypt and Algeria in 2018 was at 31.6 per cent,[37] therefore in the same ballpark as sub-Saharan Africa.

For MMO, smartphones open access to a larger customer base. Smartphones also enable operators to offer an enhanced user experience and a broader range of financial products and services. Furthermore, based on pattern in other regions of the world, higher smartphone adoption will lead to an increase of transactions performed through smartphone apps instead of USSD technology, which today is used in over 90 per cent of mobile money transactions in Africa.[38]

3.2. Regulations governing mobile money systems in Africa

The majority of African countries authorizing mobile money services have a formal regulatory framework, however there is no standard regulatory model on the continent and differences can be observed between regions and countries. Telecom and financial regulators, such as central banks, are the two main types of observed mobile money regulators, and sometimes the regulation of mobile money services is carried out jointly by the two institutions.

Some regulatory aspects are of particular interest from the law enforcement perspective. Among these are those pertaining to customers' identification, agents' eligibility, transactions and balance limits, international money and Anti-Money Laundering and Counter-Terrorism

Financing (AML/CTF) obligations to which the first listed aspects all contribute.

The risks of money laundering and terrorist financing attached to the execution of mobile money operations stem from the identification of the clientele. This is particularly the case with the difficulties of verifying the authenticity of the identity documents presented to open a mobile money account and use mobile money services. In many African countries, mobile money customer identification systems are weak as a result of insufficient national ID coverage and great diversity in the types of ID documents accepted.

Mobile money services agents perform various tasks of which enrolment of new customers and the conversion of physical money into digital value for cash-in and cash-out operations are the most important. In the majority of countries, regulation allows any person dully registered with an MMO to become an agent. The question of the accurate identification of agents is therefore essential. Any flaws in this respect can have severe consequences given their functions.

Transaction and balance limits result from a compromise between the industry's objectives of facilitating the financial inclusion of the poorest, developing further mobile money services and mitigating the risks of money laundering and terrorist financing. Mobile money regulators hence introduce limits on transactions and account balance associated to an evaluation of mobile money account holders' risk profile. There is a great versatility of practices across the continent and within various regions as regards transaction and balance limits.

International money transfers are one of the fastest growing mobile service on the African continent. They constitute additional risks with regards money laundering and terrorism financing as they may enable criminal proceeds to be relocated from the territory where they were generated to another jurisdiction in order to be cashed out or used to further crime. These proceeds can also be moved once again to another jurisdiction. 46 per cent of MMO active on the continent propose international money transfers in one form or another but the deployment of international money transfers between regions is significantly different between regions. Today, there are tens of cross-border and international mobile money-enabled transaction corridors connecting African countries among themselves and to the world.

All African countries have AML/CTF reporting obligations extended to MMOs. However, the existence of the required laws and institutions, does not always translate into effective implementation and technical compliance of the said regulatory framework. The Financial Action Task Force on Money Laundering (FATF) fourth round of countries evaluations has indeed evidenced discrepancies, for many countries, between stated laws and regulations and their actual capacity or effectiveness in enforcing them.

3.2.1. Regulating mobile money in Africa?

Telecom regulators and financial regulators such as central banks are the two main types of mobile money regulators. Sometimes the regulation of mobile money services is carried out jointly by the two institutions. Figure 12 below indicates that there are regional differences as regards mobile money regulatory bodies across the continent.

The WAPCCO region presents the most diversity as regards mobile money regulators. In this region, a new type of regulator in charge of digital economy is involved in mobile money regulation. An innovation that has not been seen in other regions.

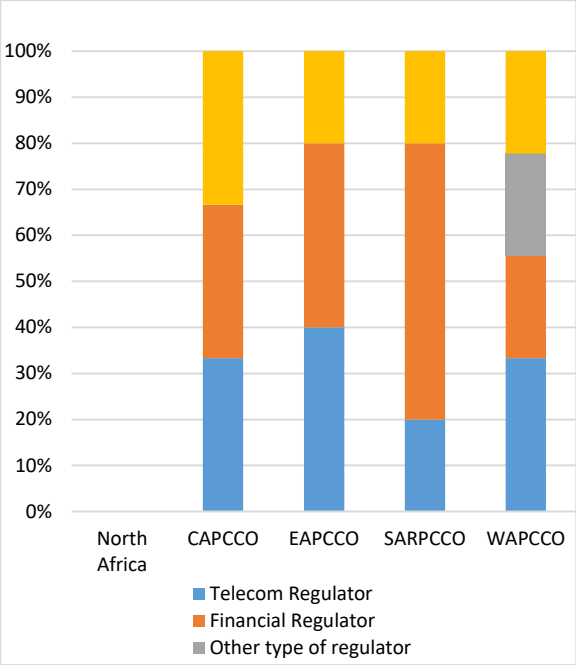


Figure 12: Mobile money regulators by type based on country reporting

3.2.2. Mobile money regulatory frameworks in Africa

The nature of the regulatory body does not seem to have an impact on the regulatory frameworks governing mobile money services in the countries and the regions. In 33 of the 42 countries surveyed, a formal regulatory framework has been set up and formal authorizations to deliver mobile money services have been released. Conversely, in 3 countries (South Africa, Mozambique, Mauritania) MMOs offer mobile money services without any regulatory framework or regulatory sandbox[39]. This overall situation is particularly worrying as it leaves operators alone to decide on their practices and does not offer sufficient guarantees either to consumers or to the services of the State. Finally, in 6 countries, MMO operate either with informal authorizations within a clear regulatory framework (Burundi, Eswatini, Tunisia) or in the framework of a regulatory sandbox, pending a formal regulatory framework (Botswana, Ethiopia, Uganda). In other words, the majority of African countries have a sound and clearly defined regulatory framework as regards mobile money services and it is likely that the minority of countries with no regulations at the moment or those in transitional situations will eventually adopt a regulatory framework.

3.2.3. Analysis of regulatory frameworks

Regulatory frameworks cover dozens of aspects. Several of the latter are of interest in the analysis of potential abuses of mobile money by criminal elements. This analysis will examine five particular aspects of regulatory frameworks:

- Customer identification;
- Agents' eligibility;
- Transactions and balance limits;
- International money; and,
- Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) obligations, to which all the previously-listed aspects actually contribute.

Customer identification

The identification of customers pertains to operators' Know Your Customer (KYC) obligations. The identification is carried out at two levels. Upstream, when registering new customers or opening a mobile money account/mobile wallet and downstream, when customers use mobile money services, especially for cash deposits and withdrawals (cash in/cash out).

To register for a mobile money account, a customer needs to appear in person at an agent or MMO service centre to complete the registration process. This involves completing a form which will materialize the contractual relationship between the user and the operator by presenting some type of identification document (ID) to the registration agent.

In the majority of African countries (32 out of 42 surveyed), customer registration requires an ID and a mobile number for those customers who already subscribed to phone services with the

MMO. Available data further indicates that in four countries (Angola, Botswana, Egypt and Tunisia), customer registration requirements extend beyond a form of identification and a mobile number, to include additional identification elements, such as proof of address. Six countries (Gambia, Lesotho, Liberia, South Africa, Uganda and Zimbabwe) allow operators' flexibility in setting the minimum KYC requirements, subject to some regulatory review or approval.

The type of ID that can be accepted for the purpose of registration has not been standardized across Africa. Acceptance of the following documents has been noted (non-exhaustive list):

- National ID
- Passport (National or foreign)
- Refugee card
- Military ID
- Diplomatic ID
- Alien ID
- ID attestation
- Driver license
- Company ID
- Government ID
- Tax certificate
- Voter's card

Such a wide range of accepted IDs for registration can be explained by the early stages of the national identification systems and regulators' desire to facilitate, through mobile money, the financial inclusion of the greatest number of people.

After registration, the completed form and photocopy of the ID document are forwarded to the MMO's central offices for processing. The processing ensures that the registering agent captured all necessary information and a legible copy of the customer's ID document. If everything is in order, the documentation is filed for regulatory compliance. The customer's mobile money account is activated, and the individual receives a notification.

National IDs are the norm in a vast majority of countries (35 out of 42), when customers are already registered with MMO and want to access mobile money services. In seven countries (Ethiopia, Lesotho, Malawi, Morocco, Nigeria, Tanzania, Uganda), documents beyond Government-issued IDs can be used as minimum requirements in the context of accessing mobile money services (e.g. employment ID, letter from ward or village executive). This does not go without raising some concerns about the trustworthiness of customers' identification processes. Finally, in Gambia and Mozambique, regulation allows provider discretion in verifying identity for the purposes of accessing mobile money services, subject to some regulatory review or approval.

As established earlier, ID documents constitute the cornerstone of the KYC and customer identification process in the majority of African countries. However, it can cause further issues in countries with lower levels of national ID registration rates or insufficiently secured ID documents.

For instance, in Ghana, which is a leading country in terms of mobile money in West Africa, the Communications Minister, indicated on the occasion of the 2018 National Cyber Security Awareness month, that only 10 per cent of reported mobile money fraud cases were investigated and prosecuted in Ghana due to the use of fake IDs to register SIM cards, making it problematic for the police to identify the criminals. According to a study by the World Bank on the state of identification in Africa published in 2017, the national ID registration rate of the population of 15 years old and above in Ghana was of only 2 per cent. It can reasonably be assumed that low national ID coverage rate is conducive to the use of fake IDs by criminals.

In addition to the national ID coverage rates, the above-mentioned World Bank study assessed supplementary criteria such as robustness, integration and legal framework for seventeen African countries that comprise approximately 50 per cent of the total population of the continent. The study reveals a wide range of identity system types and levels of development among the studied countries and that only four of them (Botswana, Kenya, Morocco and Rwanda) have relatively advanced systems based on the above mentioned criteria.[40] See Figure 13 below.

Figure 13: Snapshot of relative identity ecosystem development in 17 African countries[41]

Notes: ***Coverage*** *refers to the population coverage of foundational systems, including civil registration, national IDs, and national population registries.* ***Robustness*** *includes uniqueness, accuracy and security of identity data, credentials, and authentication.* ***Integration*** *refers to the harmonization, interoperability and interconnectivity of the identity ecosystem.* ***Legal framework*** *includes the strength of laws governing institutional roles and mandates, data protection and privacy, and oversight and accountability. Ethiopia does not have a centralized national ID system and its birth registration rate is low. However, the country has an extensive local ID system (kebele cards) that serves as the primary proof of ID for most transactions.*
Source: IMSA reports, based on identity systems as of the individual report date; does not take into account recent developments and improvements.

The study notes that the integration and interoperability of identity systems are weak in most countries. In many countries, several agencies are responsible for establishing foundational identity systems including civil registration (which are still paper based in the majority of countries) and identification. Besides, a multitude of identity registers are managed in isolation by different ministries. However, although some countries retain paper IDs, most civil identity systems are electronic and use biometric technology to "de-duplicate" people. The majority of countries have also adopted plastic cards and smart cards with advanced security features. Nonetheless, the deployment of these more modern and more secured ID documents is slow and sometimes lacks consistency over time and geographical areas, even within the same countries. All of this further facilitates the use of fake or fraudulent IDs by criminals.

Agent eligibility

Mobile money agents are at the heart of mobile money services. They are the primary interface between the customer and the mobile money companies for which they work. They do not work in mobile money company offices or premises but rather in small booths or shops. They can also be itinerant and move from one place to another.

According to data from GSMA, there were 2,327,945 registered agents in sub-Saharan Africa as of December 2018, of which 60per cent were considered active, meaning that they had facilitated at least one transaction within the past 30 days.[42]

In the MENA region, the number of registered agents amounted to 99,480 of which 23.11per cent were considered as active, meaning that they had facilitated at least one transaction within the past 30 days.[43] Agents perform various tasks such as familiarizing customers with products and services and guiding and supporting them in their transactions. Most importantly, agents can enrol new customers and they are responsible for converting physical money into digital value for cash-in and cash-out operations. Given their central role in the mobile money system, it is important to understand the regulations governing their activity especially with regard to their eligibility to become agents.

In this respect, analysis of the GSMA Global Money Dataset indicates that the vast majority of countries have fairly liberal regulations as to who can become a mobile money agent. Thus, in 36 out of 42 (85.71per cent) surveyed countries, regulation does not contain a prescriptive list on the identity of agents, which allows any person, dully registered with an MMO, to become an agent.

The question of the accurate identification of agents is therefore essential. Any flaws in this respect can have severe consequences given their function and access to customers' information and money. In three countries (Kenya, Morocco, Tanzania), agent eligibility is more restrictive since a prescriptive list on the identity of agents is in force. Finally, in three other countries (Angola, Mauritania, Tunisia), only banking agents are authorized to deliver mobile money services. These two last categories of regulations offer more security regarding the selection of agents and their control by MMO and law enforcement. However, the increased level of security they offer hampers the deployment of mobile money services in rural and/or remote areas, hence defeating the very purpose and added-value of mobile money services as a means of financial inclusion of poor and unbanked populations. This explains why these two regulatory models are not widespread across the continent.

Transactions and balance limits

The mobile money services industry has sought a balance between the objectives of facilitating the financial inclusion of the poorest, making mobile money services attractive to the greatest number of people and mitigating the risks of money laundering and terrorist financing. Mobile money regulators usually introduce limits on transactions and account balance, this is coupled with an evaluation of mobile money account holders' risk profile.

Transaction limits mostly follow one of the following approaches: [44]

- Limits on individual transactions and/or the number of transactions in a specific time period (e.g. per day);
- Limits on the total value of the transaction over a given period (usually per month, but in some instances per day or year);
- Limits on mobile money balances;
- Limits are determined or authorized for each licensed provider by the Central Bank, monitoring them regularly. There are no prescriptive transaction limits in the regulations.

- Some regulators apply a combination of transaction limits (e.g. on both single transactions and on the total monthly value).

In addition, under the risk-based approach to KYC, several levels of accounts based on the risk profile of mobile money account holders are determined. This risk profile is lowered when supplementary, verifiable KYC documentation is produced.

Entry-level or low-value accounts are subject to minimum KYC requirements, requiring low documentation demands and having lower transaction and balance limits, these are intended as a first step towards financial inclusion for the unbanked. They may present more risks for money laundering and terrorism financing given their more relaxed KYC requirements. Intermediary-level accounts or medium value accounts have medium KYC/documentation requirements and allow intermediate transaction and balance limits. Finally, top tier accounts or large value accounts allow high transaction and balance limits but come with bank grade account opening KYC documentation requirements. In many countries, top tier account holders are also banked.

In some countries, regulations can be very specific as to the amount of transactions and balance per account categories. This is for example the case in Nigeria and Ghana. In other countries, the regulator establishes general ceilings and leaves MMOs to specify the maximum balance one can hold in their mobile money account and the amount one can transact within a determined period of time, provided that the KYC requirements and risk-based accounts segmentation principles are observed. This is the case of Kenya and countries governed by the Bank of Central African States (BEAC)[45] and the Central Bank of West African States (BCEAO).[46] Furthermore, specific and usually more stringent restrictions can apply to non-identified customers and over-the-counter transactions. Conversely, there are generally separate provisions within regulations for agents and merchants authorizing higher transaction and balance limits.

Table 3 below illustrates transaction and balance limits for mobile money accounts in some African jurisdictions.

	Daily cumulative transaction limit					Cumulative balance limit				
	Nigeria	**Ghana**	**Kenya (MPESA)**	**BCEAO**	**BEAC**	**Nigeria**	**Ghana**	**Kenya (MPESA)**	**BCEAO**	**BEAC**
KYC level 1 customers	**NGN 50,000** USD 137.94	**GHS 300** USD 53.81	**KES 140,000** USD 1,388.12	**XOF 10,000,000** Monthly USD 16,811.86	**XAF 3,000,000** USD 5,043.36	**NGN 300,000** USD 827.64	**GHS 1,000** USD 179.37	**KES 100,000** USD 991.51	**XOF 2,000,000** USD 3,362.30	**XAF 5,000,000** USD 8,405.60
KYC level 2 customers	**NGN 200,000** USD 551.76	**GHS 2,000** USD 358.74				**NGN 500,000** USD 1,379.41	**GHS 10,000** USD 1,793.72			
KYC level 3 customers	**NGN 5,000,000** USD 13,794.05	**GHS 5,000** USD 896.86				**Unlimited**	**GHS 20,000** USD 3,587.44			

Table 3: Illustration of transaction and balance limits in selected African jurisdictions [47 &48& 49& 50& 51&52]

The following series of figures compare single transaction limits, monthly transactions limits and balance limits across the mobile money products offered in a country (converted into

USD Purchasing Power Parity (PPP)[53]) as prescribed by the national regulators in five African regions. From an AML/TF perspective, jurisdictions allowing the highest monthly transaction limits for entry level accounts may be the most important to consider. Indeed, such patterns have the advantage of combining limited KYC requirements with potentially high aggregated transaction amounts, over a sufficiently long period of time to avoid raising regulators' alarm. This can facilitate the placement and layering phases of the money laundering process.

The data and scoring used comes from the GSMA Mobile Money Metrics dataset and the GSMA 2018 Mobile Money Regulatory Index published in February 2019.[54] A higher score is associated with a higher limit. A score of 101 applies to countries with no transaction or balance limits and where there is no specific regulatory framework to provide authorization for the provision of mobile money services.

Analysis of the said data (see appendix 1, illustrations of transactions per region) indicates a wide range of practices across the continent and within various regions as regards transaction and balance limits. This diversity reflects different strategies and priorities on the part of national regulators with regard to combating money laundering and terrorist financing, promoting financial inclusion, furthering and diversifying mobile money services ecosystems (See "Mobile money transaction types/ transaction flows"). Indeed, as mobile money services develop, the average number of transactions per active customer grows in several countries, MMOs are calling national regulators to increase transaction and balance maximums. If the latter are too modest, mobile money users may feel inhibited to fully utilizing their mobile money accounts. This may push them to open multiple accounts with various MMOs or revert to cash transactions and hence favouring the entrenchment of the informal economy.

International money transfers

From a law enforcement perspective, international money transfers may constitute additional money laundering and terrorism financing risks. Cross-border payments can enable criminal proceeds to be relocated from the territory where they were generated to another jurisdiction where they may be cashed out or used to further crime. These proceeds can also be moved once again to another jurisdiction. Cross-border money transfers may therefore make it difficult to determine the origin of funds and hamper law enforcement capacity to investigate money laundering and terrorism financing.

Available data indicates that regulations in 44 out of 45 African countries where mobile money is available allow mobile money users to either send and/or receive international money transfers from their mobile money account. This regulatory possibility has resulted in international money transfer services availability in 27 countries on the continent. These international money transfers are mostly achieved through the following schemes:

- Partnerships between MMOs across borders. These MMOs can be of the same group or competitors. For instance, in 2014 telecom companies Airtel and MTN collaborated to allow MTN mobile money users in Ivory Coast to send remittances to Airtel money users. Depending on agreements between MMOs, some of these partnerships allow sending and receiving money while other only allow either to send or receive. Nonetheless, such partnerships have been key to developing intra-regional corridors within Africa. See Map 1 below.
- Partnerships between MMOs and money transfer operators (MTOs) such as Western Union, MoneyGram etc. In this model,

remittances are received on a mobile money account. They cannot be sent from the mobile money account to a recipient to be cashed through the MTO. This scheme facilitates North-South transfers and is reputed to be the preferred method for receiving international remittances in rural areas.[55]

- Partnerships between MMOs and digital remittance service providers (DRSP) such as WorldRemit, Small World etc. offering online money transfer services. Similarly to the MMO-MTO model, remittances are received on a mobile money account and cannot be sent from it. Being totally online based, this model eliminates the need for an agent in the sending country which enables cheaper transfer fees.

Mobile money-enabled international transactions have been flourishing since their introduction. In sub-Saharan Africa they are one of the fastest growing mobile money based services. Factually, the value of mobile money-enabled international transactions grew by 62 per cent between December 2017 and December 2018. West Africa in particular processes the highest number of mobile money based international remittances transactions in the world, thanks to low prices offered by MMOs for small transactions and strong cross-border collaboration between mobile money providers.[56]

Today, MMOs operating on the continent offer tens of cross-border and international mobile money-enabled international transaction corridors, connecting African countries with strong regional dynamics. Table 4 and map 1 below illustrates transaction corridors where mobile money could be used both to send and to receive international remittances as recorded in May 2018.[57] It is probable that since then, new corridors have appeared.

on the partnerships between MMOs, MTOs and

REMITTANCE SENDING COUNTRY \ REMITTANCE RECEIVING COUNTRY	Benin	Burkina Faso	Côte d'Ivoire	DRC	Kenya	Malawi	Mali	Niger	Rwanda	Senegal	Tanzania	Togo	Uganda	Zambia	Zimbabwe
Benin			●					●				●			
Burkina Faso			●				●	●		●					
Côte d'Ivoire	●	●					●	●		●		●			
Kenya									●		●		●		
Malawi								●	●					●	
Mali		●	●					●		●					
Niger	●	●	●	●		●	●		●	●		●		●	
Qatar					●										
Rwanda				●	●	●					●		●	●	
Senegal		●	●				●	●							
South Africa															●
Tanzania					●				●						
Togo	●		●					●							
Zambia				●		●			●						●

Table 4: Corridors where mobile money can be used both to send and to receive international remittances

Map 1: Map of corridors where mobile money can be used both to send and to receive international remittances

Table 5 below presents corridors where mobile money can be used only to receive international remittances. These corridors are mainly based DRSPs and are mostly used by the diaspora working and residing in developed countries to send money to their relatives remaining in the home country.

REMITTANCE SENDING COUNTRY \ REMITTANCE RECEIVING COUNTRY	Burundi	Côte d'Ivoire	DRC	Ghana	Kenya	Lesotho	Madagascar	Mali	Mozambique	Nigeria	Rwanda	Senegal	Somalia	Tanzania	Uganda	Zambia	Zimbabwe
Australia	●		●	●	●						●		●	●	●	●	●
Belgium											●						
Canada	●	●	●	●	●						●		●	●	●		●
Denmark			●														
Finland											●						
France		●					●	●				●					
Germany				●	●										●		
Ireland			●														
Italy				●	●												
Netherlands			●	●											●		
New Zealand																	●
Norway	●			●							●				●		
South Africa					●	●			●								
Sweden	●		●	●	●						●		●	●	●		
Switzerland		●															
United Arab Emirates					●												
United Kingdom		●		●	●	●				●	●		●	●	●	●	●
United States	●		●	●	●					●	●		●	●	●		●

Table 5: Corridors where mobile money can be used only to receive international remittances[58]

Mobile money international transfers trigger some specific questions regarding AML/CTF requirements. For instance, KYC for domestic transactions can differ from KYC for trans-border transfers and as a result, identification procedures for domestic mobile money transactions may be insufficient to meet the KYC requirements for international transfers.[59] Observed practices across studied MMOs seem to indicate that only dully registered customers can receive or initiate international transfers. Differences in the reliability of national identification systems, as mentioned in the section dedicated to customer identification in this report, are therefore of key importance when assessing KYC requirements coherence for cross border mobile money transactions.

Finally, as seen in the "Transaction and balance limits" section, there are differences in transaction and balance limits for mobile money accounts between countries. The observed practice seems to be that the lower limit either in the sending country or the receiving country applies. In other words, a customer in the sending country cannot send more than the authorized transaction ceiling and, the receiving customer cannot receive a transaction exceeding the maximum authorized received amount and balance amount.

Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) obligations

According to the GSMA, all African countries have AML/CTF reporting obligations extended to MMOs. The existence of national regulations in this field is a critical step towards combating money laundering, terrorism and organise crime financing. However, AML/CTF technical compliance, that is to say the existence of the required laws and institutions, does not always translate into effective implementation of the said regulatory framework. This has been shown by the Financial Action Task Force on Money Laundering (FATF) fourth round of country

evaluations in 2013 and which evidenced discrepancies, for many countries between stated laws and regulations and their actual capacity or effectiveness in enforcing them.

Out of the 15 African countries mentioned in the last FATF country consolidated assessment ratings published in February 2020[60], only two obtained a "Substantial level of effectiveness" for one of the 11 assessed (see appendix 2) "Immediate Outcomes." Effectiveness as regards the 10 other "Immediate Outcomes" was considered either moderate and therefore requiring major improvements or low, and therefore requiring fundamental improvements.[61] As for the 13 other African countries, their assessed level of effectiveness as regards each of the 11 "Immediate Outcomes" was either moderate or low.

Like national regulations, internal AML/CTF policies applied by MMOs may have weaknesses in their implementation. These weaknesses will potentially be greater as the level of effectiveness of national regulations is low. Little information exists in this respect, however some examples of internal fraud to operators (See typology) indicate that there are failures in their internal control systems.

According to several sources, money laundering is quoted as an offence committed using mobile money services in Africa. It could also be used by terrorist.

	Some potential vulnerabilities enabling the ML process			Controls applied by MMOs
	Loading/Placement	**Transferring**	**Withdrawing**	
Anonymity	Improper identification of customers. Multiple accounts can be opened under different identities to hide the true value of deposits. The origin of funds converted to e-money is unknown	Suspicious names cannot be flagged by system, making it a safe zone for known criminals and terrorists	Allows for cashing out of illicit or terrorist-linked funds	Customer profile building, includes registration info (name, unique phone number, etc)
Elusiveness	Criminals can structure/"smurf" proceeds of criminal activity into multiple accounts	Criminals can perform multiple transactions to confuse the money trail and true origin of funds	"Smurfed" funds from multiple accounts can be withdrawn at the same time and/or another country	Limits on amount, balance, frequency and number of transactions Real-time monitoring
Rapidity	Illegal money can be quickly deposited and transferred out to another account	Transactions occur in real time, making little time to stop it if suspicion of terrorist financing or laundering	Criminal money can be moved through the system rapidly and withdrawn from another account and/or another country	Real-time monitoring. Frequency restrictions on transactions. Restrictions on transaction amount and total account turnover in a given period
Lack of oversight	Improper or insufficient oversight by national regulators and/or MMOs can pose a systemic risk			MMOs are regulated, either through a partnership with a bank or through becoming a licenced e-money issuer.

Table 6: Main Money Laundering/Terrorism Financing risk factors associated with mobile money[62]

It should be noted, that since mobile money services are mainly deployed in developing and cash-based economy countries, mobile money is an improvement in relation to AML/CTF enforcement compared to cash. Indeed, with the exception of rapidity, the vulnerability for Money Laundering (ML)/Terrorism Financing (TF) is greater for cash than for mobile money against all the other examined risk factors. In many countries where mobile money is deployed, mobile money services attracted large amounts of liquidity that had been sitting as cash.[63]

4. Mobile money and crime

Mobile money enabled criminality certainly represents a significant threat to society in Africa. Such threats include terrorism financing, human trafficking and people smuggling, drug trafficking, stolen motor vehicle trafficking, illegal wildlife trade, stolen works of art, counterfeit goods, money laundering, extortion payments, firearm enabled crime and corruption.

Despite this, the mobile money industry at all levels, from mobile money service providers to customers and the agent network level, identifies fraud and acquisitive crime as the most prominent associated criminal activity. Fraud typologies associated to mobile money are indicated below.

4.1. Vulnerabilities and impact

Vulnerabilities and impact data indicate that criminal cases involving mobile money services within Africa are on the increase.

This increase in mobile money crime likely indicates a causal relationship between the volume of mobile money providers and the proliferation of related criminal activity. It is highly likely that this increase is a key contributing factor to the clear results indicating a status of mobile money criminality as 'on the rise.' Available data suggests a trend of increasing cases related to mobile money services with significant increases between 2016 and 2018 in all the African regions. Notable examples of crime types include money laundering, fraud, extortion (via kidnapping) and links to wider technology crime. Mobile payment systems can be abused for criminal purposes at any of the following three stages:

1) When funds are deposited onto an account (placement stage of money laundering);
2) When funds are transferred between accounts (layering stage of money laundering);
3) When funds are withdrawn from an account, with both customers and agents having opportunities to commit ML/TF-related offenses (integration stage of money laundering).

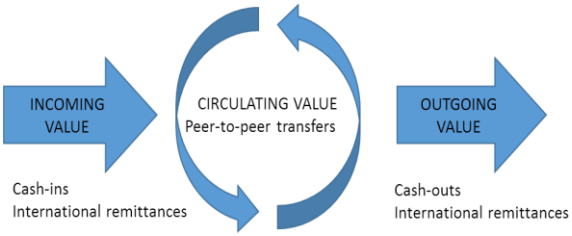


Figure 14: Mobile payments ecosystem

4.2. Key vulnerabilities

4.2.1. Fraud

During the initial stages of establishing MMS franchises and business relationships, businesses, consumers and agents have less understanding of mobile money services at the transactional stage of service. At this stage a victim of MMS fraud is typically trusting the mobile money system but often lacks experienced insight into the process and thus can be exploited by criminals.

Within new and established agent networks, a lack of enforced MMS regulation enables both master agents and sub agents to exploit their

positions. This form of criminal activity targets customers, agents and mobile financial service providers. Systemic vulnerabilities exist in the commission processes facilitating offences such as split deposit frauds.

Exploitation of newly established business relationships are possible during the addition stage of deployment. Such vulnerabilities exploit weaknesses in due diligence processes and eagerness to establish new relationships.

A key vulnerability of business practice has been identified in the lack of business risk assessment concerning staff members and the 'insider threat.' This is particularly present in small companies where few individuals may possess specialist IT skills or technical knowledge.

Concerning the potential position of insider threats, such individuals can easily identify significant investments that are of interest to fraudsters. This can be enabled and facilitated by a lack of internal controls regarding unauthorized staff access and user rights.

Systemic weaknesses in MMS processes are present at all stakeholder levels, including: agents, businesses and mobile money operators. As a result of this, vulnerabilities exist in controls focused on MMS transaction processing. An example could include small businesses operating with poor security SOPs, allocation of multiple rights to individuals or use of public IT facilities.[64]

Fraudulent exploitation of mobile money services are varied in methodology due the multi-layered business model of mobile services. As mentioned above, this includes various actors who may exploit their position to commit fraud. The following three categories of fraud have been identified and these clearly exhibit the range of vulnerabilities:[65]

Transactional:

- 'Vishing scams' occur when a fraudster makes use of phone calls or SMS to gather PINs or personal data to facilitate unauthorized access.
- 'Advanced fee scams' occur when customers are convinced to send payments under false circumstances. An example of this was encountered when a prominent African figure established a charitable donations page on a social media platform offering motorcycles to the youth of his town. To qualify for a cycle, one was supposed to register with a small amount of KSH 200 (USD 2). Criminals were able to duplicate this webpage and take advantage of the publicity of these charitable efforts. They provided a 'PayBill'[66] account number for people to make donations to via mobile money services. These funds were collected by the fraudsters and lost to the charity. The impact of this crime extends to the reputational harm of charitable and public figures.
- 'Pay role frauds' can occur when the details of non-existent employees are used.

Channel:

- 'Split transactions' occur when agents abuse their position to split cash in transactions into smaller payments in order to increase their commission.
- 'False transactions' are cases were agents transfer funds to personal accounts without the customer's knowledge.
- 'Registration fraud' provides agents the opportunity to create false/non-existent customers in order to increase their registration commissions.

Internal:

'Internal fraud' can occur when employees exploit their positions for personal gain

through their level of access to accounts/customer data.

- 'Identity fraud' offers employees the opportunity to use customer data/personal details to develop fraudulent financial profiles.

Mobile money services-orientated frauds have been categorized into the following types and associated methodologies.[67]

4.2.2. Different types of frauds

Consumer driven fraud

This form of fraud represents the most prevalent form across all stages of the mobile money services operation, where offending is enabled by a lack of system based checks and awareness. In this fraud type, agents are often targeted by criminals in the coordinated use of fake currency in distraction criminal operations. Mobile money service providers have recognized the risk of 'insider threats', particularly employees with access to large volumes of customer phone numbers that may be exploited in phishing scams. As such, some measures have been taken to limit access to multi user profiles within the industry by companies.

Agent driven fraud

Some fraudsters exploit 'loopholes' at early stages of the service delivery. This form of fraud often includes products pricing or offenses by low paid workers with access to high volumes of cash at a deliverable level.

Exploitation by master agents can include the reduction of percentage commission provided to agents. This is often facilitated by a lack of knowledge at the agent level and decreased capacity to challenge the master agent.

Business partner associated fraud

These fraudulent transactions occur within business partnership networks. These can be:

- Business to consumer (B2C)
- Consumer to business (C2B)
- Merchant originated

Staff members in financial institutions may exploit access to data to identify accounts with no mobile money facilities and add their own link to these. Alternatively, specialist IT staff in small businesses may manipulate the interface between small businesses and financial institutions to divert money thereby enabling fraudulent transactions.

Certain criminals devise fraud schemes that exploit the P2P feature of mobile payment systems in order to fund their accounts. For example, in one case a victim was fooled into believing that their spouse was involved in an accident and the victim was asked to send money to the fraudster's account using a mobile payment service to pay for the doctor's bill.[68]

Mobile financial service provider fraud

This form of fraud is most common at the activation and value stages of deployment during the mobile money process. Unauthorized transactions are carried out on behalf of the business or insider access enabled activities such as 'facilitation fees' may be applied. Alternatively, SIM numbers may be swapped granting criminals access to funds and a means of transfer or agents may continue to access master agents' accounts following liquidation.

System related fraud

This form of fraud is present at the transaction activation stage of deployment and grows during the value addition stage. Cases of ex-employees utilizing access via commonly shared PINs and passwords qualify as this method.

Insiders are able to identify opportunities for the creation of fake accounts in order to transfer money to an unauthorized point and technological practices can be exploited through security certification. For example, awareness that a computer has been previously used and is

available to the fraudster along with its certification enables fraudulent access to funds.

4.2.3. Enabling factor

The complex and varied levels of operations and actors involved in mobile money services offer multiple layers of opportunity for fraud to occur. Within this context it is clear that the primary enabling factor of these fraudulent transactions, relates to levels of actors' access. This is further increased as a fraud risk factor when considered in the context of poorly applied regulations for agents and master agents.

4.2.4. Key vulnerabilities – other crime types

Organized crime groups are able to utilize the popularity and availability of mobile money services to facilitate criminal activity in a number of diverse crime types. Available data suggests that mobile money is a key facilitating factor in criminality and has links to international organized crime.

Several sources suggest international links between organized crime groups in Africa and in the following countries: India, Russia, the UK, UAE, Germany, Oman, Saudi Arabia and France.

4.3. *Illicit goods trafficking and mobile money*

4.3.1. Drugs trade

The African continent is both a growing global transit hub for the smuggling of a large range of drugs and associated commodities. This includes developing consumer markets across Africa, as well as illicit drugs and substances being transhipped between a production/cultivation location and lucrative consumer markets located elsewhere around the world. Various socio-economic factors, such as the development of trade and transports, lack of alternative economic opportunities for youth, corruption, weak enforcement, and high profit margins for criminal syndicates are nurturing this trade throughout the continent.

Increasing flows of cocaine originating from South America and with final destinations Europe, Asia, and to a lesser extent African regional markets are transiting through the continent mostly via Western, Eastern, and Northern African regions. The African continent is also a transit point for heroin coming from Asia with Europe as final destination. Additionally, cannabis is grown in almost every African region and is trafficked and abused mostly at the regional level, except for North African hashish, which is destined for Europe. Enforcement authorities in Africa have detected an increase in the trafficking of methamphetamines, khat, synthetic drugs, and illegal pharmaceuticals, mostly imported from Asia.[69]

Concerning Eastern Africa, Kenya has a coastline which is 1420 km long and a major port located at Mombasa that is ideally situated to receive clandestine shipments of illegal commodities such as drugs. With the majority of the world's heroin originating in Afghanistan and Pakistan, this geography has contributed in East Africa to the equivalent of USD 10 billion of the global drugs trade.[70] This is enabled in part due to the logistical ease for heroin traffickers moving heroin from Asia into Kenya.

The availability of mobile money services in Kenya offers drug traffickers the opportunity to launder the profits of their criminality. It is highly likely that this opportunity, coupled with the availability of M-PESA services in Afghanistan, in India and the logistics opportunity granted for sea shipments from Asia to Kenya, has contributed to increased prominence for the drug trade in East Africa.

The drug trade is highlighted as representing one of the most significant examples of illicit financial flows in Kenya. It is highly likely that the inter-operability currently developed between mobile money service providers in Kenya, Tanzania and

Uganda will offer international traffickers in heroin the opportunity to increase the efficiency of their operations.

With mobile money services playing an increasingly prominent role in Western and Central African countries, it is highly likely that the trade in cocaine will benefit from this and be enabled by the utilization of mobile money services due to access to such services at all levels of society.

Available data suggests that Marungi (khat) has become an increasing problem associated with mobile money enabled criminality in South Sudan and surrounding countries since the substance was largely outlawed in 2014.[71] Khat is a psychotropic substance with moderate psycho dependency properties that is largely grown in the Maracha district of Uganda[72] from where traffickers use established trade routes to supply markets in wider Uganda, DRC and South Sudan.

Available data suggests that mobile money services have been used in the proliferation of illicit prescription medication, specifically tramadol in Western Africa. Tramadol is a synthetic opioid used to treat pain. It has a stimulating, euphoric effect on the brain and represents 87 per cent of opioids seized globally.[73] It is likely that the stated use of mobile money services in the illicit supply of tramadol in Africa has enabled the expansion of the trade seen in Benin, Ghana, Ivory Coast and Nigeria.[74]

4.3.2. Stolen motor vehicles

Motor vehicles stolen abroad are smuggled to recipients throughout Africa. This smuggling primarily takes place through the major commercial sea ports either in maritime cargo containers or roll-on/roll-off ships. These vehicles are often shipped as second-hand vehicles to conceal their illegitimate origin. In North Africa, stolen vehicles also arrive from Europe on board ferries, driven by smugglers hired by crime syndicates.

In addition to trafficking vehicles as a whole, there is a growing illicit trade in components and parts of vehicles that were stolen and subsequently stripped. Large quantities of vehicles are also stolen and trafficked at national, regional and continental levels in Africa.[75]

Available data suggests the prominent role of the trade in stolen motor vehicles in relation to mobile money abuse. It is likely that mobile money services are enabling organized criminal networks to conduct large scale highly lucrative transactions in this form of criminality across all of Africa. Indeed the UK, being one of the primary source countries for such vehicles, has indicated that stolen vehicles, worth USD 474.6 million, were shipped to the East African region alone in 2015.[76]

Previous ENACT reporting indicates that criminal groups are targeting mid-range segments and sports utility vehicles for importation into Africa from Western Europe (primary source) and Central Europe or Northern America (secondary sources), in order to achieve this organized criminal sale utilizing the various African diasporas present in these regions.[77]

Other regions of Africa are also not spared from this form of criminality. As early as 2012, it was identified that 160 vehicles, with a value of USD 8 million were identified as stolen and intended to be shipped to West Africa, and particularly Ghana.[78]

This criminal trade in stolen motor vehicles connects organized crime groups in Africa to counterparts in other parts of the world. Indeed high value vehicles that are in demand in Africa are sourced in Europe and the United State of America (USA). An example of this criminal connectivity can be seen in an organized crime group based in New Jersey, USA that shipped USD 1.2 million to Nigeria, Ghana, Sierra Leone

and Gambia.[79] This shows the extent to which criminality in Africa has a wide social and economic implications.

Various sea ports across Africa have been identified as crucial to the trade in stolen motor vehicles.[80] Information suggests that the trade in stolen motor vehicles is still a key form of criminality enabled by mobile money services abuses in African countries without any major shipping ports. It is therefore highly likely that the pan Africa trade in stolen motor vehicles is highly dependent on the anonymity and developing interconnectivity offered by mobile money service exploitation.

The pan African trade in stolen motor vehicles is also relevant to high value vehicles stolen in Africa itself. Transnational criminality has been identified in the form of vehicle hijacks in South Africa, following which these vehicles are transported to other African regions. This has particularly been the case concerning Eastern Africa, where mobile money services play a particularly significant social/economic role.[81] Previous ENACT reporting indicated that the inter-African trade in stolen motor vehicles and parts is enabled by firearms usage and that there are markets in Central and Eastern Africa for vehicles stolen in Southern Africa.[82] This trade is highly likely to benefit from criminal exploitation of mobile money interoperability between services in these regions, linking criminal's payment and logistical methods.

4.3.3. Firearm enabled crime

The availability of firearms remains a significant risk to public safety across Africa and has been evident as an enabling factor in many other forms of criminality. Firearm availability fuels conflicts and criminal enterprises within Africa and as such attracts economic resources in order to enable such activities. The value of this trade has been estimated to be USD 1 billion per year.[83] Further, it is enabled by a variety of actors including criminals, corrupt security officials and returning peacekeepers.[84]

There are an estimated 30 million firearms in circulation in Africa.[85] However, it is the frequency of conflict on the continent that creates a prominence with this availability from a law enforcement perspective. Recent conflicts in Congo, Libya, Liberia, Ivory Coast and Sierra Leone have been fuelled and exacerbated by the availability of firearms.[86] It is estimated that between 60 and 70 per cent of conflict-related deaths in Africa are a result of this illicit trade.[87]

Mobile money transactions in the trade of firearms across Eastern Africa, for example, have been identified as a primary means of purchase. These transactions occur within countries and across national borders. It is likely that mobile money transactions play a part in this trade and further investigation is required to establish the prominence of such transactions, including into the prominence played by South Sudan and the Democratic Republic of Congo as source countries of firearms in Africa.[88]

In addition to opportunities to buy firearms, the mobile money industry has provided specific opportunity for criminals with access to firearms. This relates to the presence of mobile money agents on many streets in the region, holding sometimes large volumes of cash with poor security infrastructures and inadequate training and safety awareness. This results in frequent firearm enabled robberies that target these agents.

Agents have often been the victims of robbery. Such robberies are a result of the common knowledge that funds held by agents are secured by a poor level of protective physical infrastructure. Agents have expressed concerns in cities such as Nairobi, Kampala or Arusha of their vulnerability to this threat. They have further sited the lack of support and adequate security training from the mobile money service provider as an area of required improvement.

Mobile money is used as a payment method for criminal acts. An example of this is seen in Uganda during August 2019, when, following an investigation a murderer was found to have been paid via mobile money to kill an individual. This offender was exploited by an organized crime gang in order to arrange contract killings and while the payment method used offered anonymity to the gang due to the regulatory weaknesses of mobile money services registration. In the case of contract killings, individuals (primarily male), often have substance dependencies and seek to identify means to make additional money

It is highly likely that the current conflicts in Libya and DRC will increase the availability of firearms in the illicit market and these in turn will be utilized across Africa by criminal networks.[89]

4.4. Other illicit commodities

African member countries have identified that mobile money services have also been used in the trade in illicit commodities such as wildlife, works of art and counterfeit goods. The trade in these commodities benefits from the anonymity offered to organized crime group members in the same manner as seen in the drug trade

4.4.1. Wildlife crime

Africa is home to a great diversity of animal species including some of the most endangered, and subsequently, vulnerable species on the planet. Animals are poached and trafficked for various reasons, including to be used as pets, for their meat and for their body parts for traditional medicine. Wildlife crime poses a great threat to Africa. The poaching of animal species impacts negatively on the development and economy of countries and erodes the biodiversity and environmental integrity of the continent to varying degrees. This type of criminality generates large profits for criminal syndicates. It is typically transnational, interconnecting African countries, and connecting the continent to the world, and is often linked to corruption.[90]

The illegal trade in wildlife is estimated to be worth between USD 5 and 23 billion and is the fourth most lucrative criminal enterprise after trafficking in drugs, humans and arms.[91] Due to the biodiversity of Africa and the continent's wide range of species of interest to organized crime groups, it is highly likely that mobile money services will continue to offer an opportunity for illegal wildlife traders to purchase and sell such commodities. Available data suggests links between illegal wildlife trade and the abuse of mobile money services.

4.4.2. Works of art

The African continent is affected by an increase in the illicit trafficking of cultural heritage. Antiquities trafficking is an increasingly attractive activity for criminal organizations as there is high market demand for cultural objects, which makes their illegal trade profitable. Due to poor socio-economic and security conditions in some regions, these objects are fairly easy to obtain through theft, illicit excavation and removal of cultural property. Moreover, regulation and detection are not very effective due to the interconnections between the licit and illicit antiquities sectors. Works of art are mostly trafficked from the African continent to Europe, North America and the Gulf states.

Available data suggests that mobile money is also linked to works of art trafficking, in West Africa.

4.4.3. Counterfeit goods

Trafficking in counterfeit goods represents a major threat to public safety and health across the world, in particular on the African continent. Counterfeiting harms public safety as well as businesses that produce and sell legitimate products. It also affects national economies when governments lose tax revenues from products manufactured or sold on the black

market, which put consumers at risk from substandard products. Organized criminal groups play a central role in the trade of counterfeit and pirated goods and generate important revenues from such illicit markets.[92] Available data suggests that by the year 2022, it is estimated that the total value of piracy and counterfeiting could reach a staggering USD 2.3 trillion with a negative global impact of USD 4.2 trillion.[93]

A variety of products is affected by counterfeiting and piracy on the African continent, however, counterfeit pharmaceuticals are the largest trafficked commodity in most parts of Africa. According to the World Health Organization (WHO), every year, around 100 000 individuals die in Africa as a result of fake pharmaceuticals. These fake drugs account for approximately 30 to 60per cent of the total market of pharmaceutical on the continent.[94]

African countries have taken enforcement action against this activity, for example in South Africa during a raid in 2018, when authorities seized over USD 8,000 worth of counterfeit goods.[95] Nevertheless, it remains highly likely that criminal syndicates will propagate this trade. Due to the widespread sale of counterfeit goods across Africa it is likely that mobile money services offer criminals the opportunity to move these items and the related money across the continent whilst avoiding law enforcement detection.

4.5. Corruption

Transparency International suggests that 75 million people across Africa are estimated to pay bribes each year, and that 22 per cent of Africans who have had contact with public officials have been required to pay for access to services.[96] The implications of this are clear. For many citizens of African countries, corruption would provide a significant barrier to accessing the state and its civil support mechanisms. It is highly likely that citizens use the means of financial interaction most common to them in order to facilitate bribes and access to these crucial state functions. As mobile money services are increasingly deployed across Africa, they will be utilized in the payment of corrupt officials.

It has been suggested that surveillance represents a key component to tackling corruption.[97] The regulatory frameworks discussed earlier in relation to mobile money services provide a potential mechanism to identify suspicious payments that may indicate corruption. Such information would be highly valuable to subsequent police investigations. Despite this, the application of these regulations throughout the mobile money services industry in Africa varies in effectiveness. The weak application of the identification regulations avails options for corrupt officials to receive payments.

4.6. Money laundering

Following the acquisition of property and other assets through illicit activities, criminals are faced with the challenge of legitimizing this property to avoid the attention of law enforcement. In addition, criminal networks involved in international trades, such as the drugs trade, are often faced with the challenge of moving money between countries and jurisdictions. Criminals transfer funds across multiple jurisdictions almost instantaneously using mobile money services as African mobile payment system service providers, such as M-PESA, have partnered with peers in other countries in order to enable their customers to transfer funds across international borders.[98]

Money launderers can exploit mobile money services to transfer the proceeds of crime to co-conspirators located in other countries or supporters of terrorist organizations can exploit

this functionality to send funds to terrorist group members throughout the region.

It is highly likely that African countries with well-established mobile money service industries represent an attractive proposition to criminal networks across Africa and indeed the world, as a means to launder illicit profits. This is due to the availability of mobile money services and the weak application of regulations in the industry. Furthermore, the enforcement activities of policing agencies are hindered by the facilitation factors discussed below.

Criminals split large financial transactions into multiple smaller ones, which are more likely to go undetected by authorities. Mobile payment systems' transaction fees are lower than those of traditional banking, therefore, 'smurfing'[99] offers a better risk/reward ratio for criminals. Money launderers transfer proceeds to co-conspirators in multiple transactions of limited size each or multiple terrorist financiers transfer small amounts of money to militant members of the group.

Further to this, criminals are also registering multiple sim cards using personal data available from government sites. Where Names, ID numbers and dates of birth can be obtained from these sites. Using this information, a sim card can then be registered and loaded with illegally acquired money, which can later be sent to legitimately registered businesses through PayBill numbers or till number. The transaction appears legal when in fact the operation has effectively assisted in the laundering of criminal proceeds.

The prominence of money laundering in relation to mobile money services enabled criminality can be seen in the variety of international links identified in various sources. Available data has linked money laundering networks across Africa as well as to India, Russia, UK, UAE, Germany, Oman, Saudi Arabia and France.

4.7. Trafficking in human beings and people smuggling

Millions of persons migrate annually in Africa both fleeing armed conflict and seeking out greater economic opportunities. The majority of African migrants resettle or seek refuge in other African nations.[100] Intrinsically linked to this mass movement of persons is the exploitation of vulnerable populations for material gain by criminal organizations or syndicates. Differences between the offences of people smuggling and human trafficking can be seen in the table below[101]:

	People smuggling	**Human trafficking**
Crime	Against the state	Against the person
Relationship	Provides a service	Exploited as a commodity
Length	Voluntary short term	Long term exploitation
Profit	One off payment	Ongoing appropriation
Borders	Always crosses state borders	Can be internal

Table 7: Differences between the offences of people smuggling and human trafficking

Trafficking in human beings and people smuggling are crime threats of significant concern to the entire continent, with nearly all countries qualifying as source, transit, and/or destination countries. These two crimes are often linked, as migrants can become victims of human trafficking at any point throughout their journey before reaching their final destination.[102]

Available data suggests that human trafficking represents a key form of criminality enabled by mobile money services. This indicates the

prominence of economic migration on the continent of Africa and unsurprisingly provides insight into the motivations of organized crime groups to exploit this. The latter was reflected upon during a Commonwealth telecommunications organizations conference, which took place in London on 7 October 2015. Senior representatives from the mobile money services industry, civil society and governmental partners highlighted the need to address the risks of mobile money and other forms of telecommunication technology being utilized in the exploitation of African migrants.[103]

Organized crime groups have capitalized in this area, as indicated by member countries in Africa, by using mobile money services to manage their financial affairs and launder the illicit profits of human trafficking. In the region, these profits are indicated to be around USD 150 billion per year.[104] The role of mobile money services in the facilitation of this criminal activity must be considered in the context of the wider impact it has on societies. It has been indicated that human trafficking is often committed to facilitate: sexual exploitation, forced labour/modern slavery and trade in human organs.[105]

Due to the transnational nature of human trafficking, the anti-human trafficking intelligence initiative has indicated that mobile money and other crypto-currencies offer an opportunity, if utilized effectively by law enforcement, to identify organized criminal activity.[106] This would however require the stringent application of regulations concerning customer identification in order to avoid the issue of anonymity so that the perpetrators cannot conceal their identity.

4.8. Extortion

There have been occasions of mobile money use to facilitate kidnap for ransom. In the example of Eastern Africa, a kidnaper's motives is to extort money from close relatives of the victims. Kidnappers demand ransom ranging from KES 100,000 to 200,000 (USD 976 to USD 1,952).

Kidnappers have previously registered mobile money accounts using lost ID cards. There have been examples of fake kidnappings, where an individual acted in collusion with others and staged her kidnapping in order to extort money from parents or relatives.

On 4 April 2019, an American tourist was kidnapped in Uganda following which the kidnapper demanded USD 500,000. Following an extensive and successful police investigation, a rescue operation was conducted, it was apparent that the kidnappers relied on mobile money services as a mean of collecting the ransom. It is likely that such attempts will continue in Africa motivated by financial gain and facilitated by mobile money services.

In February 2020, a Chinese national was abducted and held as hostage for three days by four armed men claiming to be officers of the Directorate of Criminal Investigations (DCI), Nairobi, Kenya. The victim was rescued on 29 February by the police. A police officer was among the perpetrators.[107] The intention was for the kidnappers to seek ransom payment via mobile money services.

In addition to kidnapping, examples were identified of death threats for extortion purposes. In such cases individuals are identified and contacted by a criminal who indicates that they have details of the victim's routine and are able to kill them or their family if a payment is not received.

4.9. Enabling factor

In the crime types identified in this section one common theme has been prevalent, that of criminal anonymity. Criminals use false identification documents to open mobile payment accounts, which hinders law enforcement in identifying and arresting these

individuals. This modus operandi is an increasing challenge for law enforcement as many African countries have underdeveloped civil registration and national identity card systems, which enable criminals to use fake ID documents to access mobile money services. Specifically, criminals may use aliases and third party names, including those of the deceased persons, to open accounts at mobile payments service providers. In addition, criminals can open multiple mobile payment accounts under different aliases.

For example, Organized crime syndicates in Eastern Africa, pay young unemployed locals to purchase and register SIM cards. These are used to open mobile money service accounts that are subsequently used by the network for criminal activity or sold to other criminals to use.

The vulnerability of potentially corrupt agents has been identified as a key enabling factor. This specifically relates to agent complicity in criminal networks, money laundering/terrorism-related activities, by not fulfilling KYC obligations and unknowingly facilitating the creation of mobile payment accounts using false identification documents. Agent negligence can also allow customers to exceed deposit or withdrawal limits or ignore suspicious account activity.[108] These risks are summarized as anonymity, rapidity and elusiveness in the risk factors depicted in Table 6.

Due to the transnational nature of organized crime in Africa generally, another significant enabling factor of mobile money services use in criminality is interoperability. Interoperability entails several dimensions. Firstly, it enables MMS customers to transfer money between accounts held with different mobile money services. Secondly, it enables a customer to transfer money between accounts held with MMOs and other financial system players such as banks, remittances companies or online payments companies. Lastly, the third dimension of interoperability is geographical, as it enables customers to transfers money across borders.[109] Whilst these components of interoperability contribute towards the beneficial, financially inclusive characteristics of mobile money services, they also offer significant opportunities for organized crime to exploit these services.

5. Mobile money and terrorism

Since the end of the Cold War the international system has seen the development of a new style of asymmetrical conflict between state and non-state actors. This has been typified by the extent of terrorist activities on the African continent[110] and can be seen in all African regions and the developments in mobile money interoperability across Africa offers such groups increased means of financial support.

In Western Africa, Boko Haram was established in 2002 in Borno State, Northern Nigeria, as a proposed attempt to establish strict Islamic law in Nigeria. During the course of its history Boko Haram has conducted 3,416 terrorist attacks and incidents, and caused 36, 000 fatalities.[111]

In Central Africa, the Lord's Resistance Army has modelled itself as a Christian liberation force. This group was established in the 1980's in Uganda but has, more recently, taken residence in the Democratic Republic of Congo and Central African Republic. Throughout its history this organization has displaced 2 million people.[112]

Al-Shabaab represents a significant terrorist threat to stability in the Eastern African region. Following multi-lateral interventions in Somali, Al-Shabaab has continuously threatened to target countries such as Kenya for their role in peacebuilding operations. As a result, a number of high profile terrorist attacks have occurred in Kenya and beyond. Al-Shabaab is connected to the mobile money ecosystem given that in the past it has "outlawed" mobile money transactions in territories under its control. Al-

Shabaab notably outlawed mobile money services in 2010, arguing it might funnel money to the Transitional Federal Government and could expose Somalia to interference by Western countries, through the international partners of Somali telecommunications firms. Some observers believed the ban was intended to block a rival to the traditional hawala companies, which Al-Shabaab could influence or tax more easily. More recently in 2014, Al-Shabaab again threatened mobile money providers. As a result, MNOs are supposedly under regular pressure from Al-Shabaab group. Discussion have been initiated with Al-Shabaab through mediation[113] into a number of these issues.

Available data suggests that there is currently perceived to be limited use of mobile money services in order for terrorist organizations to facilitate their activities with the notable exception of countries in the EAPCCO region. It is of particular note that this is the region in which Al-Shabaab operates. Despite this, there remains a likelihood that as the expansion of mobile money services continues across Africa and interoperability enables wider usage, terrorists will be granted increased opportunities to use mobile money facilities to enable their activities. As mobile money services develop in Nigeria, Ethiopia and Egypt, all of whom have faced challenges concerning terrorism, it is highly likely terrorist organizations will seek to exploit opportunities from this.

An example of such an opportunity includes sympathetic users transferring their mobile phones to members of terrorist organizations. Terrorists can use third party mobile phones to transfer/receive funds to/from other co-conspirators. Third party phones are less likely to be monitored by authorities than those belonging to designated persons. Due to the significant harm posed by terrorist groups and the opportunities presented by mobile money services, diligence from law enforcement and security services will continue to be required.

6. Law enforcement capacity to investigate and fight mobile money abuses

This report has considered law enforcement agencies capacity to fight and investigate mobile money crime in light of their collaborative work with the mobile money industry. Overall, data indicate that efforts are being made to address the threat posed by this form of criminality. There are considerable challenges for law enforcement agencies in working in an interoperable manner with the mobile services industry. However police stakeholders indicate that these are being addressed.

Data indicates that criminal justice proceedings against individuals involved in mobile money related crime has had a marked increase in conviction rates.

Despite successes there appears to be a distinct difference between the regions regarding overall success rates. Data indicates that member countries across Africa have adopted measures to increase awareness of the risk of criminality related to mobile money services and in the majority of cases have some form of framework for cooperating with private industry to secure evidence.

The key challenges in policing mobile money crime relate to identifying and locating offenders. Police stakeholders indicated that in some cases the technical expertise and equipment required to complete investigations prove difficult to integrate into the court process and support the prosecution of offenders.

Conclusion

This assessment explores how the expanding mobile money services industry in Africa has offered criminals the opportunity to exploit weaknesses in security and regulation implementation in order to commit fraud and enable other offences. While mobile money has initially concentrated in East Africa, it has spread to all African countries. As of September 2019, there were 153 active mobile money service providers operating in 45 African countries with peer-to-peer transfers representing the most common use of mobile payment services. This gives clear indications of the expanding significance of mobile money services in Africa and the extent to which they offer criminals an opportunity to exploit these services.

In the case of fraud, the complex structure of mobile money services, with distinct actors, offers criminals access to personal data and control systems enabling this form of criminality. The enforcement of regulations aimed at controlling the activities of agents and other 'insider' actors has been insufficient in mitigating the risk of fraud. It is highly likely the prevalence of fraud will continue to grow as mobile money services expand across Africa, enabled by developments in services interoperability and expansion into new markets.

Non fraud criminal exploitation of mobile money services is enabled by the weakness of individual identification systems, the lack of consumer awareness and the lack of resources / training of law enforcement agencies when it comes to collecting and presenting evidence in the criminal justice system. Concerning regulations it has been indicated that the ability of criminals to exploit 'loopholes' and maintain anonymity, creates a significant hurdle for law enforcement in investigating cases when mobile money services have been exploited. Further to this, several African countries indicated their regulations do not provide requirements for the level of identification necessary for mobile money users to register. This emphasises the challenges of regulation within systems that have weak national ID registration regimes and has been exploited in criminal activities ranging from terrorism and money laundering to extortion and drugs trafficking.

Criminal syndicates and terrorist organizations operating in Africa have the opportunity to continue exploiting mobile money services for criminal gain. This will expand as mobile money services technology increases and establishes increased transnational relevance as services move towards interoperability. If left uncontrolled by law enforcement, this will increase the level of harm such groups can inflict on members of society attempting to increase their access to financial services, as well as on state security. Law enforcement will be required to develop their technical expertise in mobile money services in order to ensure best practice evidence collection and support the application of this in criminal justice proceedings to ensure convictions.

The findings of this ENACT report have been given prominence by the current Covid-19 pandemic. Within African member countries mobile money operators have been encouraged to decrease or remove the costs associated with low level financial transactions in order to combat the spread of the Covid-19 virus through physical cash. Whilst this has clear benefits for public health it increases the social reliance on mobile money in Africa, exposes an increasing numbers of people to mobile money, furthers the proliferation of such services to new member countries and as such could offer organized criminals greater numbers of potential victims. These circumstances further increase the need of member countries to address the criminal opportunities presented by the use of mobile money services.

APPENDIX 1 - Analysis of mobile money transactions and balance limits regulations per region

In the CAPCCO region, there is a great coherence as regards the transaction and balance limits. This is due to the centralizing role of the BEAC which set up rules pertaining to mobile money for all Central Africa countries. Only the DRC, which is not part of the BEAC but is a member of CAPCCO, stands out with limits that differ from other countries in the zone.

Region	Country	Entry account single transaction limits	Top account single transaction limits	Entry account monthly transaction limits	Top account monthly transaction limits	Entry account balance limits	Top account balance limits
CAPCCO	Cameroon	79	56	87	55	68	47
CAPCCO	Chad	77	53	85	53	66	44
CAPCCO	Republic of Congo	75	51	83	51	63	41
CAPCCO	Equatorial Guinea	74	50	83	51	63	40
CAPCCO	Gabon	73	49	82	50	62	39
CAPCCO	Central African Republic	70	45	79	48	58	34
CAPCCO	Democratic Republic of Congo	41	38	51	62	79	60

Illustration of transaction and balance limits in Central Africa

The WAPCCO region as well has a high level of convergence between countries in terms of transaction and balance limits. Here too, we can see the integrative effect of BCEAO for countries under its authority. Ghana, Liberia, Mauritania and Nigeria who are not part of the BCEAO have different profiles. Mauritania stands out due to the lack of regulation pertaining to transactions or balance limits. Indeed, the country has not yet enacted a specific regulatory framework governing the provision of mobile money services. See also section “Mobile money regulatory frameworks in Africa/Market authorisation.”

Region	Country	Entry account single transaction limits	Top account single transaction limits	Entry account monthly transaction limits	Top account monthly transaction limits	Entry account balance limits	Top account balance limits
WAPCCO	Mauritania	101	101	101	101	101	101
WAPCCO	Ghana	100	100	37	41	41	71
WAPCCO	Sierra Leone	100	100	100	100	34	4
WAPCCO	Burkina Faso	90	68	75	44	80	62
WAPCCO	Mali	90	68	75	44	80	62
WAPCCO	Niger	90	68	75	44	80	62
WAPCCO	Benin	90	68	74	44	80	62
WAPCCO	Togo	89	67	74	43	79	61
WAPCCO	Côte d'Ivoire	89	67	74	43	79	61
WAPCCO	Senegal	89	67	74	43	79	61
WAPCCO	Guinea Bissau	88	67	73	43	79	60
WAPCCO	Gambia	68	43	52	24	56	32
WAPCCO	Nigeria	47	92	58	79	60	100
WAPCCO	Liberia	31	0	39	38	50	68

Illustration of transaction and balance limits in Western Africa

There is no regional regulator in the EAPCCO zone and this results in a quite diverse landscape in terms of transactions and balance limits. A country like Uganda stands out with high transaction and balance limits expressed in USD PPP for entry and top tier accounts. This may be due to the fact that MMOs in Uganda operate in the framework of a regulatory sandbox, pending a formal regulatory framework. See also section “Mobile money regulatory frameworks in Africa/Market authorisation.”

Region	Country	Entry account single transaction limits	Top account single transaction limits	Entry account monthly transaction limits	Top account monthly transaction limits	Entry account balance limits	Top account balance limits
EAPCCO	Seychelles	100	100	43	100	20	100
EAPCCO	Uganda	100	100	100	100	100	100
EAPCCO	Ethiopia	93	83	100	73	84	80
EAPCCO	Rwanda	66	52	84	60	65	66
EAPCCO	Kenya	65	39	65	36	58	34
EAPCCO	Tanzania	62	73	72	84	60	99
EAPCCO	Burundi	33	39	75	44	17	27

Illustration of transaction and balance limits in Eastern Africa

Like the EAPCCO region, the SARPCCO region also does not have a regional regulator and this translates, similarly, into a diversity of practices as regards transaction and balance limitations. Two countries, Angola and Namibia noticeably have the highest ceilings across the board.

Region	Country	Entry account single transaction limits	Top account single transaction limits	Entry account monthly transaction limits	Top account monthly transaction limits	Entry account balance limits	Top account balance limits
SARPCCO	Angola	100	100	100	100	100	100
SARPCCO	Lesotho	100	100	33	15	100	100
SARPCCO	Malawi	100	100	41	49	60	50
SARPCCO	Namibia	100	100	100	100	100	100
SARPCCO	Seychelles	100	100	43	100	20	100
SARPCCO	Madagascar	83	60	91	58	73	53
SARPCCO	Zambia	73	100	82	85	62	100
SARPCCO	Mozambique	63	37	73	42	50	25
SARPCCO	Tanzania	62	73	72	84	60	99
SARPCCO	Zimbabwe	59	33	49	22	57	33
SARPCCO	South Africa	56	100	44	18	43	16
SARPCCO	Eswatini	56	58	66	100	100	100
SARPCCO	Botswana	56	100	100	100	42	15
SARPCCO	Democratic Republic of Congo	41	38	51	62	79	60

Illustration of transaction and balance limits in Southern Africa

Finally, among the three North African countries for which data is available in the GSMA Mobile Money Metrics dataset, Tunisia has the highest ceilings across the board, while Egypt presents a more cautious approach as regards monthly transaction limits and accounts balance limits.

Region	Country	Entry account single transaction limits	Top account single transaction limits	Entry account monthly transaction limits	Top account monthly transaction limits	Entry account balance limits	Top account balance limits
North Africa	Morocco	100	80	100	100	101	50
North Africa	Egypt	100	100	63	34	66	45
North Africa	Tunisia	100	100	100	100	100	100

Illustration of transaction and balance limits in North Africa

It is important to note that in countries where customers can have more than one mobile money account with the same MMO, it is the cumulative amount of transactions or account balances that cannot exceed the applicable ceilings. Some mobile money account holders may nevertheless try to circumvent ceilings deemed too restrictive by opening mobile money accounts with different MMOs.

APPENDIX 2 - Financial action task force on money laundering country consolidated assessment ratings published in February 2020:

List of FATF's 11 measured "immediate outcomes" to assess effectiveness of AML/CTF frameworks[114]

"Immediate Outcomes" are 11 key goals identified by the FATF that an effective AML/CTF framework should achieve. These key goals or 'immediate outcomes' are organized by thematic targets. During its mutual evaluations, the FATF through its nine FATF Style Regional Bodies (FSRBs), assesses the effectiveness of a country's efforts against each of these 11 "immediate outcomes." The figure above presents the list of the 11 measured "Immediate outcomes."

References

[1] World Bank Group, 'The Global Findex Database 2017', Asli Demirgüç-Kunt, Leora Klapper, Dorothe Singer, Saniya Ansar, Jake Hess, 2018, https://globalfindex.worldbank.org/#about_focus (accessed: 23/12/2019).
[2] GSMA, 'Mobile money: Methodology for Assessing Money Laundering and Terrorist Financing Risks', Marina Solin and Andrew Zerzan, January 2010, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/03/amlfinal35.pdf (accessed: 15/10/2019).
[3] World Bank Group, 'Risk management in Mobile money: Observed Risks and Proposed Mitigants for Mobile money Operators', Andrew James Lake, 1 November 2013, http://documents.worldbank.org/curated/en/155161501149762325/Risk-management-in-mobile-money-observed-risks-and-proposed-mitigants-for-mobile-money-operators (accessed: 03/12/2019).
[4] UNCTAD, *Mobile money for Business Development in the East African Community. A Comparative Study of Existing Platforms and Regulations*, UNCTAD, 8 June 2012, https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=139 (accessed: 03/12/2019) & World Bank Group, 'Risk management in Mobile Money: Observed Risks and Proposed Mitigants for Mobile Money Operators', 01 November 2013, Andrew James Lake, http://documents.worldbank.org/curated/en/155161501149762325/Risk-management-in-mobile-money-observed-risks-and-proposed-mitigants-for-mobile-money-operators (accessed: 03/12/2019).
[5] SUBEX, 'Preventing Mobile money Frauds with Appropriate Countermeasures', SUBEX, 17 August 2017, https://info.subex.com/preventing-mobile-money-frauds-with-appropriate-countermeasures (accessed: 13/01/2020) & GSMA, 'Enabling Mobile money Policies in Kenya: Fostering a Digital Financial Revolution', Brian Muthiora, 01 January 2015, http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2015/02/2015_MMU_Enabling-Mobile-Money-Policies-in-Kenya.pdf (accessed: 06/01/2020).
[6] As per GSMA definition, this refers to domestic transfers that were made between two customer accounts including Over The Counter (OTC) transactions, off-net/cross-net transfers, bank account-to-mobile money account transfers, and mobile money-to-bank account transfers.
[7] GSMA Mobile money Metrics, The full dataset is available at: https://www.gsma.com/mobilemoneymetrics/#global?y=2018?v=overview?g=global, (accessed: 27/09/2019).
[8] The Consultative Group to Assist the Poor (CGAP), 'Wallet and OTC Transactions: Understanding financial incentives', William Cook and Naeha Rashid, 28 August 2017,https://www.cgap.org/research/slide-deck/wallet-and-over-counter-transactions-understanding-financial-incentives (accessed: 15/10/2019).
[9] World Cocoa Foundation (WCF), *Mobile money Market Study for the World Cocoa Foundation*, WCF, 01 October 2015, http://www.worldcocoafoundation.org/wp-content/uploads/files_mf/1476454396WS5_SIAWCFMobileMoneyStudy11302015.pdf (accessed: 06/12/2019).
[10] CGAP, 'Wallet and OTC Transactions: Understanding financial incentives', William Cook and Naeha Rashid, 28 August 2017, https://www.cgap.org/research/slide-deck/wallet-and-over-counter-transactions-understanding-financial-incentives (accessed: 15/10/2019).
[11] *Ibid.* (accessed: 15/10/2019).
[12] Telecom Regulatory Authority of India, 'Telecom Regulatory Authority of India. Consultation Paper on USSD-based Mobile Banking Services for Financial Inclusion', 20 September 2013. https://main.trai.gov.in/sites/default/files/CP_Mobile_Banking_20.09.2013_0.pdf (accessed: 09/01/2020).
[13] GSMA, *2018 State of the Industry Report on Mobile money*, GSMA, 2019, https://www.gsma.com/r/state-of-the-industry-report/ (accessed: 03/04/2019).
[14] Service offered in 10 African countries. Airtel, ' Airtel Money Favorites and Self Transaction Reversal', Airtel, 01 May 2019, https://www.comviva.com/wp-content/uploads/2019/05/Airtel-Money-favorites-and-self-transaction-reversal.pdf (accessed: 10/01/2020).
[15] Sokoine University of Agriculture (SUA), Tanzania, 'Security Perspectives For USSD Versus SMS In Conducting Mobile Transactions: A Case Study Of Tanzania', Baraka Willy, 22 October2013. https://www.researchgate.net/publication/260392872_Security_Perspectives_For_USSD_Versus_SMS_In_Conducting_Mobile_Transactions_A_Case_Study_Of_Tanzania (accessed: 15/01/2020).
[16] *Ibid*.
[17] GSMA, 'The Mobile Economy 2019', GSMA, 19 February 2019, https://www.gsma.com/r/mobileeconomy/ (accessed: 16/01/2020).
[18] GSMA, 'The Mobile Economy Sub-Saharan Africa 2019', GSMA, 10 July 2019, https://www.gsma.com/r/mobileeconomy/sub-saharan-africa/ (accessed: 16/01/2020).
[19] GSMA, *SS7 Vulnerabilities and attack exposure report 2018*, GSMA, 28 February 2018, https://www.gsma.com/membership/resources/ss7-vulnerabilities-and-attack-exposure-report-2018/ (accessed: 17/01/2020).
[20] Wikipedia, https://en.wikipedia.org/wiki/Consumer_protection, (accessed: 16/01/2020).
[21] *Methodology: To measure the level of protection enjoyed by mobile money consumers, the GSMA, in its mobile money metrics dataset, set up a country ranking matrix in which 25 points are awarded are for each of the following that apply:*

(i) There are consumer protection rules in the mobile money regulatory framework;

(ii) The customer protection rules in the mobile money regulatory framework require that customers are granted access to recourse and complaint procedures in order to resolve disputes;

(iii) *The customer protection rules in the mobile money regulatory framework require price disclosures for mobile money transactions;*

(iv) *The customer protection rules in the mobile money regulatory framework provide a general disclosure requirement to make the terms of the service available to customers.*

Data pertaining to African countries was extracted from global datasets and a total of points was calculated for each country. In Figure 7 above, a total of 100 is translated as "Strong." A total of 75 is translated as "Advanced." A total of 50 is translated as "Intermediate." A total of 25 is translated as "Weak" and a total of 0 is translated as "Non-existent."

[22] Prudential regulation is a type of financial regulation that requires financial firms to control risks and hold adequate capital as defined by capital requirements, liquidity requirements, by the imposition of concentration risk (or large exposures) limits, and by related reporting and public disclosure requirements and supervisory controls and processes. Wikipedia https://en.wikipedia.org/wiki/Prudential_regulation.

[23] GSMA, 'Safeguarding Mobile Money: How providers and regulators can ensure that customer funds are protected', GSMA, 07 January 2016 , https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/01/2016_GSMA_Safeguarding-Mobile-Money_How-providers-and-regulators-can-ensure-that-customer-funds-are-protected.pdf (accessed: 17/01/2020).

[24] Regions as per INTERPOL breakdown on the basis of regional Police Chiefs Cooperation Organizations.

[25] GSMA Mobile money Metrics, The full dataset is available at: https://www.gsma.com/mobilemoneymetrics/#global?y=2018?v=overview?g=global, (accessed: 27/09/2019).

[26] Total exceeding 153 MMO as some countries are at the same time member of several Police Chiefs Cooperation Organizations i.e Democratic Republic of Congo, Seychelles, Tanzania.

[27] GSMA, '2018 State of the Industry Report on Mobile money', GSMA, 2019, (accessed: 03/04/2019).

[28] Estimate based on quarterly transaction values reported in the GSMA Mobile money Metrics, https://www.gsma.com/mobilemoneymetrics/#global?y=2018?v=overview?g=global, (accessed: 27/09/2019).

[29] *Ibid*.

[30] M. Panara, 'Mobile money: quel chemin depuis M-PESA au Kenya', *Le Point*, 23 December 2018, https://www.lepoint.fr/economie/mobile-money-quel-chemin-depuis-M-PESA-au-kenya-23-12-2018-2281578_28.php (accessed: 14/05/2019).

[31] GSMA, *2018 State of the Industry Report on Mobile Money*, 2019, GSMA, https://www.gsma.com/r/state-of-the-industry-report/ (accessed: 03/05/2019).

[32] In this figure GSMA regional designation are used instead of INTERPOL's, because the used dataset presented the figures in a regionalized and not a country base manner. Nonetheless, GSMA and INTERPOL's regional membership mostly overlap.

[33] As per GSMA definition, this refers to domestic transfers that were made between two customer accounts including Over the Counter (OTC) transactions, off-net/cross-net transfers, bank account-to-mobile money account transfers, and mobile money-to-bank account transfers.
GSMA, *2018 State of the Industry Report on Mobile Money*, 2019, GSMA, https://www.gsma.com/r/state-of-the-industry-report/ (accessed: 03/05/2019).

[34] CIA, The World Factbook country profiles, CIA, https://www.cia.gov/library/publications/the-world-factbook/docs/profileguide.html.

[35] *Ibid.*

[36] GSMA, *2018 State of the Industry Report on Mobile money*, GSMA, 2019, (accessed: 03/04/2019).

[37] Morocco: 37.9per cent, Algeria: 29.1per cent, Egypt: 28per cent. Average = (37.9+29.1+28)/3=31.66per cent. Date source: https://en.wikipedia.org/wiki/List_of_countries_by_smartphone_penetration#cite_note-:0-1, (accessed: 03/04/2019).

[38] GSMA, *2018 State of the Industry Report on Mobile mone*y, GSMA, 2019, (accessed: 03/04/2019).

[39] A regulatory sandbox is a framework set up by a financial sector regulator to allow small scale, live testing of innovations by private firms in a controlled environment (operating under a special exemption, allowance, or other limited, time-bound exception) under the regulator's supervision. The purpose of a regulatory sandbox is to adapt compliance with strict financial regulations to the growth and pace of the most innovative companies, in a way that does not smother the fintech sector with rules, but also does not diminish consumer protection.
CGAP, *Regulatory Sandboxes and Financial Inclusion*, I. Jenik and K. Lauer, 2017, https://www.cgap.org/sites/default/files/Working-Paper-Regulatory-Sandboxes-Oct-2017.pdf, (accessed: 14/10/ 2019) & BBVA, 'What is a regulatory sandbox?', BBVA, 2017, https://www.bbva.com/en/what-is-regulatory-sandbox/ (accessed: 14/10/2019)

[40] World Bank Group, *The state of identification systems in Africa. A synthesis of Country Assessments*, World Bank Group, 2017, (accessed: 15/10/2019).

[41] *Ibid.*

[42] GSMA, 'Explore the growth of the mobile money industry through this comprehensive set of global metrics', Mobile money Metrics, https://www.gsma.com/mobilemoneymetrics/#global?y=2018?v=overview?g=global (accessed: 27/09/2019).

[43] *Ibid.*

[44] GSMA, 'The Mobile Money Regulatory Index 2019', February 2019, Kalvin Bahia and Brian Muthiora, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/03/The-Mobile-Money-Regulatory-Index-1.pdf (accessed: 04/12/2019).

[45] The Bank of Central African States (French: Banque des États de l'Afrique Centrale, BEAC) is a central bank that serves six central African countries which form the Economic and Monetary Community of Central Africa. These countries are: Cameroon, Central African Republic, Chad, Equatorial Guinea, Gabon and Republic of the Congo.

Wikipedia: https://en.wikipedia.org/wiki/Bank_of_Central_African_States, (accessed: 27/01/2020).
[46] The Central Bank of West African States (French: Banque Centrale des États de l'Afrique de l'Ouest, BCEAO) is a central bank serving the eight west African countries which share the common West African CFA franc currency and comprise the West African Economic and Monetary Union (UEMOA). These countries are: Benin, Burkina Faso, Guinea-Bissau, Ivory Coast, Mali, Niger, Senegal and Togo.
Wikipedia: https://en.wikipedia.org/wiki/Central_Bank_of_West_African_States, (accessed: 27/01/2020).
[47] Centre for Financial Regulation & Inclusion (CENFRI), 'Payment systems in sub-Saharan Africa, Note 2: Case studies of National and Regional payment systems market development', 21/12/2018, Barry Cooper, Christine Hougaard, Laura Munoz Perez, Christiaan Loots, Rose Tuyeni Peter, Matthew Ferreira, Matthew Dunn, https://cenfri.org/wp-content/uploads/2018/12/Payment-systems-in-SSA-Note-2.pdf (accessed: 27/01/2020).
[48] Central Bank of Ghana, 'Bank of Ghana - Guidelines for E-Money Issuers in Ghana', 06/07/2015, https://www.bog.gov.gh/privatecontent/Banking/E-MONEYper cent20GUIDELINES-29-06-2015-UPDATED5.pdf (accessed: 27/01/2020).
[49] 'Business deals push Kenya's mobile money accounts to 45m', Business Daily Africa, 17/12/2018, https://www.businessdailyafrica.com/markets/marketnews/Business-deals-push-mobile-money-accounts-to-45m/3815534-4898484-nbhccyz/index.html (accessed: 27/01/2020).
[50] BCEAO, 'Instruction N°008-05-2015 Régissant Les Conditions Et Modalités D'Exercice Des Activités Des Emetteurs De Monnaie Electronique Dans Les Etats Membres De L'Union Monétaire Ouest Africaine (UMOA)', 31/07/2015, https://www.bceao.int/sites/default/files/2017-11/instruction_no008_05_2015_intranet.pdf (accessed: 24/01/2020).
[51] Groupe d'Action contre le blanchiment d'Argent en Afrique Centrale (GABAC), 'Les nouveaux moyens de paiement face aux défis de la lutte anti blanchiment et contre le financement du terrorisme dans la zone CEMAC', 01/08/2017, http://spgabac.org/site/wp-content/uploads/2016/09/les_NMP_face_aux_defis_de_la_LAB_CFT.pdf (accessed: 23/01/2020).
[52] Conversion in USD as of 25/01/2020. Service used: Xe.com.
[53] Purchasing power parities (PPPs) are the rates of currency conversion that try to equalize the purchasing power of different currencies, by eliminating the differences in price levels between countries. Source: OECD https://data.oecd.org/conversion/purchasing-power-parities-ppp.htm.
[54] GSMA Mobile money Metrics https://www.gsma.com/mobilemoneymetrics/#global?y=2018?v=overview?g=global (accessed: 27/09/2019) & GSMA, 'The Mobile Money Regulatory Index 2019', February 2019, Kalvin Bahia and Brian Muthiora, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/03/The-Mobile-Money-Regulatory-Index-1.pdf (accessed: 04/12/2019).
[55] GSMA, 'Guidelines on International Remittances through Mobile Money', GSMA, 18 October 2017, https://gsma.com/mobilefordevelopment/wp-content/uploads/2017/09/GSMA_September_2017_Guidelines_On_International_Remittances_Through_Mobile_Money.pdf (accessed: 10/02/2020).
[56] GSMA, '2016 State of Mobile Money in West Africa', GSMA, 23 May 2017, ,http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/05/2016-State-of-Mobile-Money-in-Western-Africa.pdf (accessed: 10/02/2020).
[57] GSMA, 'Mobile money, Competing with informal channels to accelerate the digitisation of remittances', GSMA, 16 May 2018, https://gsma.com/mobilefordevelopment/wp-content/uploads/2018/05/Mobile_Money_Competing_with_informal_channels_to_accelerate_the_digitisation_of_remittances.pdf (accessed: 10/02/2020) & GSMA, 'Driving a price revolution. Mobile money in international remittances', GSMA, 28 October 2016, https://www.gsmaintelligence.com/research/?file=8F31B31705C20A63A41DB9711BF84C25&download (accessed: 10/02/2020) & GSMA, '2016 State of Mobile Money in West Africa', GSMA, 23 May 2017, http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/05/2016-State-of-Mobile-Money-in-Western-Africa.pdf (accessed: 10/02/2020).
[58] *Ibid.*
[59] Alliance for Financial Inclusion. Mobile Financial Services Working Group (MFSWG). 'Mobile Financial Services. Mobile-Enabled Cross-Border Payments', 02/09/2014, https://www.afi-global.org/sites/default/files/publications/mfswg_guideline_note_no_14_en9-2.pdf (accessed: 03/12/2019).
[60] FATF, *Consolidated assessment ratings*, https://www.fatf-gafi.org/publications/mutualevaluations/documents/assessment-ratings.html, (accessed: 15/10/2019).
[61] FATF, *Money Laundering Using New Payment Methods, FATF, October* 2010, http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf, (accessed: 15/10/2019).
[62] GSMA, 'Mobile money: Methodology for Assessing Money Laundering and Terrorist Financing Risks', GSMA, Marina Solin and Andrew Zerzan, January 2010, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/03/amlfinal35.pdf (accessed: 15/10/2019).
[63] USAID, 'Better Than Cash: Kenya Mobile Money Market Assessment'; USAID, November 2011, https://solutionscenter.nethope.org/assets/collaterals/Kenya-Mobile-Money-Assessment.pdf
[64] Consult Hyperion and FSDAfrica, 'Fraud Risk Management for Mobile Money: An Overview, S. Lonie', August 2017, https://www.chyp.com/wp-content/uploads/2018/06/Fraud-Risk-Management-for-MM-31.07.2017.pdf (accessed: 22/01/2020) and Microsave, 'Fraud in Mobile Financial Services', J. Luminzu Mudiri, 26 November 2012, https://www.microsave.net/files/pdf/RP151_Fraud_in_Mobile_Financial_Services_JMudiri.pdf (accessed: 22/01/2020).

[65] GSMA, 'Managing the Risk of Fraud in Mobile money', L. Gilman and M. Joyce, 01 October 2012, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/10/2012_MMU_Managing-the-risk-of-fraud-in-mobile-money.pdf. (accessed: 30/07/2019).
[66] A PayBill account is an account provided by Safaricom that can receive payments from M-PESA.
[67] Consult Hyperion and FSDAfrica, 'Fraud Risk Management for Mobile Money: An Overview, S. Lonie', August 2017, https://www.chyp.com/wp-content/uploads/2018/06/Fraud-Risk-Management-for-MM-31.07.2017.pdf (accessed: 22/01/2020).
[68] FATF, *Money Laundering Using New Payment Methods, FATF, October* 2010, https://www.fatf-gafi.org/media/fatf/documents/reports/MLper cent20usingper cent20Newper cent20Paymentper cent20Methods.pdf
[69] INTERPOL, *Project ENACT: Overview of Serious and Organized Crime* in Africa, *INTERPOL*, public version, October 2018.
[70] *Ibid.*
[71] F. Warom Okello, 'Mairungi: A banned drug flourishing in Arua', 4 August, 2016, *Daily Monitor* https://www.monitor.co.ug/artsculture/Reviews/Mairungi--A-banned---drug-flourishing--in-Arua-/691232-3329374-76rqihz/index.html, (accessed: 09/04/2020).
[72] *Ibid.* (accessed: 09/04/2020).
[73] L. Salm Reifferscheidt, 'Doing the 'tramadol dance': what this latest craze says about pill addition', 16August 2019, *Mail and Guardian*, https://mg.co.za/article/2019-08-16-00-doing-the-tramadol-dance-what-this-latest-craze-says-about-pill-addiction/ (accessed: 6/04/2020).
[74] *Ibid.*
[75] INTERPOL, *Project ENACT: Overview of Serious and Organized Crime* in Africa, *INTERPOL public version*
[76]P. Redfern, 'Stolen luxury cars find new owners in East Africa', 8 September 2015, *The East African*, https://www.theeastafrican.co.ke/news/ea/Stolen-luxury-cars-find-new-owners-in-East-Africa/4552908-2862588-nf1fqqz/index.html, (accessed: 22/03/2020).
[77] INTERPOL, *Project ENACT: Overview of Serious and Organized Crime* in Africa, *INTERPOL public version.*
[78] T. Sherman, 'Illicit cargo: Why are more stolen cars disappearing overseas', 19 October 2014, updated 29 March 2019, NJ Advance media, https://www.nj.com/news/2014/10/illicit_cargo_why_are_more_stolen_cars_disappearing_overseas.html, (accessed: 23/03/2020).
[79] T. Sherman, 'International luxury car theft ring busted in Newark, 19 arrested', 24 May 2012 updated 30 march 2019, NJ Advance media, https://www.nj.com/news/2012/05/international_high-end_car_the.html, (accessed: 22/03/2020).
[80] T. Sherman, 'Illicit cargo: Why are more stolen cars disappearing overseas', 19 October 2014, updated 29 March 2019, NJ Advance media, https://www.nj.com/news/2014/10/illicit_cargo_why_are_more_stolen_cars_disappearing_overseas.html, (accessed: 23/03/2020).
[81] L. SHiundu, 'Six High end cars stolen from UK, South Africa impounded Kenya', *Tuko*, https://www.tuko.co.ke/316510-six-high-cars-stolen-uk-south-africa-impounded-kenya.html, (accessed: 24/03/2020).
[82] INTERPOL, *Project ENACT: Overview of Serious and Organized Crime* in Africa, *INTERPOL* public version.
[83] M. Schroeder and G Lamb, 'The illicit arms trade in Africa, A global enterprise', June 2006 https://fas.org/asmp/library/articles/SchroederLamb.pdf, (accessed: 23/03/2020).
[84] Ineke Mules, 'Stemming the flow of illicit arms in Africa', 26 July 2019, DW, https://www.dw.com/en/stemming-the-flow-of-illicit-arms-in-africa/a-49761552, (accessed: 21/03/2020).
[85] M. Schroeder and G Lamb, 'The illicit arms trade in Africa, A global enterprise', June 2006 https://fas.org/asmp/library/articles/SchroederLamb.pdf, (accessed: 23/03/2020).
[86] Ineke Mules, 'Stemming the flow of illicit arms in Africa', 26 July 2019, DW, https://www.dw.com/en/stemming-the-flow-of-illicit-arms-in-africa/a-49761552, (accessed: 21/03/2020).
[87] M. Schroeder and G Lamb, 'The illicit arms trade in Africa, A global enterprise', June 2006 https://fas.org/asmp/library/articles/SchroederLamb.pdf, (accessed: 23/03/2020).
[88] *Ibid.*
[89] M. Fleshman, 'Small arms in Africa', December 2011, *Africa Renewal,* https://www.un.org/africarenewal/magazine/december-2011/small-arms-africa, (accessed: 25/03/2020).
[90] D. A. Williams & P. L. Billon (ed.), 'Corruption, natural resources and development: From resource curse to political ecology', Cheltenham, Northampton, *Edward Elgar Publishing*, 2017.
[91] W. Lehmacher, 'Wildlife crime: a $23 billion trade that's destroying our planet', *World Economic Forum*, https://www.weforum.org/agenda/2016/09/fighting-illegal-wildlife-and-forest-trade/, (accessed: 22/03/2020).
[92] INTERPOL, *Project ENACT: Serious and Organized Crime in the Northern Africa Region*, *INTERPOL*, public version, August 2018.
[93] International Chamber of Commerce, 'Global impacts of counterfeiting and piracy to reach US$4.2 trillion by 2022', ICC, 6 February 2017, https://iccwbo.org/media-wall/news-speeches/global-impacts-counterfeiting-piracy-reach-us4-2-trillion-2022/ (accessed: 17/09/2018).
[94] C. Walters, 'Africa Steps up Fight against Counterfeits', *Managing Intellectual Property*, March 2017, https://www.spoor.com/docs/4549/Featureper cent20Africa.pdf (accessed: 12/09/2018).
[95] S. Mchunu, 'Counterfeit goods threaten SA economy', 26 August 2018, *IOL*, https://www.iol.co.za/business-report/economy/counterfeit-goods-threaten-sa-economy-16720574, (accessed: 25/03/2020).
[96] Transparency International, *Corruption in Africa, 75 million people pay bribes,* 30 November 2015, Transparency International, https://www.transparency.org/news/feature/corruption_in_africa_75_million_people_pay_bribes, (accessed: 25/03/2020).

[97] M. Okwuagbala Uzochukwu, 'Corruption: causes and solutions', February 2020, *Soapboxie,* https://soapboxie.com/world-politics/corruption-solutionandcuses (accessed: 11/04/2020).
[98] Consult Hyperion and FSDAfrica, 'Fraud Risk Management for Mobile Money: An Overview, S. Lonie', August 2017, https://www.chyp.com/wp-content/uploads/2018/06/Fraud-Risk-Management-for-MM-31.07.2017.pdf (accessed: 22/01/2020) and Microsave, 'Fraud in Mobile Financial Services', J. Luminzu Mudiri, 26 November 2012, https://www.microsave.net/files/pdf/RP151_Fraud_in_Mobile_Financial_Services_JMudiri.pdf (accessed: 22/01/2020).
[99] Smurfing is the process of withdrawing or depositing small funds to avoid attention from regulators or law enforcement through suspicious transactions reporting schemes.
[100] INTERPOL, *ENACT Project: Overview of Serious and Organized Crime in the Central African Region*, *INTERPOL*, public version, August 2018.
[101] Stop the traffic, https://www.stopthetraffik.org/smuggling-trafficking-knowing-differences/ 20 October 2017, (accessed: 10/04/2020).
[102] INTERPOL, *Project ENACT: Overview of Serious and Organized Crime* in Africa, *INTERPOL*, public version, October 2018
[103] R. Peterson, 'Mobile money in Africa: Access, regulations and risks', 17 April 2019, DLA Piper, https://www.dlapiper.com/en/uk/insights/publications/2019/04/africa-connected-issue-2/mobile-money-in-africa/, (accessed: 12/03/2020).
[104] N. G. Miralis, 'What is the connection between Human Trafficking and Money Laundering?', 28 September 2018, Lexology, https://www.lexology.com/library/detail.aspx?g=00370da4-c982-4543-8e41-f1841495d16f (accessed: 11/03/2020).
[105] *Ibid.*
[106] P. Clegg, 'Fighting Human Trafficking by following the money', 1 February 2020, *CypherTrace* https://ciphertrace.com/fighting-human-trafficking-by-following-the-money/ (accessed: 11/03/2020).
[107] Security Alert - International SOS riskinsights@internationalsos.com Kenya: Nairobi: Abduction of foreign national underscores HIGH crime risk, 03/02/2020.
[108] Consult Hyperion and FSDAfrica, 'Fraud Risk Management for Mobile Money: An Overview, S. Lonie', August 2017, https://www.chyp.com/wp-content/uploads/2018/06/Fraud-Risk-Management-for-MM-31.07.2017.pdf (accessed: 22/01/2020) and Microsave, 'Fraud in Mobile Financial Services', J. Luminzu Mudiri, 26 November 2012, https://www.microsave.net/files/pdf/RP151_Fraud_in_Mobile_Financial_Services_JMudiri.pdf (accessed: 22/01/2020).
[109] *Ibid.*
[110] L. Kambela, 'Terrorism in Africa', Conflict Trends, 2019, ACCORD, https://www.accord.org.za/conflict-trends/terrorism-in-africa/, (accessed: 22/03/2020).
[111] *Ibid.*
[112] Institute of Diplomacy and International Studies, University of Nairobi, 'Impact of terrorism on economic development in Africa, a case study of Kenya foreign direct investment', E. Mbula Baraga, November 2016, http://erepository.uonbi.ac.ke/bitstream/handle/11295/99711/Baragaper cent20per cent20_Impactper cent20Ofper cent20Terrorismper cent20Onper cent20Economicper cent20Developmentper cent20Inper cent20Africaper cent20Aper cent20Caseper cent20Studyper cent20Ofper cent20Kenyaper cent20Foreignper cent20Directper cent20Investment.pdf?sequence=1&isAllowed=y, (accessed: 25/03/2020).
[113] Altai consulting for the World Bank, *Mobile money Ecosystem in Somalia*, April 2017, http://www.altaiconsulting.com/wp-content/uploads/2017/11/WB-MME_Final-Short-Version_20170608.pdf, (accessed: 04/12/2019).
[114] FATF, 'An effective system to combat money laundering and terrorist financing', http://www.fatf-gafi.org/publications/mutualevaluations/documents/effectiveness.html.

ABOUT INTERPOL

INTERPOL is the world's largest international police organization. Our role is to assist law enforcement agencies in our 194 member countries to combat all forms of transnational crime. We work to help police across the world meet the growing challenges of crime in the 21st century by providing a high-tech infrastructure of technical and operational support. Our services include targeted training, expert investigative support, and specialized databases and secure police communications channels.

OUR VISION: "CONNECTING POLICE FOR A SAFER WORLD"

Our vision is that of a world where each and every law enforcement professional will be able through INTERPOL to securely communicate, share and access vital police information whenever and wherever needed, ensuring the safety of the world's citizens. We constantly provide and promote innovative and cutting-edge solutions to global challenges in policing and security.

INTERPOL