EMERGING ISSUES IN DIGITAL ID PART 1

MOBILE MONEY DURING A PANDEMIC

A Use Case and Issue Brief
Prepared by CIPIT

Strathmore University
Centre for Intellectual Property and Information Technology Law

01

BACKGROUND

Mobile money allows persons to store, spend, send and receive money on their mobile phones. Mobile money services encompass: mobile transfers, mobile payments and mobile banking.[1] Mobile transfers facilitate person-to-person money transfers; mobile payments facilitate person-to-business payments and; mobile banking connects a mobile phone and a personal or business bank account allowing customers to use their mobile phones for banking services.[2] Business models for mobile money can be led by mobile network operators (MNOs), financial institutions such as banks, or collaborative efforts among them.[3]

In the wake of COVID-19, the use of contactless payments rather than banknotes and coins is being encouraged to limit the spread of COVID-19, which can survive on surfaces for certain periods. This has led some governments, regulators and mobile money providers to adopt measures that encourage the use of mobile money. These measures include: person-to-person transaction fee waivers; increasing transaction and balance limits; easier access to digital credit; support of agents; waivers on bank-to-wallet and wallet-to-bank transaction fees; waivers of interchange fees and; flexible on-boarding and Know Your Customer (KYC) procedures.[4] It may also include enablement of mobile money payments for services for which it was previously unavailable.

Digital ID plays a major role in mobile money transactions. A mobile money account is tied to a mobile phone number, and initial registration of a mobile number in most African countries (including Kenya) requires a government issued ID. Then, for each transaction done via mobile money, the collection of users' data and the generation of financial transaction data is required. The benefits and risks of this system are discussed below in the context of a global pandemic such as COVID-19.

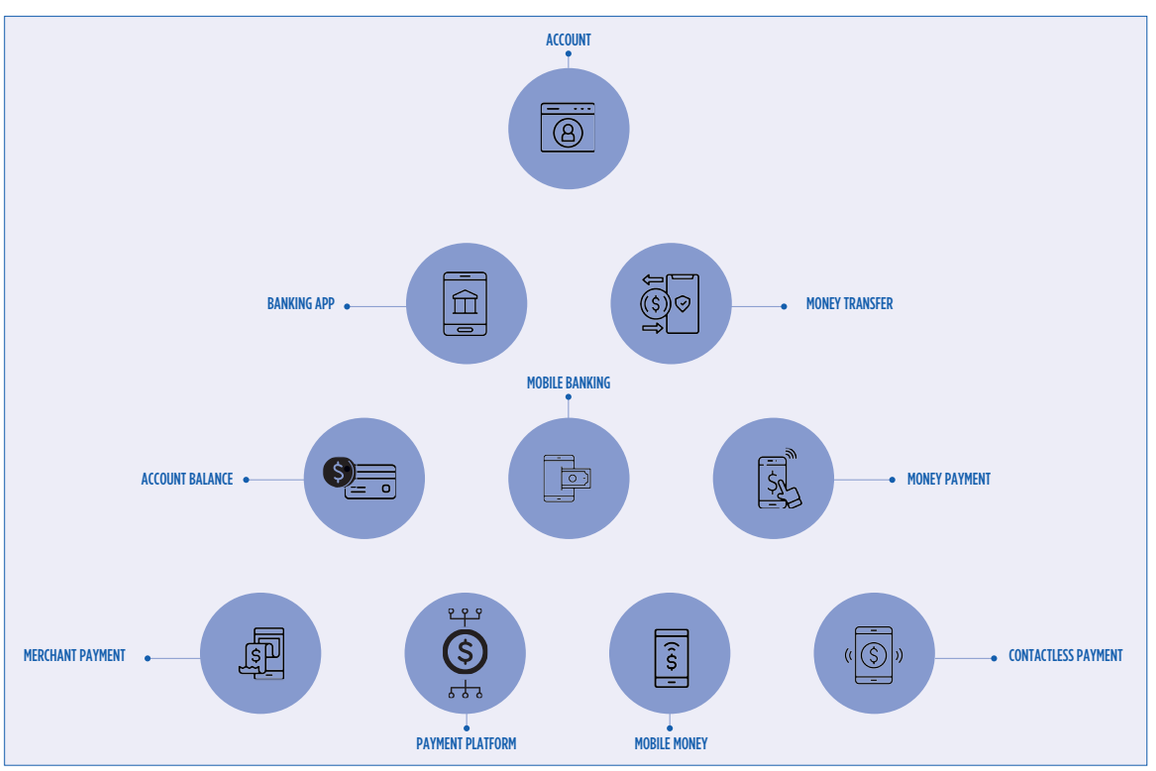


Fig1. Mobile Banking is a broad suite of interacting technologies

JUSTIFICATIONS FOR THE USE CASE

In the use case of mobile money, the issues raised for which Digital ID is a proposed solution are:

1. Reduced risk of further transmission of COVID-19 through cash to cash transactions
2. Increased access to mobile financial services
3. Promote financial inclusion among the most vulnerable segments of the society
4. Facilitate easy access to digital lending services

DATA INVOLVED IN THE USE CASE

The data collected for Digital ID with the use case of mobile money may include:

1. Identification Information
    - *a. Contact details*
    - *b. Biometric data*
    - *c. Government ID information*
2. Bank account details (if a mobile money account is linked to a bank account)
3. Data linkage to other identity databases. (e.g. links to the Credit Reference Bureau, government tax Authority, etc.)
4. Mobile money transaction data
    - *a. purchasing data*
    - *b. vendor data*
    - *c. user location data*

RISKS INVOLVED IN THE USE CASE

The risks associated with Digital ID in the use case of mobile money include:

1. Susceptibility to Identity theft
2. Risk of fraud
3. Risk of impersonation by unauthorised agents
4. Risk of abuse of customer details.
5. Manipulation of customers' financial information leading to misuse of information for criminal activity.
6. Use of financial information in a way that may compromise the right to privacy and /or other fundamental rights and freedoms.

[1] UNCTAD, 'Mobile Money for Business Development in the East African Community.'
<https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=139>

[2] Firpo J (2009) 'E-Money – Mobile Money – Mobile Banking – What's the Difference?' World Bank Blogs,
< https://blogs.worldbank.org/psd/e-money-mobile-money-mobile-banking-what-s-the-difference>

[3] Gutierrez, Eva, Choi, Tony (2014) , 'Mobile Money Services Development: The Cases of the Republic of Korea and Uganda.'<https://openknowledge.worldbank.org/handle/10986/17339>

[4] GSMA, (2020) 'Mobile Money Recommendations to Central Banks in response to COVID-19.' Mobile for Development Blog
<https://www.gsma.com/mobilefordevelopment/resources/mobile-money-recommendations-to-central-banks-in-response-to-covid-19/>

[5] GSMA, (2019) , 'Data protection in Mobile Money.'
<https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/03/Data-Protection-in-mobile-money.pdf>

[6] GSMA, (2019) , 'Data protection in Mobile Money.'
<https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/03/Data-Protection-in-mobile-money.pdf>

02

ANALYSIS

Maintaining a functioning economy remains, even in a global pandemic situation, a top priority for all countries. Developing economies have less slack to absorb economic shocks, and must make use every available resource, or else risk further economic hardship that can ultimately result in civil unrest and necessitate harsher containment measures. In some countries, including Kenya, mobile money has grown into a vital component of the flow of money through the economy. The actions taken by governments and the private sector that make mobile money easier and cheaper to use demonstrate the importance of this technology.

With an increased demand for mobile money services due to COVID-19 and the likely increase in the financial transaction data that mobile money providers handle, however, privacy and data protection concerns are increasingly important.

The collection of financial transaction data is essential in providing mobile money services. Legal justifications for collecting and processing the data include: consent, public interest, contractual obligations and legal obligations.[5] Personal data may be necessary to meet KYC requirements and anti-money laundering and counterterrorism provisions.[6]In Zambia, mobile money operators may be called upon to report violations of anti-money money laundering and financial intelligence legislation. [7]KYC requirements in the country also require an original and valid identity card for customer authentication in the process of registering SIM cards. The same applies to Kenya. In some cases, the original identity credentials must be presented for all or selected mobile money transactions, such as cash deposits and withdrawals.

Mobile money financial transactions leave a trail of data that may be misappropriated by third parties, particularly where there is regular and/or legally required sharing of data. Third parties may take advantage of financial transaction data acquired for unwelcome commercial approaches, spam and other questionable or unlawful purposes at the cost of customers' right to privacy. This may be facilitated by the absence of a clear guide in policies defining the circumstances in which third parties can get access to financial transaction data. Notably, in the East African region, no country defines who can get access to a mobile money trail, how, when, or under what criteria such access may be enabled.[8]

Additionally, vulnerabilities in the storage of financial transaction data creates risks of identity theft, fraud and financial harm which can ultimately diminish consumer trust and the growth of mobile money services.

Generally, KYC requirements, cyber protection regulations and other technical measures may guard against this. Some mobile money operators set up call centers with staff that can deal with customer queries and complaints. Other data security risks include accidental destruction, alteration, loss and unauthorised access and disclosure.

GOOD ID PRINCIPLES IN THE USE CASE

1. Secure mobile money systems, applications and networks in accordance with privacy requirements.
2. Presenting users with information about their personal data and choice and control over their data.
3. Openness, transparency and notice so that users understand how their data is used, and are able to make informed choices about whether to use a service.
4. Data Minimisation; only the minimum personal data necessary for valid business purposes should be collected, accessed or used.
5. Where data is transferred to third parties, steps to ensure the data remains protected.
6. Reducing risks through KYC capabilities, identity validation and fraud detection.
7. Accountability and compliance with applicable laws and regulations.
8. Data security organisational policies which provide appropriate plans and mechanisms in the event of breach.

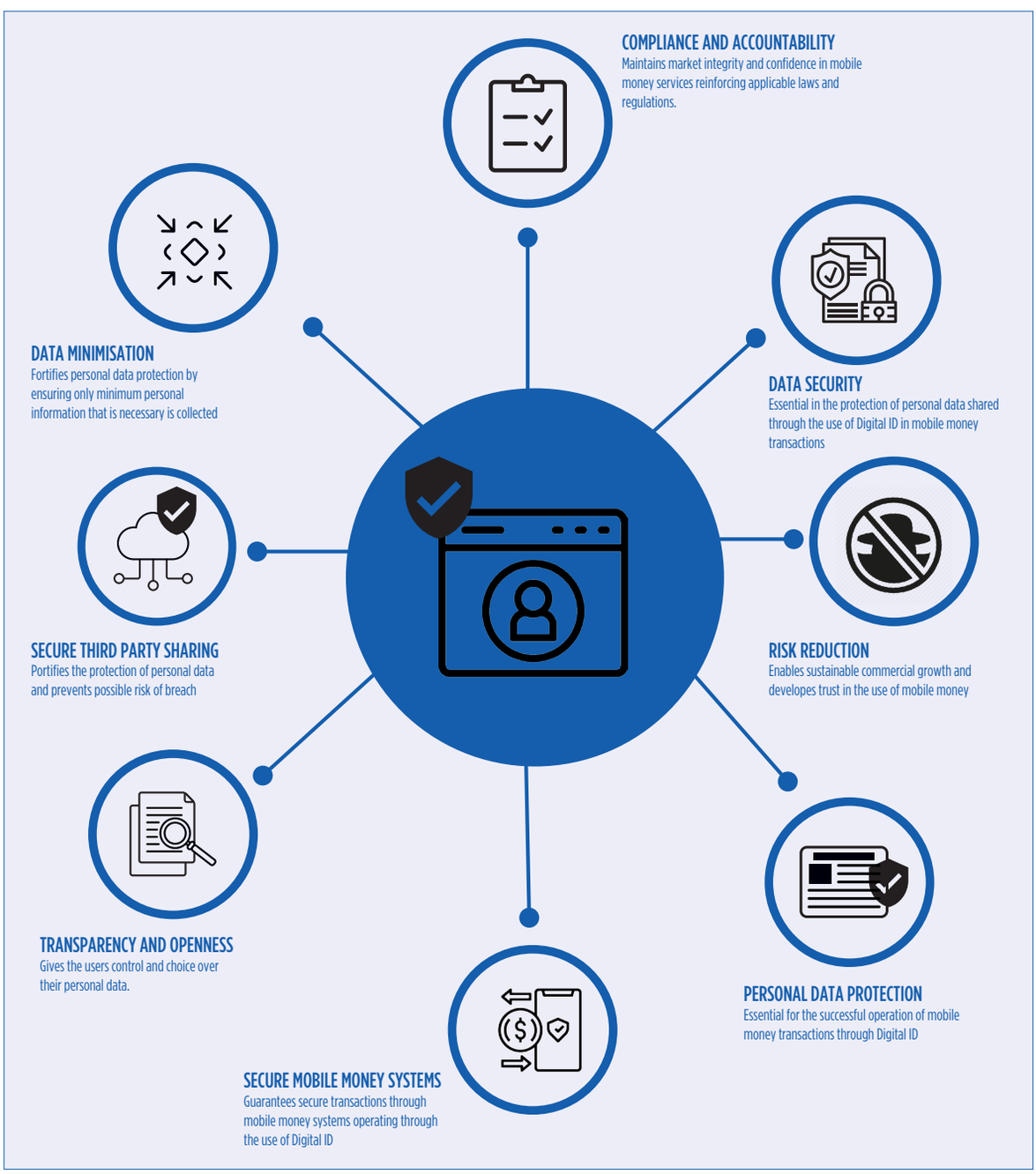


Fig2. Components of Data Protection integrated with Mobile Money

FOCUS ON: MITIGATING HARM

Where measures are in place to encourage the use of mobile money, users can take certain steps to mitigate potential harms.

1. For Users: register a separate phone number that is dedicated for mobile money activities. By keeping mobile money activities separate from other personal activities such as personal phone calls, data usage, and location data, a user can reduce the amount of centralized data that relates to the user.
    a. *Keep all business-related mobile money activities separate from personal activities, using two different mobile money accounts.*
    b. *Where registering a separate mobile money account, use a separate ID, if possible. By using different IDs, such as passports and national IDs, it becomes more difficult to link activities for a single user.*
2. For Users: monitor accounts on a regular basis. A user should check mobile money balances and account statements regularly, looking for any evidence of fraud or suspicious activity.
3. For governments: ensure an effective data protection framework is in place. An effective framework includes the legal framework as well as executive and judicial infrastructure that rigorously enables the law.
4. For governments: avoid emergency measures that take advantage of users. Mobile money transaction data will become more plentiful during a global pandemic such as COVID-19, particularly where measures have been taken to encourage its use. Use of such data must be transparent and limited.
5. For service providers: avoid data sharing except to the extent required by law. As the amount of mobile money transaction data increases, the value of that data increases. There is a great temptation to use or sell that data; use or sale of the data increases the risk of the harms mentioned above.

CONCLUSION

Mobile money offers a relatively secure alternative to cash in the fight against COVID-19. The collection, storage and sharing of customer data enhances the provision of the service and can provide an opportunity for financial inclusion. The digital ID involved is deserving of proper governance so as not to be misused.

[5] GSMA, (2019) , 'Data protection in Mobile Money.'
<https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/03/Data-Protection-in-mobile-money.pdf>

[6] GSMA, (2019) , 'Data protection in Mobile Money.'
<https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/03/Data-Protection-in-mobile-money.pdf>

[7] Peterson R, (2020) 'Mobile money in Africa: Access, regulations and risks' DLA Piper
<https://www.dlapiper.com/en/belgium/insights/publications/2019/04/africa-connected-issue-2/mobile-money-in-africa/>

[8] UNCTAD, 'Mobile Money for Business Development in the East African Community.'
<https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=139>

03

ADDENDUM

MOBILE MONEY AND DATA PROTECTION IN KENYA DURING COVID-19, A CASE STUDY.

As the world grapples to contain and mitigate the spread of the novel coronavirus (COVID-19) different preventive measures are being taken by governments the world over to address social and economic changes driven by the effect of the virus. Kenya has not been spared the burden of dealing with the spread of the virus. Since the report of the first case in the country the government has been swift in implementing preventive measures to contain the virus and cushion Kenyans from the economic effects of COVID-19. Among these preventive measures was a directive to reduce risk of transmission through the handling and transacting with bank notes and alternatively fully embrace mobile money transactions.

The directive was followed by a request by the Kenyan President H.E Hon. Uluru Kenyatta through a press statement asking banks and mobile network operators facilitating mole money products to consider the reducing the cost of transactions to allow customers / consumers adopt this cashless mode of payment as a preventive measure in containing the transmission of the virus.

In response to the directive the Central Bank of Kenya after consultations with other industry stakeholders issued a press statement with emergency measures to facilitate mobile money transactions. While the immediate objective was to reduce the risk of transmission of COVID-19, it was also meant to reduce the use of cash in the economy. Charges on mobile money transactions up to Kshs. 1000 were waived, transaction limit for mobile money was increased to Kshs. 150,000, the daily limit for mobile money transactions was increased to Kshs. 300,000, the mobile money wallet limit was also increased to Kshs. 300,000, the monthly total limit for mobile money transactions was eliminated, tariff for mobile money transactions was increased to apply to transactions up to Kshs. 150000 and commercial banks and PSPs were directed to eliminate charges for transfers between mobile money and wallets and bank accounts.

In the previous year, Central Bank of Kenya data showed that mobile money transactions stood at 3.98 trillion moving nearly half of the country's GDP through mobile money transactions, the data also recorded 224,108 registered mobile money agents registered through Mobile Network Operators(MNOs). Safaricom is Kenya's largest mobile network operator with the largest mobile money product Mpesa, which has approximately 20.5 million customers across its network holding the dominance in the mobile money space in Kenya.

The directive to move to mobile money transactions somewhat eliminating the use of bankers notes will undoubtedly lead to an increase in the already large number of mobile money users creating a surge in personal identifiable financial information. Mobile money users are often already registered to a specific mobile network operator, as the registration is linked to customers' identification information. This registration process provides each user with their own kind of digital identity.

Personally Identifiable Financial Information (PIFI) is any information that a consumer provides to a financial institution that would not be available publicly. PIFI enables the unique searching, identification and validation of a person's financial information through a specialized database and/or system. The data stored within PIFI is used for a set of different applications and/or business services.

In Kenya banks use digital wallets for mobile money enabling money transfer from M-Pesa for example to a customer's bank account and vice versa. Validation is often done through the sharing of PIFI where money can be moved from one's bank account to M-Pesa for example and from M-Pesa to the bank. With the expected increase is the sharing of personally identifiable financial information data security becomes a paramount importance. The primary objective for MNOs providing mobile banking products and banks that use digital wallets at this time would be to create an operating environment where security, privacy and authenticity are at the center of their operating systems.

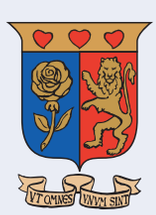
Kenya recently enacted the Data Protection Act 2019 , the act clearly highlighting provisions for the regulation of processing personal data. The provisions of this act consequently apply to mobile money transactions in respect to PIFI. Data processing, security, sharing and localisation impact key aspects of the delivery of mobile money services, and necessitate flexibility and adaptability among mobile money providers.

The Kenya Information and Communications (Consumer Protection Regulations 2010) offer an applicable degree of protection against surveillance through licenses systems in this case licensed systems of MNOs. The provisions of the Computer Misuse and Cyber Crimes Act 2018 also apply to the security related aspects of mobile money covering possible cyber security threats that may affect financial data shared in the course of mobile money transactions.

The use of mobile money heavily intersects with the digital identity landscape of any economy, it is therefore because of this intersection that data protection particularly of identifiable financial information in mobile money transactions is necessary in maintaining the market integrity and confidence but also important in preserving the right to privacy.

ACKNOWLEDGEMENTS

This work is part of #GoodID, a Global South project funded by Omidyar Network.
For more information please visit www.cipit.strathmore.edu and www.good-id.org



Ole Sangale Rd, Madaraka Estate.
PO Box 59857 00200, Nairobi, Kenya | Tel +254 (0)703 034 612
Email: cipit@strathmore.edu | Website: https://cipit.strathmore.edu