POLICIES, REGULATIONS AND PROCEDURES AND THEIR EFFECTS ON MOBILE MONEY SYSTEMS IN UGANDA

Frederick Kanobe
Tshwane University of Technology
South Africa
fred.kanobe@gmail.com

Patricia M Alexander
Tshwane University of Technology
South Africa
AlexanderMP@tut.ac.za

Kelvin J Bwalya
University of Johannesburg
South Africa
bwalyakelvinjoseph@gmail.com

ABSTRACT

The introduction of mobile money systems in emerging economies has enabled the would-be unbanked population to gain access to financial services. The number of mobile money users and value of transactions is on the increase. This rapid growth of mobile money services and value transactions in emerging economies is attributed to the light-touch regulatory framework which allows minimal limitations on who should operate mobile money system and few restrictions on who can function as an agent. These increases both in services and transactions indicate that mobile money systems hold a lot of valuable customer financial information that needs to be jealously protected against information breaches and abuse by the various stakeholders in the mobile money ecosystem.

Taking an interpretive qualitative approach, Activity Theory (AT) has been used to analyse the mobile money management activities focusing on information security policies, regulations and procedures. In order to comprehend the aspects revealed by the Activity Theory analysis that raise information security management concerns in mobile money operations, Mobile Network Operator (MNO) management issues, in terms of the security of mobile money operations, are detailed.

Our findings look at the reasons given by various stakeholders for information security management gaps in mobile money operations in emerging economies. Our findings disclose the roles of MNO staff, who are not information security experts, in the development and compliance monitoring of policies, regulations and procedures related to the safety of financial information in mobile money systems.

KEYWORDS

Mobile Money, Mobile Network Operators, Mobile Money Ecosystem, Activity Theory

1. INTRODUCTION

Mobile money systems can help to improve access to financial services in emerging economies. In Africa, several such systems have been developed specifically to assist the unbanked to get financial services. The most dominant is the mobile network operator (MNO) provider-led type of system where mobile money customers do not need to be attached to a traditional bank account but perform banking transactions through their MNOs. Mobile money payments have gained wide acceptance as an emerging payment method in both developed and emerging economies (Dittus & Klein, 2011). It is clear that these are fulfilling a need as a rise in the number of global mobile users has been predicted from 0.8 billion in 2014 to 1.8 billion in 2019 (KPMG, 2015). This view is supported by East African Community reports of an increase in mobile money transactions of many millions of dollars annually (EACO, 2014) while the Bank of Uganda reports indicate an increase in mobile money transactions from 33 billion Uganda shillings in 2009 to 32,506 billion Uganda shillings in 2015 (BoU, 2016).

Mobile money systems have generally gained wide acceptance as an emerging payment method in both advanced and emerging economies (IMF, 2014). In emerging

economies, where the majority of the people have previously had access only to formal banking services, mobile money systems have reduced the gap between the banked and the unbanked population. Gartner (2013), point out that mobile money transactions are growing fast and are expected by 2017 to reach over 450 million subscribers with a mobile money transaction value of more than $720 billion. However, this repid growth in the use of mobile money systems needs to be sustained with customers' confidence and safety of their information, therefore there is a need for good information security management practices and standards.

In nations where formal banking is not used widely, mobile money systems have been generally accepted as an easy means to make emergency payments and for electronic money transfers to settle domestic financial matters. Ndiwalana et al. (2014) note that mobile money systems in Uganda are commonly used to settle utility bills, parking fees, school fees, remote purchase of airtime, medical bills, taxes, university fees, insurance premium, fuel, air ticketing and electronic money transfer to relatives and friends. Hence, this is an important tool in the fight against financial inclusion in emerging economies and has sparked a wave of economic activities involving many players at various economic levels.

UNCTAD (2012) notes that mobile money systems in emerging economies operate in complex and changing environments with many new players who have varying interests and objectives and whose roles and responsibilities may overlap. The relationships and roles of the various mobile money stakeholders are summarized Figure 1 as follows.

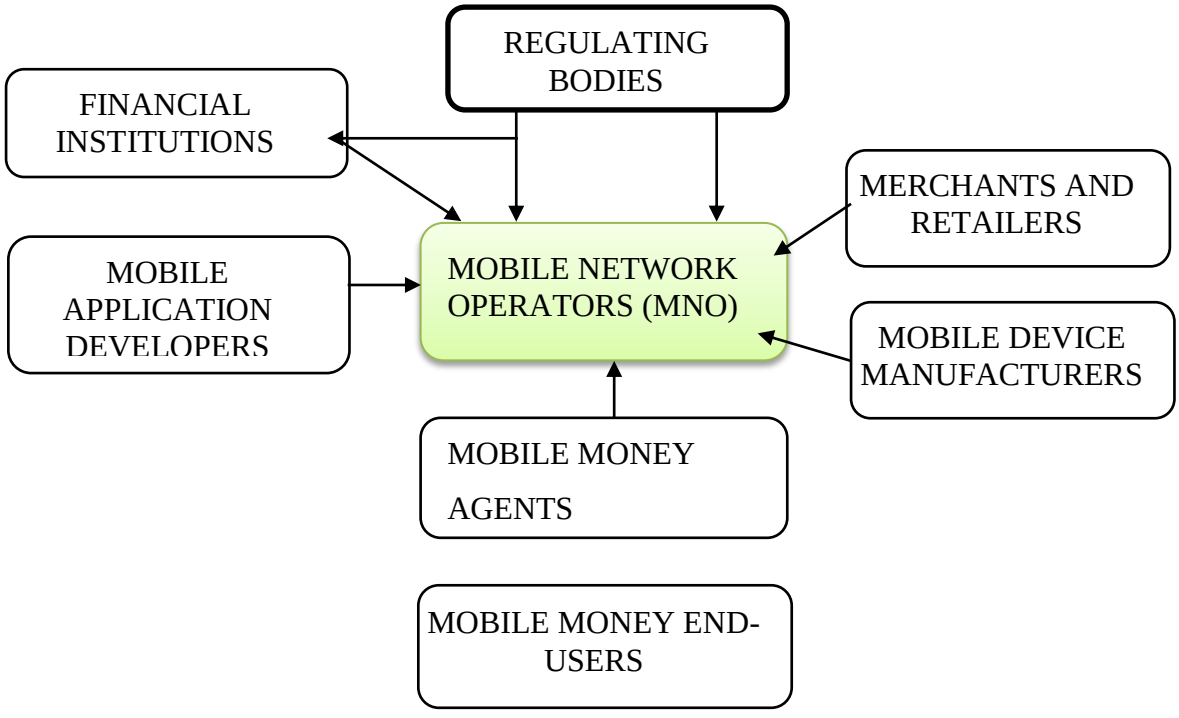

Figure 1: Roles of Mobile Money Stakeholders

The roles of the stakeholders involved in the mobile process are described in Table 1.

Table 1: The Roles of the Stakeholders Involved in the Mobile Process

Regulating Bodies	*Mobile Network Operators (MNO)*
Set minimum operating requirements for mobile network operators Set know-your-customer norms for mobile	Host and manage individual mobile money accounts for end-users Set end-user operational requirements for

network operators Supervise mobile network operators *Financial Institutions* Host the main mobile money account on behalf of the mobile network operators Manage foreign exchange	mobile money Manage and control mobile money transactions Administer end-user mobile money accounts Responsible for the information security management of mobile money *Mobile Application Developers* Develop mobile money applications
Mobile Money Agents Register mobile money users Give cash to mobile money end-users Keep money float on behalf of MNO Process electronic money for mobile money end-users	*Mobile Money End-users* Hold mobile money accounts (electronic wallets) Send electronic money to intended Receive mobile cash
Merchants and Retailers These include supermarkets, petrol stations, insurance companies, wholesale and small business entities, government bodies, utility corporations who accept mobile money in exchange for goods and services	*Device Manufacturers* Manufacture and sell mobile devices such as mobile phones, tablets that MNO purchase to run the mobile money applications used by mobile money customers.

The existence of the diverse mobile money stakeholders (shown in Table 1) who are involved at different levels of mobile money transactions is seen to be an advantage but is also a possible risk to the safety of information. This is because each of the stakeholder's attributes must be considered with respect to the security of mobile money systems. Therefore, information security management guidelines are needed that can tap into the synergies created by the mobile money ecosystem in order to provide adequate security for the financial information.

2. STUDY PURPOSE

The main purpose of the study was to explore information security management policies, regulations and procedures by taking a qualitative case study approach in order to gain detailed understanding of mobile money activity. Whereas it is true that studies in information security for mobile money systems have been conducted in the East African region where Uganda inclusive, such studies have focused mainly on objective security, rendering information security research incomplete. D'Arcy and Hovav (2007) say that objective security is characterized by technical applications and tools which alone cannot fully address the information security problem. This current study intends to take a management approach (*subjective*) to information security to fully address the current security problem in mobile money systems. Merkow and Breithaup (2014) contend that "*when people are left on their own they tend to make the worst security decisions*" therefore it was necessary to undertake this study to avoid people take the worst security decisions concerning mobile money operations.

3. CONCEPTUAL FRAMEWORK: ACTIVITY THEORY

Activity Theory (AT) was selected as appropriate to underpin this study since mobile money transactions are viewed as activities made up of many tasks. Activity Theory (AT) was developed in the Soviet Union in the 1920's and 1930's by Russian psychologists Vygotsky, Rubinshtein and Leont'ev. Vygotsky maintains that human activity is purposeful and is carried out by a set of actions through the use of tools which can be physical or psychological.

Leont'ev (1981) described an activity as a holistic, high level, collaborative construct, such as undertaking a work project that is at a higher level than goal-oriented actions and underlying operations. An activity both facilitates, and is facilitated by the psychological or physical tool used. Tools can be primary (physical artifacts such as technologies and machines), secondary (organisation customs and practices) or tertiary (operational environment).

Engestrom (1987) describes Activity Theory using the notion of a collective activity system with the following elements: subject, object, tools, rules, division of labour and a community (environment). Activity Theory has evolved and been expanded over time, but it is Engestrom's (1987) approach that has served as the basis for much of the AT-oriented work in information security and human-computer interaction research.

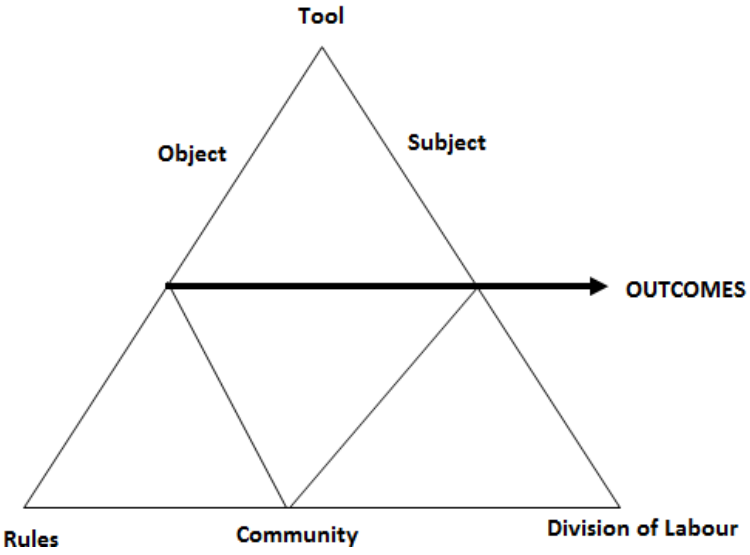

Figure 2: Representation of a Collective Activity System (Engestrom, 1987)

Kaptelinin and Nardi (1997), Engeström (1999) explain the fundamental principles of Activity Theory and these include the following:

- **Hierarchical structure of activity** - Activities are composed of goal-directed actions that are undertaken to fulfil the object and different actions may be undertaken to meet the same goal. Actions are executed through automatic operations. Operations do not have their own goals; rather they provide an adjustment of actions to current situations. The unit of analysis is an activity. Activity Theory holds that the constituents of activity are not fixed, but can dynamically change as conditions change.
- **Object-orientedness** - The principle of "object-orientedness" states that human beings live in a reality that is objective in a broad sense: the things that constitute this reality have not only the properties that are considered objective according to natural sciences but socially defined properties as well.

- **Internalization/externalization -** Activity Theory differentiates between internal and external activities. It emphasizes that internal activities cannot be understood if they are analyzed separately from external activities, because they transform into each other. Internalization is the transformation of external activities into internal ones. Externalization transforms internal activities into external ones. It is also important when a collaboration between several people requires their activities to be performed externally in order to be coordinated.
- **Mediation -** Activity Theory emphasizes that human activity is mediated by tools in a broad sense. Tools are created and transformed during the development of the activity itself and carry with them a particular culture - historical remains from their development. So, the use of tools is an accumulation and transmission of social knowledge. Tool use influences the nature of external behavior and also the mental functioning of individuals.
- **Development -** In Activity Theory development is not only an object of study, it is also a general research methodology. The basic research method in Activity Theory is not traditional laboratory experiments but the formative experiment which combines active participation with monitoring of the developmental changes of the study participant.
- **Contradictions and tension** - Activity Theory takes contradiction as source of change and development. Contradictions are not the same as problems or conflicts instead contradictions are historically accumulating structural tensions within and between activity systems. When an activity system adopts a new element from the outside it often leads to an aggravated secondary contradiction where some old element rams with the new one.

In the context of this study, a mobile money transaction is viewed as the activity system. The **object** (mobile money information security management) is attained through many **subjects** (such as mobile money information security experts, internal auditors, legal specialist, finance professionals, human resource experts, and mobile money agents) who use the **tools** (mobile phones) or mediating artifacts such as mobile money application, to directly or indirectly facilitate the activity. The activity is accomplished through **division of labour**. For example, internal audit managers develop controls on mobile money transactions and monitor compliance, human resource managers design information security job roles and responsibilities for IT experts, finance managers keep record of mobile money transactions. The subjects relate to their organisation through regulations, such as company policies and mobile money regulating policies that shape the actions and behaviours of mobile money stakeholders.

Activity Theory has been used in a number studies focusing on information systems, information security and studies involving human activities and use of technology, (Mohamad Said et al., 2014; Bardram & Doryab, 2011). This study also involves activities and use of technology (activities and use of MM) making it the most suitable to underpin the study.

4. LITERATURE REVIEW

4.1. Mobile Money Systems in Uganda

The first mobile money system in Uganda, *"MTN Uganda"* was introduced in 2009, a year after the successful launch of M_PESA in Kenya (Jack & Suri, 2011). In addition to MTN Uganda, mobile money platforms currently in Uganda include Airtel Money, M-Sente for Uganda Telcom and Africell Money. Mobile money in Uganda was initially introduced basic services such as buying airtime, making small monetary deposits and withdrawals, sending

and receiving electronic money to other users and non-users of mobile money systems. It is important to note that the first mobile money users in Uganda were not registered and were anonymous allowing whoever had a mobile phone to have access to mobile money services. This weakness in the policy framework and procedures has been difficult to eradicate. Currently mobile money in Uganda is the prime means of money transfer, dominating financial services in the country especially in rural and semi-urban areas where the majority of the population is unbanked.

In Uganda, mobile money systems offer many benefits to end users such as payment of utilities, paying church offerings, settlement of individual debts, financial domestic settlements, clearance of medical bills, tax payments, payments of wages, payment of school fees. They also play a key role in addressing the financial inclusion problem. Despite their many benefits, mobile money systems in operate in a complex environment in which there are many new and inexperienced players whose boundaries of operation and interests seem to overlap. For example, the role of mobile money application developers, who are at the same time users of the application they have developed, creates some vulnerability in the systems.

Macmillan et al. (2016) point out that by 2015 there were 21.1 million registered mobile money users in Uganda, representing a penetration of about 54%. The wide spread of mobile money systems in Uganda have two main enablers. Firstly an existing, countrywide, wireless network and the deep penetration of mobile phones have laid the background for mobile money. And secondly the majority of the population live in rural areas where traditional banks have found it expensive to extend financial services due to poor infrastructure leaving the majority of the people unbanked. The MNOs have taken advantage of this to extend financial services through mobile money to the unbanked population. The following table gives a summary of the mobile money platforms and their market share.

Table 2: MNO with Mobile Money Platforms in Uganda in 2015 (Evans & Pirchio, 2015)

Mobile Money Product/service	Mobile subscribers (Millions)	Mobile Money subscribers (Millions)	Market share (percentage)
MTN/MTN mobile money	10.5	7.3	58.4
Airtel/Airtel Money	7.5	3.4	27.2
Mango/M-Sente	9.8	1.5	10.4
Africell/ Africell Money	0.6	0.5	4.0
Total	20.5	12.5	100

From Table 2 it is clear that MTN has the lion's share in terms of mobile money services due to its countrywide mobile network coverage including rural areas. In Uganda there are two mobile money regulating bodies governing mobile money operations, namely, the central bank (Bank of Uganda) that controls mobile money services and Uganda Communication Commission (UCC) that oversees the mobile network.

As in other emerging economies, MNO in Uganda have endeavoured to extend a variety of mobile money services to their customers with the aim of retaining existing users and at the same time attracting new ones. The main mobile money services in Uganda include:

- **Person-to-Person (P2P):** This was the first mobile money service in Uganda and is still the most popular. It involves the transfer of electronic money using mobile money systems from one individual to another.

- **Person to Business (P2B):** This allows individuals to transfer money to companies to settle their utility bills, insurance premiums, medical fees, school fees, air ticketing, buying fuel and other services.
- **Person to government (P2G):** This is mainly used to settle statutory charges like taxes, traffic offences by payment to government bodies through mobile money transfers.
- **Business to Person (B2P):** This is where an organisation transfers money to individuals commonly in the form of salaries and wages.
- **Government to Persons (G2P):** Here the government pays individuals their social benefits through mobile money transfers.

Recent offerings, such as micro-loans and SACCO wallets, are in a pilot phase. The market demands and a competitive business environment among mobile money service providers are possible reasons for the increase in the number of services.

Table 3: The Status of Mobile Money Services offered in Uganda (Nampewo et al., 2016)

Product/Service	Status
Domestic transfers/remittances (P2P)	Live
Merchant payments - enabling corporates to receive payments (P2B)	Live
Statutory payments (taxes) person to government (P2G)	Live
Bulk payments: Salaries and wages. Business to Person (B2P)	Live
Micro-loans and savings	Pilot
Group wallets for SACCOs	Pilot
Cross boarder transfers	Live
Mobile banking - transfer from bank account to M-Wallet	Live
Government payments (Social benefits) Government to Person (G2P)	Live

Because more sensitive data now resides on mobile money services as listed in Table 3, these services have become a target of abuse by some stakeholders and more especially where light touch regulations and minimal information security policies exist.

4.2. Importance of Mobile Money Systems

Mobile money has taken dominance in money transfers in emerging economies and more especially in rural areas where the majority of the population lack access to formal financial services. In East Africa it is challenging to identify a household without a mobile money accounts yet it is very easy to locate households without conventional bank accounts. The introduction of mobile money has stimulated some economic activities and created jobs for many people in emerging economies including: Mobile network providers, mobile network agents, mobile application developers, retail mobile money outlets, mobile money system administrators, finance analysts, information system auditors among others. However it has also given citizens who are not involved in the mobile money "business" access to money and hence increased their opportunities to engage in the economy in new ways. The mobile money ecosystem is a rich environment with a variety of stakeholders each with their own objectives and goals that have economic impact.

Whereas the rest of the world has embraced mobile money systems to some extent, the comparative advantage in emerging economies where there is poor infrastructure and the majority of the people live in rural and remote areas where conventional financial services are limited, is predominantly important.

Mobile money systems have to some degree helped to increase savings among persons who have limited access to traditional banking services. Jack and Suri (2011)

recognize that mobile money systems allow individuals to keep their savings hidden from friends or relatives who might ask for money. Mobile money systems give end users an opportunity to own virtual money accounts where they can make deposits for purposes of saving for future use.

Mobile money systems also greatly reduce the expenses and delays associated with opening, operating and maintaining a traditional bank account. The requirements for opening a mobile money account are minimal as compared to conventional bank account and interestingly there is no minimum account balance required for a mobile money account. Mobile money permits its end user to control the electric money.us

Mobile money systems are very convenient to use in times of access and time and provide the best means of settling emergency financial problems. Unlike the conventional bank account that has limits on access time, mobile money can be accessed at any time (24/7).

Mobile money systems physically safeguard money. In rural areas where the majority of the people limited access to formal financial services, money has in the past been stored in houses where thieves and rodents could easily access and destroy it. Therefore, mobile money systems provide an alternative, safe way for storing money. In business communities where people move big volumes of money from one location to another, mobile money minimizes the risks associated with cash transactions.

Leung and Wei (2000) contend that mobile money has mobility and prompt access by its users as the key advantages of over cash money. Mobile money provides the quickest mechanism for clearing unplanned domestic financial payments.

Mobile money systems are a powerful tool for fundraising for disaster and emergency responses by the community. Many humanitarian organizations in East Africa are using mobile money systems to raise funds to assist the victims of disaster. For example, Uganda Red Cross has on several occasions used its mobile money s platform to raise funds to assist victims of landslides, floods and Ebola so is the Kenya Red Cross and both have yielded good results.

ISACA (2012) points out a number of additional importance of mobile money systems and these include:

Mobile money systems have extensive networks that can reach even remote rural areas where there is poor infrastructure and where people have limited access to other forms of digital financial services.

Mobile money systems are also more cost effective to extend financial services to rural than to offer traditional financial services. ISACA (2012) cite the Asian Banker report (2007) that used evidence from the Philippines to indicate that a typical bank account transaction costs the bank US $2.50 while a mobile money transaction costs only US$ 0.5.

Mobile money systems provide an opportunity to extend financial services to very large populations more quickly and easily than other the conventional financial services. The level of mobile phones penetration globally is very much deeper than the conventional banks. Therefore, mobile money services can easily be provided to large numbers of people using the existing voice communication infrastructure.

Mobile phones are multifunctional and are frequently used by the owners, therefore, when there is any abuse of the mobile money end users are likely to discover anomalies more quickly than credit card users will. Although this does not guarantee the security of the system, it provides a fast means to follow up on any suspicious actions

4.3. Mobile Money Challenges in Emerging Economies

Despite its fast growth and the enormous benefits of mobile money systems in emerging economies, there exist serious information security management concerns that have led to information breaches related to mobile money operation.

Mobile money information security challenges in emerging economies, including Uganda, are related in one way or another. Regardless the fact that mobile money has generally received acceptance as a means of payment for addressing urgent financial and domestic problems in emerging economies, weaknesses in the security policies, regulations and procedures, financial information breaches and other forms of information misuse continue to appear.

In Uganda, the Observer (2013) reveals that on average 100 mobile money users lose money every week and some lose large quantities of money. Nevertheless the unreported cases may surpass the reported ones. There are limited information security policy guidelines and regulations to support the diverse mobile money stakeholders and to provide adequate security for key financial information. Unfortunately, limited research has been conducted to adequately address the mobile money information security management concerns. Instead it has been largely left for discussion in the media where it often makes dramatic headlines for the audience but lacks detailed suggestions regarding an appropriate solution to the escalating problem.

Whereas some level of information security for mobile money systems in emerging economies has been proposed by information security experts to minimize the contemporary mobile money security challenges, they focused mainly on technical tools leaving the information security management roles only in the hands of information security specialists and locking out none-information security professionals. For example, Nyamtiga et al. (2013), in their study enhanced Security model for mobile money systems in Tanzania, concentrated on technical solutions that include enhanced confidentiality of data through data encryption and introduce logical authentication to verify mobile money users' identities; Deshmukh and Naware's (2014) study about security challenges for mobile money payment in India emphasizes biometric identification for mobile money users and encryption of mobile money messages; Obodoeze et al. (2011), in their study, enhanced a modified security framework for Nigerian e-cashless systems and focused on encryption standards, user authentication and security vulnerability scans for mobile money transactions; Feroze and Basharat's (2011) study about security of mobile money in Pakistan concentrated on SMS technical architecture and design of the mobile money system.

Certainly, a solution that is inclined only to one side of technical information security provides a partial solution to the escalating information security concerns in mobile money systems. Therefore, there is a need to supplement it with the management aspect of security through adequate policies, regulations and procedures. In addition, each of the stakeholders in the mobile money ecosystem (see **Error! Reference source not found.**) need to have a recognized security role. Unmanaged strategies for information security lead to a piecemeal approach. Implementing controls, such as firewalls and CCTV cameras, encryption of data and the application of intrusion detection tools may not address all risks to information (ISO 2700, 2013)

Light regulations have mainly on the protection of the monitory value of the money, Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) rather than the protection and control of mobile money information. Mbiti and Weil (2011) argue that the introduction of mobile money in East Africa was built on a weak information security policy foundation because the MNO received *"a simple letter of no objection"* from the central bank to start the mobile money business. It is tempting to conclude that mobile money systems in East Africa kicked off without comprehensive controls, adequate guidance and

compliance monitoring from the regulatory bodies, leading to some of the current information security management policy challenges.

5. MOBILE MONEY INFORMATION SECURITY POLICIES CONCERNS IN UGANDA

The first users of mobile money systems in Uganda were not registered by the MNO making them anonymous in the mobile money system. This is because there was no well-defined information security policy or regulation for the mandatory registration of mobile money end-users. This made it very challenging for MNO to identify and verify the authenticity of the transactions, leaving customers' valuable information at risk. It is not easy to trace suspicious mobile money use for users are not registered in the system and this threatens the security of the mobile money transactions. Bersudskaya and Kuijpers (2015) content that Uganda in East Africa region experience the highest level of mobile money abuse with 53% of mobile money agents reporting mobile money abuse as compared with Tanzania and Kenya who had 42% and 12% cases of mobile money abuse respectively in their operation. It is also noted that higher risk of mobile money abuse is inclined more to agents who handle more than 40 transactions a day than those who conduct 20 transactions or fewer a day and most abuses are perpetuated by employees. It also follows that the higher the volume of mobile money information or transactions on the system the more insecure the mobile money information and transaction becomes. This is possibly because, as UNCTAD (2012) contend, the initial MNO in East Africa had an open door operation for mobile money users who were not registered due to the poor national identification scheme in the East Africa Community. Incidents of mobile money information security abuse in Uganda and other emerging economies have been linked to weakness in security policies (CGPA, 2014). In time the large scale of mobile money may undermine the confidence of mobile money customers.

COBIT 5 for information security management points out the consequences of a lack of adequate information security management policies and procedures for businesses such as mobile money system transaction results to the following:

- It exposes the business to legal risks and more especially when the end-users came to realize that failure of the organization to protect their information is the cause for information breach.
- It leads to financial loss to both the company and the customers
- It also leads to operational challenges and failure to transact payments.
- It damages business relationships with the customers and other partners
- It can also lead to a loss of business secrets and increased scrutiny from regulatory bodies
- It damages the entire business reputation and image

6. METHODOLOGY

6.1. Research Perspective and Stance

This study was carried out using a multi-case interpretative study to investigate the information security policies, regulations and procedures focusing on mobile money operations. This paper is based on a detailed study of two MNO (referred to as MNO_1, MNO_2) managing mobile money systems in Uganda. The role and involvement of professionals who are not information security experts, in the development of information security policies, regulations, their deployment, adherence, compliance and administration was studied critically.

6.2. Research Participants

The research participants were purposively selected basing on their expertise, experience, skills relating to the subject under study in order to get rich and relevant information. The

first round of included sixteen semi-structured interviews conducted with informants from the participating MNO (MNO_1) (see Table 4).

Table 4: Research Participants from MNO_1

Department	Alias	Position	Race/Gender	Origin of Organisation
IT	IT01	IT manager	Black/Male	Uganda
IT	IT02	IT officer	Black/Male	Uganda
Legal	LG01	Assistant Legal corporate secretary	Black/Female	Uganda
Legal	LG02	Corporate legal officer	Black/Female	Uganda
Audit	AD01	Senior Internal Audit manager	Black/Male	Uganda
Audit	AD02	Internal audit manager	Black/Female	Uganda
Human Resource	HR01	Human resource manager	Black/Female	Uganda
Human Resource	HR02	Human resource officer	Black/Female	Uganda
Security & Compliance	SC01	Security & Compliance assistant	Black/Male	Uganda
Security & Compliance	SC02	Security & compliance managers	Black/Male	Uganda
Finance	FN01	Finance manager	Black/Male	Uganda
Finance	FN02	Finance officer	Black/Male	Uganda
Sales & Marketing	SM01	Senior corporate marketing manager	Black/Female	Uganda
Sales & Marketing	SM02	Corporate marketing manager	Black/Male	Uganda
Procurement	PR01	Procurement manager	Black/Male	Uganda
Procurement	PR02	Procurement Assistant	Black/Male	Uganda

All the correspondents were involved in the management of mobile money system operations and therefore, were well-informed and provided relevant information that guided the investigation. The semi-structured interviews were conducted in a private board room and lasted between 40 and 55 minutes. Besides the interview, data pertaining to mobile money operations such as the customers' terms of operation, agents' recruitment forms, mobile money operation training manuals, mobile money regulation guidelines 2013 were viewed and critically analysed to further inform the study. Some participant observations were conducted to check the actual use of the mobile money operation procedures and practices. Items that were checked were: do they provide sufficient information security and management for the mobile operation?

7. FINDINGS AND DISCUSSIONS

The research questions created with guidance from Activity Theory informed the semi-structured interviews used in the data collection exercise. A summary of the findings following the completion of the first phase of data collection is given in Figure 3.

The mobile money and mobile application tool were identified the basic tools required for the operation of mobile money system. The tools are the main conduit for transmission of critical services that hold a verity of services to the mobile money customers. The security of the tools that houses critical financial information for mobile money customers ought to have the most adequate security for successful operation of the mobile money systems. Unfortunately the role of information security management had been inclined to information security experts mainly. Another of rules have been identified which if information security aspects and integrated in them, it enhances shared information security management function among the core mobile money stakeholders and will strive to achieve shared accountability of the safety of the mobile money systems. The rules identified are include; job descriptions and terms of employment.

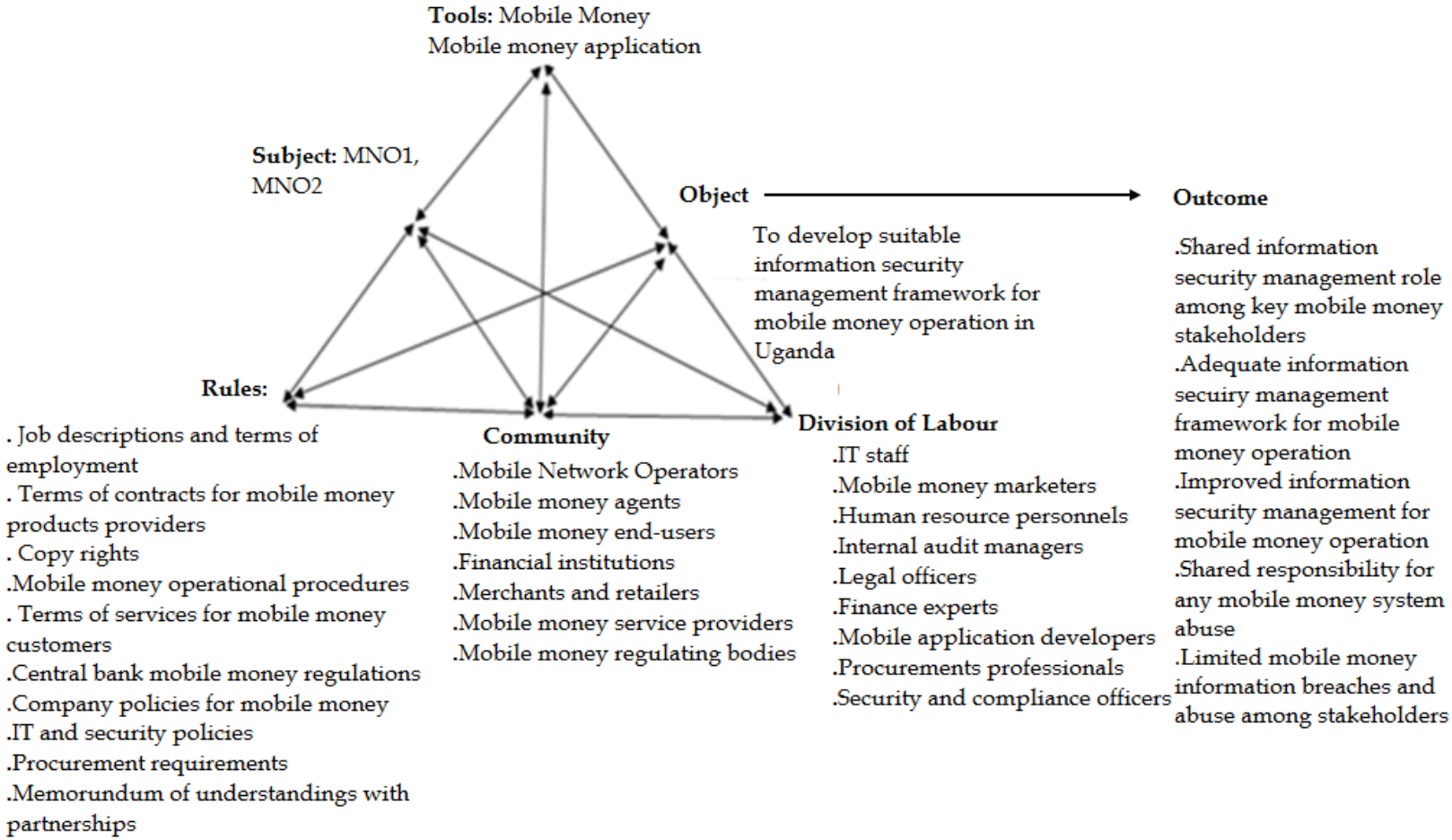

Figure 3: Summary of Findings with the Lens of Activity Theory

The inclusion of job descriptions and terms of employment for all staff are needed as the information security management role described in the human resource policy creates shared responsibility for the information security function among all staff irrespective of the profession. Likewise, all contract terms for both long term and short term outsourced mobile money product providers state that information security is a binding responsibility to safeguard customers' information. This is because some outsourced personnel, such as mobile application developers and mobile money agents have access to sensitive information by nature of their work. Similarly procurement requirements and memoranda of understanding with business partners are included to safeguard the mobile money information and are guided by binding information security policy clauses.

The community in which mobile money system operates (who constitute the environment) is rich with a variety of stakeholders subjecting the mobile money information to move along a chain of people whose interests and targets in the mobile money ecosystem vary. The mobile money community is composed of the operators, agents, merchants and retailers, regulating bodies, financial institutions, service providers and. Each of the stakeholders in the mobile money community has an information security role.

Division of labour is demonstrated by the shared information security management role at different levels of mobile money operation and management. The officers whose functions need to contribute to this security management include IT, human resource, legal, procurement, sales and marketing, finance, information security and compliance and finance among others.

The anticipated outcome of the study, once the information security function is integrated into the identified rules and information security roles is: adequate information security management for mobile money operations, improved mobile money operation, improved and shared information security management role among all the stakeholders and limited information security breaches and abuses within the mobile money ecosystem.

Identifying contradictions and tensions is critical in Activity Theory guided studies and play an important role in spearheading development and rapid change for the activity. Key contradiction that that eventually created tensions among the mobile money stakeholders were: mobile phone SIM card registration; the verification order issued by the Uganda Communication Commission (UCC), one of the mobile money regulating body. In February, 2017 UCC issued a seven day ultimatum to all subscribers of mobile phones in Uganda to register or verify the registration of subscriber Identification module cards or be switched off. This created a crisis and sparked disagreements with UCC from various interested parties including human rights activists (Rights Trumpet Limited), Uganda members of parliament, the prime minister's office, Uganda Law Society and the office of the president of the Republic of Uganda. Eventually the High court of Uganda issued an interim order restraining the mobile phone service providers from enforcing or implementing the directive from UCC regarding SIM card registration and verification using National Identification cards.

The core contradictions stem from the UCC, a government body that issued the order for SIM card registration that other government entities, such as the office of the prime minister and office of the president, rejected. Further contradiction emerged related to the SIM card registration deadlines. UCC set the SIM card registration deadline as 28th February, 2017, however, the office of the prime minister set it to 19th May, 2017 and the President's office set it to 30th August, 2017. However, as the national identification scheme in Uganda is not yet complete and many citizens do not have the national identification cards that were made a requirement for the SIM card registration. Yet it is the wide spread of mobile money systems has been attributed as the cause of minimal Know Your Customer norms including non-registration of SIM cards. Due to the tension and the fear to losing money housed in the mobile money systems, some users were prompted to register and verify their cards while a

number of them are still anonymous mobile money users on the mobile money platforms that threatens the safety of mobile money systems.

8. CONCLUSION

The main aim of this paper was to fully understand the information security management policies, regulations and procedures of the mobile money activity for the first round of the study. A qualitative case study was conducted, but at this stage only at a single site. Activity Theory is shown to have helped the researchers to fully comprehend mobile money operation activity and information security policy management challenges. The Activity Theory is believed to have delivered the most appropriate lens to cognize, appreciate and analysis of the various aspects of mobile money information security policies, regulations and procedures in relation to the tools, rules, community, division of labour, contradictions and tensions. The second round of the empirical study and further refinement of the data will inform the study further leading to its desired outcome.

9. REFERENCES

Bardram, J. & Doryab, A. (2011). Activity Analysis: Applying Activity Theory to Analyse Complex Work in Hospitals. In *Proceedings of the ACM 2011 Conference on Computer Supported Cooperative Work* (455-465). New York: ACM.

Bersudskaya, V. & Kuijpers, D. (2015). Network Accelerator Survey: Uganda Country Report 2015. http://www.helixinstitute.com/sites/default/files/Publications/070931%20ANA%20Uganda%20Country%20Report%20-%20FSDU%20-%20Final.pdf

BoU. (2013). Uganda Mobile Money Guidelines 2013. http://ucc.co.ug/files/downloads/mobile-money-guidelines-2013.pdf

D'Arcy, J. & Hovav, A. (2007). Deterring Internal Information Systems Misuse. *Communications of the ACM*, 50, 10, 113-117.

Deshmukh, S.P. & Naware, A.M. (2014). Mobile Money: M-Payment for India. *International Journal of Computer Science and Information Technologies*, 5, 2, 2672-2675.

Dittus, P. & Klein, M.U. (2011). On Harnessing the Potential of Financial Inclusion. (BIS Working Papers No. 347). Bank for International Settlements.

EACO. (2014). The East Africa Community Report on mobile and agency banking. https://www.google.co.za/?gfe_rd=cr&ei=N3BEVtWUAeKo8wfXp5zoCA&gws_rd=ssl#q=East+Africa+Community+mobile+phone+transactions+2014

Engeström, Y. (1987). *Learning by Expanding: An Activity-Theoretical Approach to Developmental Research*. Helsinki: Orienta-Konsultit Oy.

Engeström, Y. (1999) Innovative Learning in Work Teams: Analyzing Cycles of Knowledge Creation in Practice. In Engeström, Y., Miettinen, R. & Punamaki, R.-L. (Eds.). *Perspectives on Activity Theory* (377-406). Cambridge: Cambridge University Press.

Evans, D.S. & Pirchio, A. (2015). An Empirical Examination of Why Mobile Money Schemes Ignite in Some Developing Countries but Flounder in Most. (Coase-Sandor Institute for Law and Economics Research Paper No. 723). The University of Chicago.

Feroze, A. & Basharat, A. (2011). Security Analysis of Mobile Banking Services in Pakistan. *Asian Transactions on Fundamentals of Electronics, Communication & Multimedia*, 1, 3, 1-17.

IMF. (2014). Oversight Issues in Mobile Payments. (IMF Working Paper). International Monetary Fund.

ISO 2700. (2013). ISO 2700 Implementation Guide. https://www.bsigroup.com/LocalFiles/en-GB/iso-iec-27001/resources/ISO-27001-implementation-guide.pdf

Jack, W. & Suri, T. (2011). Mobile Money: The Economics of M-PESA. (NBER Working Paper No. 16721). National Bureau of Economic Research.

Kaptelinin, V. & Nardi, B.A. (1997). Activity Theory: Basic Concepts and Applications. In *Proceedings of CHI 1997 Extended Abstracts on Human Factors in Computing Systems* (158-159). New York: ACM.

KPMG. (2015). Mobile Banking Global Trends and Impacts on Bank. KPMG Report. https://www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublications/Documents/PDF/mobile-banking-report-2015.pdf

Leont'ev, A.N. (1981). *Problems of the Development of the Mind*. Moscow: Progress.

Leung, L. & Wei, R. (2000). More Than Just Talk on the Move: Uses and Gratifications of the Cellular Phone. *Journalism and Mass Communication Quarterly*, 77, 2, 308-320

Macmillan, R., Paelo, A. & Paremoer, T. (2016). The "Evolution" of Regulation in Uganda's Mobile Money Sector. *The African Journal of Information and Communication*, 17, 89-110.

Mbiti, I. & Weil, D.N. (2011). Mobile Banking: The Impact of M-PESA in Kenya. (NBER Working Paper No. 17129). National Bureau of Economic Research.

Merkow, M.S. & Breithaupt, J. (2014). *Information Security: Principles and Practices* (2nd ed.). New York: Pearson IT Certification.

Mohamad Said, M.N.H., Tahir, L.M., Ali, M.F. Noor, N.M., Atan, N.A. & Abdullah, Z. (2014). Using Activity Theory as Analytical Framework for Evaluating Contextual Online Collaborative Learning. *International Journal of Emerging Technologies in Learning*, 9, 5, 54-59.

Nampewo, D., Tinyinondi, G.A., Kawooya, D.R. & Ssonko, G.W. (2016). Determinants of Private Sector Credit in Uganda: The Role of Mobile Money. *Financial Innovation*, 2, 1, Article 13.

Ndiwalana, A., Morawczynski, O. & Popov, O. (2014). Mobile Money Use in Uganda: a Preliminary Study. Paper Presented at the 15th International Conference on Human-Computer Interaction: Users And Contexts of Use - Volume Part III, Las Vegas, NV - July 21-26.

Nyamtiga, B.W., Sam, A. & Laizer, L.S. (2013). Enhanced Security Model For Mobile Banking Systems in Tanzania. *International Journal of Technology Enhancements and Emerging Engineering Research*, 1, 4, 4-20.

Obodoeze, F.C., Okoye, F.A., Asogwa, S.C., Ozioko, F.E. Mba, C.N. (2011). Enhanced Modified Security Framework for Nigeria Cashless e-Payment System. *International Journal of Advanced Computer Science and Application*, 3, 11, 189-196.

Observer (2013). MTN Was Warned of Likely Mobile Money Frauds in 2009. http://www.observer.ug/business/38-business/36522-mtn-was-warned-of-likely-mobile-money-fraud-in-2009

UNCTAD (2012). Mobile Money for Business Development in the East African Community: A Comparative Study of Existing Platforms and Regulations. (United Nations Conference on Trade and Development Report). http://unctad.org/en/PublicationsLibrary/dtlstict2012d2_en.pdf