INFORMATION ABOUT THE AUTHORS

Title: Policies, Regulations and Procedures and their effects on Mobile Money systems in Uganda

Kanobe Fredrick

Email: fkanobe2010@gmail.com

Fredrick is currently a PhD candidate in the Department of Informatics at Tshwane University of Technology, South Africa. He holds a Master of Science degree in Information Technology (MIT), a Post-graduate Diploma in Computer Science, and a Bachelor of Social Sciences all from Makerere University, Uganda and a Postgraduate Diploma in project planning and management from Uganda Management Institute. He is a Microsoft Certified Systems Engineer (MCSE). He has more than ten years of experience in information systems design, implementation, support, maintenance, network management, hardware and software installation and management, IT project management, monitoring and evaluation. He has worked as Assistant Director ICT and ICT coordinator with Uganda Red Cross.

Prof. PM Alexander

Trish Alexander is a supervisor for Fredrick Kanobe's PhD. She has a contract with Tshwane University of Technology to supervise Masters and Doctoral candidates. She is also Prof Extraordinarius in the School of Computing at University of South Africa and Prof Emeritus (School of IT, University of Pretoria).

Prof. Kelvin Joseph Bwalya

Bwalya Kelvin Joseph is an Associate Professor at the Centre for Information and Knowledge Management, University of Johannesburg. He is also a member of the Board of Directors – Mosi-oa-Tunya University of Science and Technology – MUST. Prof Bwalya is also a PhD supervisor and member of the Board of Exams at Tshwane University of Technology and 7 other universities. He has supervised 5 PhDs to completion, several Masters and undergraduate projects. He has published 7 books and over 100 pieces of peer reviewed articles and has also managed research funds over US$500,000 in total.

Policies, Regulations and Procedures and their effects on Mobile Money systems in Uganda

1 Introduction

Mobile money (MM) can help to improve access to financial services in emerging economies. In Africa, several mobile money systems have been developed specifically to assist the unbanked to get financial services. The most dominant is the mobile network operator 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 mobile networker operators (MNO). Mobile money payments have gained wide acceptance as an emerging payment method in both developed and emerging economies (Dittus and 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 is also 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).

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, Morawczynski and Popv (2014) note that mobile money systems in Uganda are commonly used to settle utility bills, school fees, medical bills and other debts, for buying goods, and to transfer money 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 in figure 1 below.

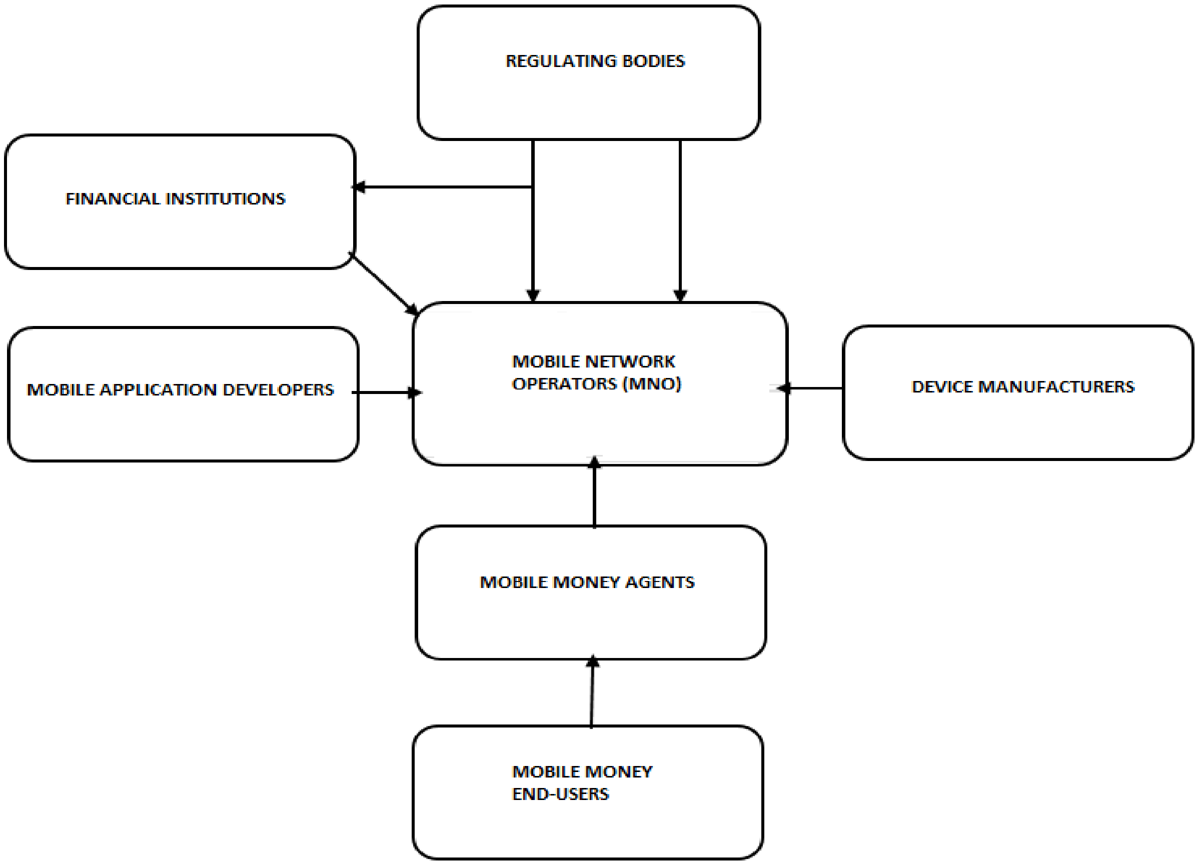

Figure 1: Roles of mobile money stakeholders (Source: Author, 2017)

The roles of the stakeholders involved in the mobile process (shown in Figure 1) are described as follows:

Regulating Bodies	Set minimum operating requirements for mobile network operators; set know-your-customer norms; supervise mobile network operators
Financial Institutions	Host the main mobile money account on behalf of the mobile network operators and manage foreign exchange
Mobile Application Developers	Develop mobile money applications
Mobile Network Operators (MNO)	Host and manage individual mobile money accounts for end-users; set end-user operational requirements for mobile money; manage and control mobile money transactions; administer end-user mobile money accounts; responsible for the security of mobile money

Mobile Money Agents	Register mobile money users; give cash to mobile money end-users; keep money float on behalf of MNO; process electronic money
Device Manufacturers	Manufacture and sell mobile devices to MNO
Mobile Money End-users	Hold mobile money accounts; send electronic money; receive mobile cash

The existence of diverse mobile money stakeholders involved in different levels of mobile money transactions is seen to be an advantage but is also a possible threat to the safety of information as each of the stakeholder attributes need to be considered with respect to the security for mobile money systems. Therefore, there is need for a strong information security management framework that can tap into the synergies created by the mobile money ecosystem in order to provide adequate security of the financial information.

2 Literature review

2.1 Mobile money challenges in Africa

Despite the fact that mobile money has generally received acceptance as a means of payment for addressing domestic financial problems and payment of utility bills in Africa, financial information breaches and other forms of information misuse seem to be common. 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 a lack of sufficient information security strategies to support the diverse mobile money stakeholders in providing adequate security for key financial information. Unfortunately, limited research has been conducted to adequately address the mobile money information security concerns, instead it has been majorly left for discussion in the media (newspapers) where it often makes headlines.

Whereas some level of information security has been proposed by information security experts to minimize the current mobile money challenges in Africa (Kwashaie; 2010) these measures focused mainly on technical tools. As a result, security roles are left in the hands of technical information security experts without the involvement of other mobile money stakeholders such as strategic managers, the end-users and the mobile money agents who take part in the transaction processes. Certainly, a solution that is inclined only on one side of technical security, provides an incomplete solution to the escalating information security concerns in mobile money systems.

All stakeholders in the mobile money ecosystem (see Figure 1) need to have a recognized security role. In addition, it has been noted that unmanaged approaches to 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). The human aspect of information security to supplement the technical security tools and applications, and which includes policies, procedures, practices, standards, reviews and compliancy monitoring, helps to provide a comprehensive information security management framework.

The following example is attributed to weaknesses in information security policy; Uganda mobile network operator X lost about USD $3.4 million when employees exploited this weakness and USD $ 4.7 million was spent on the associated recovery process. In the same year Rwanda's mobile network operator Y lost over USD $ 170,000 when internal staff exploited information security policy weakness in the mobile money system (CGPA, 2014:13). These examples indicate that the information security management of information in mobile money has not been addressed well because in both incidences mentioned it was not technical weakness such as hacking the mobile money system but information security policy issues. Therefore, the need for the sharing of the information security management role among the varying mobile money stakeholders is overdue.

Most African countries seem to copy the M-PESA mobile money platform of Kenya and hence share related mobile money challenges. The lack of awareness by mobile money customers about the risks involved in mobile money payments in Kenya that Luvanda, Kimani and Kimele (2014) compared to a time bomb waiting to explode at any time is not different from the fears of Kwashaie (2010) about mobile money in Ghana. Masamila (2014) also notes that mobile money users in Tanzania are not likely to be aware of the risks associated with mobile money payments and this makes them susceptible to fraudulent schemes. There have been, however, attempts in various African countries to regulate their mobile money services. In Uganda, Bank of Uganda mobile money guidelines (BoU, 2013) play an important role, the central bank of Kenya (Act 2009) plays similar role, and Rwanda law regulations relating to electronic messages, electronic signatures and electronic transactions guide mobile payments in that country (NBR 2010). The mobile money payments in Tanzania are under the umbrella of the electronic schemes guidelines 2007 (BOT, 2007). However, according to UNCTAD (2012), the mobile money regulatory tools in Africa are characterized by gaps and overlaps. At the same time there is limited experience that African countries can obtain from advanced and mature economies when drafting relevant policies, regulations and practices because it is believed that the first mobile money, M-PESA, was started in Africa (Mbiti and Weil, 2011).

2.2 Mobile Money Information Security Management Concerns

No tangible receipt is given to mobile money end-users involved in a transaction process to indicate the successful conclusion of the transaction (Simpson, 2014), although it is true that an SMS is usually received by the mobile money end-user to verify completion of the transaction as is the case with mobile banking by conventional banks. However, full transaction details are not shared in the case of mobile money in contrast with conventional banks which send detailed transaction information via emails and also have downloadable updates that can easily be obtained and saved by the customers for future reference purposes. The mobile money end-user has to rely entirely on the SMS and if the phone is stolen the history of mobile money SMS is very difficult, if not impossible to retrieve.

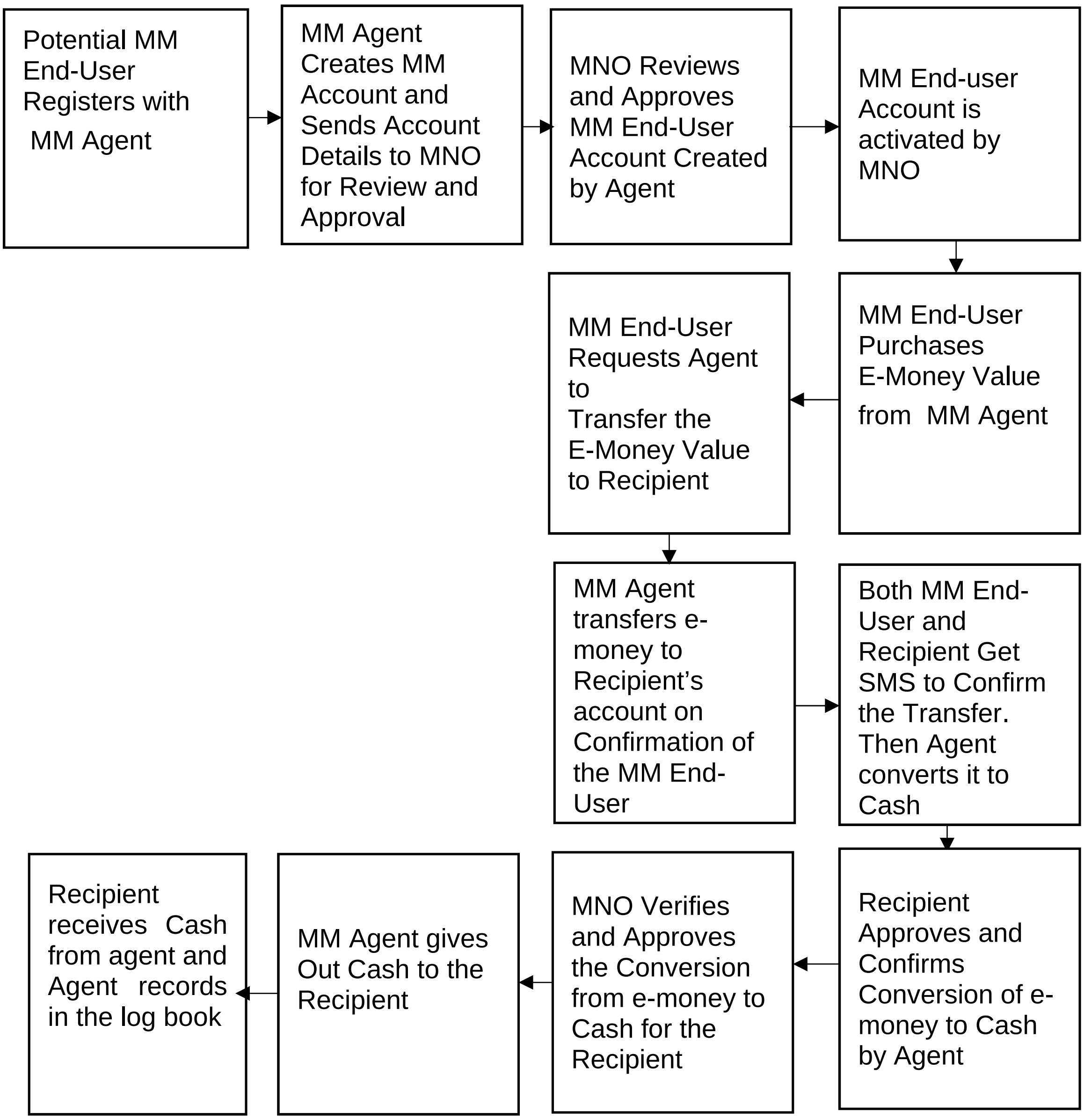
Potential MM End-User Registers with MM Agent
MM Agent Creates MM Account and Sends Account Details to MNO for Review and Approval
MNO Reviews and Approves MM End-User Account Created by Agent
MM End-user Account is activated by MNO
MM End-User Purchases E-Money Value from MM Agent
MM End-User Requests Agent to Transfer the E-Money Value to Recipient
MM Agent transfers e-money to Recipient's account on Confirmation of the MM End-User
Both MM End-User and Recipient Get SMS to Confirm the Transfer. Then Agent converts it to Cash
Recipient Approves and Confirms Conversion of e-money to Cash by Agent
MNO Verifies and Approves the Conversion from e-money to Cash for the Recipient
MM Agent gives Out Cash to the Recipient
Recipient receives Cash from agent and Agent records in the log book

Figure 2: Mobile Money registration and transfer process in East Africa (Source: Author, 2017)

As shown in **Error! Reference source not found.**, in the mobile money transactions process a limited transactions history is obtained apart from the SMS and no tangible receipt given to mobile money user as proof of transaction.

UNCTAD (2012) notes that the first users of mobile money services in Africa had mobile phones that were not registered and these users have continued to access the service despite the fact that recently mobile phone registration is one of the first steps required to get access to mobile money services. The fact that mobile network operators still allow unregistered mobile phone users to access mobile money services in a country such as Uganda puts mobile money end-users' information at risk because it is difficult to trace an unregistered mobile phone user who has no national identification card or passport after an illegal transaction has been made.

The introduction of mobile money in East African countries was built on a weak policy and procedural foundation because the mobile network operators received *"a simple letter of no objection"* from the central bank to start the mobile money business (Mbiti and Weil, 2011). As in Uganda, UNCTAD (2012) agree with Mbiti and Weil (2011) that the first mobile money platform (M-PESA) in Kenya was also largely managed by and was started by MNO following *"a simple letter of no objection*" from the central banks.

One can conclude that mobile money systems in East Africa kicked off without comprehensive controls, guidance and compliance monitoring from the regulatory bodies, resulting in the current information security management abuses and resultant financial losses to both mobile money end-users and mobile network operators.

Unlike in the conventional financial services where bank customers are required to produce their identification documents before permitted to withdraw cash at the counter from their accounts, the story with mobile money is different. For mobile money, identification documents are commonly required at the registration phase only, mobile money agents issue out cash to mobile money customer provided they know the phone number and PIN for a particular line. No verification of identities is carried out at the cash out phase, yet cell phones can easily be accessed, lost or even stolen putting the e-money at risk and breach of information to illegal users.

Harris, Goodman and Traynor (2013) claim that the introduction of mobile money in East Africa was also not accompanied by sufficient concern for privacy, opening doors to abuse and financial loss. A privacy breach, for instance, that allows others to know that a client has recently transferred a large amount into a particular account could make that account a target. It common practice for mobile money agent to attend two or even more mobile money customers at the same time on the same counter that raises the risk of information breaches to untargeted customers.

3 Research Methodology

3.1 Study Focus

The study focuses on a deep exploration of mobile money information security management policies, procedures and practices suitable to guide mobile money systems in Africa. Previous studies of mobile money systems that attempted to address the information security concerns focused mainly on technical security tools which alone cannot adequately address the information security question. The full scope of this study includes: (i) Study existing information security management policies, procedures, practices and standards and determine their strengths and weaknesses. (ii) Develop information security management framework for mobile money systems in Uganda. (iv) Validate the information security management framework developed. This paper addresses only the first of these objectives.

3.2 Methods

A qualitative, multi-case study strategy will be used in order to get an in-depth understanding of mobile money systems' information security challenges and concerns. The research participants will include the MNO who play a coordination and management role in mobile money activities, the mobile money agents who register the mobile money end-users, have access to mobile money information and process mobile money and the end-users who use the mobile money systems. The data collection will include observation, face-to-face interviews and has been preceded by a review of existing commentaries and published work on policies, procedures, regulations and practices about mobile money services. In addition, to achieve the first objective of the study, a comprehensive literature review has been conducted to obtain preliminary findings (see Section 4). The other data collection methods shall be used in the future stages of this research in addressing the remaining objectives and obtaining empirical findings and the final conclusions the thesis.

4 Preliminary findings

The findings of this paper are from the document review and there is no empirical component being reported yet. The literature related to existing policies, procedures, regulations and standards reveals that, despite the benefits of mobile money systems, mobile network operators experience information security oversight challenges when protecting financial information during and after the transactions. Previous studies of mobile money have attempted to address the security problem but gave piecemeal solutions that focus on security tools and pay little attention to the strategic management of information security (policies, awareness, training and ethics) leading to a situation that has left the problem not fully addressed.

The Uganda national ICT policy (2012) reveals that there is lack of a national information security management framework and indeed information security in developing countries is still in its infancy. A national information security management framework should provide a basis for mobile money regulation bodies in the country in order to guide and direct the implementation of adequate policies and procedures for the operation of mobile money activities.

Mobile money transactions are based largely on trust between the end users and the agents because the mobile money end user receives no tangible receipt from the agents on completion of the transaction. To make it worse there is no contractual obligation between the mobile money end users and the agents who undertake the bulk of the mobile money key activities. This poses a serious risk for mobile money end users because the legal basis is weak if they wish to raise a complaint. The SMS that is received by the mobile money end user to mark the failure or success of a financial transaction may not stand up in court as it is the only evidence available and could be falsified.

The recent “A” mobile money guidelines (drawn up in 2013) to address mobile money challenges have placed attention on the safety of financial information in mobile money transactions but the need for a collective information security role for the diverse stakeholders is not mentioned. These guidelines also indicate little concern for privacy in mobile money transactions exposing mobile money end users' accounts to risks of information breach. A guideline that leaves room for the exposure of financial information to third parties without obtaining permission and approval from the owner puts the mobile money end-user account at risk and makes it a target for abuse. It has been observed (and it appears to be common practice in Africa) for a mobile money agent to serve two mobile money end users at the same counter at the same time. This creates risks of financial information exposure and abuse.

Evans and Pirchio (2015) contend that MNO led mobile money systems that dominate in low income countries Uganda inclusive are characterized by what they termed as "*light touch regulations*". The light touch regulations mainly enforce minimal requirements about who should provide mobile money services, impose light Know Your Customer (KYC) requirements and limited restrictions and controls who should serve as mobile money agent. In a rich data environment of mobile money ecosystem where there are many stakeholders with varying interests and goals absence strong regulatory framework demands strong information security management framework to mitigate information breaches and subsequence system abuses.

UNCTAD (2012) points out that there is insufficient information security advice given to mobile money end users (customers) by the MNO. New registrants are not briefed nor are they given information related to how to minimize information security abuses in mobile money transactions. Instead these end users have to figure out how to navigate such pitfalls if and when they occur. Although MNO websites usually include frequently asked questions, questions and answers concerning information security issues surrounding mobile money systems are limited. Yet most mobile money users in Uganda, due to their limited exposure to computers and low computer literacy, neither have sufficient skills to use the internet nor are ready to access it.

The policy that guides the authorization and authentication methods used to access the mobile money application is weak given the fact that, as noted above, there are still anonymous mobile money users due to loose restriction on identification of users. The four digit PIN used by the mobile money users never changes or prompts the user to update it, and this is a problem since the majority of the users are unware of the information security preventative measures that can be used to minimize information breaches and abuses.

Atanu et al (2014) reveal that key mobile money activities and information for mobile money systems are handled by a network of third parties (mobile money agents) who have no contractual obligations to the mobile money end users. Mobile money agents register and manage mobile money customer information including mobile money account particulars. They process customer requests, process electronic money and give out cash. Exposure of mobile money information to third parties not only erodes privacy of customer transactions but also increases the risks of information security breaches because most mobile money agents also have limited knowledge and skills about information security management. Most of the abuses in mobile money systems have not been attributed to highly skilled hackers but to breaches of information by key stakeholders like agents, internal staff of MNO and unawareness of end-users about the information security risks surrounding mobile money transactions.

5 Conclusions and recommendations

Mobile money services have developed rapidly in developing economies and their benefits are enormous as outlined above. Their role in the fight against financial exclusion should not be underestimated. However, despite their benefits, mobile money systems in emerging economies raise critical information security concerns and challenges.

The future of successful and sustained mobile money use will depend on the implementation of comprehensive information security policies, guidelines, regulations and practices to assist the various key stakeholders whose interests and goals vary as illustrated in Table 1:

Table 1: Mobile money stakeholders' information security risks and concerns

Stakeholder	Role and Information security risks and concerns
Regulating bodies	*Regulate and control mobile money service companies.* However two independent regulators exist ("A" and "B") who have varying interests in mobile money systems. Each of these intend to get full control of mobile network operators yet neither of them has laid out comprehensive information security strategies to protect mobile money financial information. "A" tends to focus mainly on monetary control while "B" controls communication, leaving the security of the mobile money not fully addressed by either body.
Financial Institutions	Using the policy of regulating body "A", the financial institutions' background role is managing main mobile money accounts on behalf of the mobile network operators. However, financial institutions and mobile networker operators seem to be competitors, thus mobile banking is competing against mobile money services therefore trusting data with your competitor raises some level safety information risks to mobile network operators.
	The public image of the mobile network operators is at stake if there are incidents of information breaches and abuse by the financial institution. This is because in mobile money operations, only MNO have binding obligations with mobile money end-users yet both the financial institutions MNO have access to financial information for mobile money end-users.
Mobile Money Application Developers	These employees develop the mobile money applications but at the same time, they may be users of the applications they have developed because they are also mobile money customers. Mobile money application developers are experts who know the security weaknesses of the application

	they have developed and changes of exploiting those weaknesses in absence of strong information security policies, procedures and practices.
Mobile Network Operators (MNO)	MNO control and manage individual mobile money accounts for their customers and they are key players of mobile money security role. The mobile money information security role not been shared among all stakeholders and that leaves the mobile money security concerns not fully dressed.
Mobile Money Agents	These people register mobile money customers, process mobile money and give out cash yet they do not have binding contractual agreements with the mobile money customers. The fact that they have access to copies of financial information belonging to mobile money customers but they have no contractual obligation with them puts customers' information at risk and therefore, there is a need for strong information security policies, procedures, practices and regulations.
Mobile Device Manufacturers	These parties sell mobile devices such as the mobile phones sold to MNO. The mobile phone comes with the manufacturers' operating system and that may need to be scrutinized by MNO for security reasons. There is a possibility that a hidden code in the operating system has been inserted (possibly by a third party) and is intended to steal and share customer information with third parties. Therefore, there is need for collective information security roles among all the stakeholders including device manufacturers and this calls for strong international policies and practices.
Mobile Money End-users (Customers)	The mobile money customers use the mobile money application to do transactions through the mobile money agents. In most cases they are the ones who are affected by weak policies, procedures and practices. Literature reviewed indicates that most of the customers have limited skills, training and awareness about information security risks in mobile money payments and their security role remains inadequate.

Comprehensive guidelines are needed to bridge identified gaps such as:

- the information security role is not shared among mobile money stakeholders,
- allowing unregistered mobile phone users to get access to mobile money services constitutes a risk,
- there is a lack of concern for privacy in mobile money transactions,
- the use of third parties to handle customers' financial information needs monitoring and controls.

These weaknesses have been identified from the referenced literature. The following stage of the research will focus on checking whether these are considered to be real and pervasive problems, how they affect the various stakeholders, and finding ways to implement the recommendations.

6 References

ATANU, D., KWON, H., AND GILL, R., (2014). Mobile Money: opportunities for mobile operators. 2014 Report. https://www.google.co.za/?gfe_rd=cr&ei=98RgV_PhHO-o8weOv5nQBw&gws_rd=ssl#q=Atuna%2C+Kwon+and+Gill+2014+mobile+money+pdf [Accessed on 28/12/2016]

BOU MOBILE MONEY GUIDELINES (2013) http://ucc.co.ug/files/downloads/Mobile-Money-Guidelines-2013.pdf [Accessed on 27/12/2016]

CGAP REPORT (2015). Fraud in Uganda: how millions were lost to internal collusion http://www.cgap.org/blog/fraud-uganda-how-millions-were-lost-internal-collusion [Accessed on 07/01/2017]

DESAI, S., (2012). Mobile money for the unbanked, GSMA (annual report 2012) ttp://www.gsma.com/mobilefordevepment/wpcontent/uploads/2012/10/ [Accessed: 03/01/2017]

DITTUS, P. AND KLEIN, M. (2011), "On Harnessing the Potential of Financial Inclusion," BIS Working Papers No. 347.

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 [Access on 22/12/2016]

ELOFF, J., AND ELOFF, M., (2003). Information Security Management – A new Paradigm. Proceedings of SAICSIT 2003, South Africa.

EVANS, D., & 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 Working Paper, 723. The University of Chicago Law School. http://chicagounbound.uchicago.edu/law_and_economics/744/ [Access on 11/11/2016]

HARRIS, A., GOODMAN, S., AND TRAYNOR, P., (2013). Privacy and Security Concerns Associated with Mobile Money Applications in Africa. Washington Journal of Law, Technology and Arts, 8(3).

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1859412 [Accessed on 03/03/2017]

KPMG REPORT (2015). Mobile Banking global trends and impacts on Bank https://www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublications/Documents/PDF/mobile-banking-report-2015.pdf [Accessed on 28/12/2016]

LUVANDA, A., KIMANI, S. AND KIMWELA, M., 2014. Identifying threats associated with man-in-the middle attacks during communication between a mobile device and the back end server in mobile banking applications. IOSR Journal of Computer Engineering (IOSR-JCE), 10(2), pp.35-42.

MASAMILA, B. 2014. State of Mobile Banking in Tanzania and Security issues. International Journal of Network Security and its applications (IJNSA) 6 (4) 2014 pp 1-12

MBITI, I.; & WEIL, D. N. (2011). Mobile Banking: The Impact of M-Pesa in Kenya. National Bureau of Economic Research, Working Paper 17129.

MUDIRI, J., L., (2012).Fraud in mobile financial services, MicroSave Publication http://www.microsave.net/files/pdf/RP151_fraud_in_mobile_financial_services_JMudiri.pdf [Access: 30/12/2016]

NDIWALANA, A. AND O. POPOV (2008), Mobile Payments: A Comparison between Philippine and Ugandan Contexts. IST-Africa 2008. P. Cunningham and M. Cunningham. Namibia, IIMC.

NDIWALANA, A., MORAWCYNSKI, O., AND POPOV, O. (2014). Mobile Money Use in Uganda: a Preliminary Study. pp 8-10

OBSERVER (2013) http://www.observer.ug/business/38-business/36522-mtn-was-warned-of-likely-mobile-money-fraud-in-2009 [Accessed on 05/01/2017]

SIMPSON, R., (2014). Mobile payments and consumer protection. Consumers international report 2014. http://www.consumersinternational.org/media/1439190/ci_mobilepaymentsbriefing_jan14_final.pdf [Accessed on 03/12/2016]

UNCTAD (2014). Mobile Money for Business Development in the East African Community. A comparative Study of Existing platforms and Regulations in UNCTAD/DTL/STIC/2014/2 2014: United Nations