Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 10, October-2023

An analysis of the Potential Risks and Frauds involved in Mobile Money Transaction in Freetown Sierra Leone

A Case Study Of: Orange and Africell Mobile Telecommunication Company in Freetown, Sierra Leone.

Morris Ayodele Peacock
School of Computing and Software
Nanjing University of Information Science and Technology
No.219 Ningliu Road, Jiangsu Province, China, 210044

ABSTRACT

The research work focused on looking at an analysis of the potential risk and fraud involved in mobile money transactions in Sierra Leone with a focus on Orange and Africell mobile telecommunication companies. The implementation of mobile money service like any other financial service faces risks and challenges. This research addresses fraud as a challenge in the provision of mobile money service to customers in Sierra Leone. Mobile money usage for transactions is steadily growing across Africa with the potential to revolutionize the cash-dominant economy of this continent to be cashless. With the increased use of mobile money services and number of business use cases designed each day, it is imperative to design a holistic approach to mobile money risk, security that will reduce security exposures and prevent fraud, as some mobile money service providers have lost millions of Leones to this growing threat. This research, therefore, examines the measures that mobile network operators providing mobile money services can employ to prevent fraud. The study also discusses the mobile money users' perception about the linkage between mobile phone protection and security of the mobile money service on their phones. The research was a case study of Orange and Africell mobile telecommunication company in Sierra Leone and used qualitative and quantitative data collected through questionnaires and structured interviews of key staff of the mobile network operator (MNO), mobile money subscribers and agents of these services. Some of the main findings of this research include the general perception that there is no direct linkage between mobile phone protection and mobile money risk/security. It was further identified that one of the major causes of consumer driven fraud is PIN sharing giving it to MNO agents. In addressing mobile money fraud, it is suggested that the service provider should give mobile money security tips to the users at least twice in a year through short message service (SMS) to alert them of ways to enhance the security of their mobile phones.

Keywords: Risk, Fraud, Security, PIN sharing, Mobile network operators (MNO), Mobile money

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 10, October-2023

INTRODUCTION

Mobile money is the use of telecommunication platforms or networks by mobile phone subscribers to perform banking services. In short, mobile money enables subscribers to bank directly from their mobile phones without physically being in a financial institution to pay bills, receive money, and transact business all through virtual mobile accounts known as mobile money wallets. The use of mobile money for transactions has been steadily growing across Africa, positioned as the next "big thing" to revolutionize the cash dominant economy of Africa. A recent survey revealed that there are 20 countries in which more than 10% of adults used mobile money at some point in 2011, of which 15 are in Africa. For example, in Sierra Leone, Liberia, Ghana, Sudan, Kenya, and Gabon, more than half of adults used mobile money (The Economist, 2012). From this survey, it is evident that mobile money has become one of the "must offer" services for telecom companies in Africa. For example the top ranked telecommunication companies in Sierra Leone – Orange and Africell all offer mobile money services to their clients and usage statistics are increasing daily.

Mobile money was initially made popular by Safaricom and Vodafone's M-Pesa ("M" for "mobile", "pesa" for "money" in Swahili) in Kenya, which started in2007. The M-Pesa application is installed on the SIM cards of customers and works on all handset brands. It is free to register and the user does not need to have a bank account. Safaricom receives fees for withdrawals and transfers, but keeps deposits into the mobile wallets free. The transfer service was quickly picked up for use as an informa savings account system and electronic payment mechanism for bills, goods and services. With M-Pesa, Kenya is at the forefront of the mobile money revolution: the number of agents across the country increased by 40 percent in 2013. It is now estimated that 24.8 million subscribers use mobile money services, like M-Pesa, in Kenya (Communication Commission of Kenya, 2013). According to the Pew Research Center's 2013 survey report, the number of Kenyans using mobile wallets to make or receive payments is higher than any of the other 24 countries surveyed: 50 percent of the Kenyan adult population uses mobile money services (Pew Research Center, 2013). Mobile money services have spread rapidly in many developing countries. However, only a handful of these initiatives have reached a sustainable scale, in particular GCASH and Smart Money in the Philippines; Wizzit, MTN Mobile Money and FNB in South Africa; MTN Mobile Money in Uganda; Vodacom M-PESA and Airtel in Tanzania; Celpay Holdings in Zambia and MTN Mobile Money, Orange Money in Côte d'Ivoire. The Philippines was one of the earliest adopters of mobile money services when SMART Communications launched SMART Money in 2001. The service, which uses SIM Tool-Kits, enables customers to buy airtime, send and receive money domestically and internationally via mobile, and pay for goods using a card. In 2004, Globe Telecom launched GCASH. This service provides a cashless method for facilitating money remittances, settle loans, disburse salaries or commissions and pay bills, products and services via text message. In South Africa, MTN Mobile Money was launched in 2005 as a joint venture between the country's second largest network operator MTN and a large commercial bank, Standard Bank. In Uganda, MTN was the first operator to launch mobile money services in 2009 and remains, by far, the market leader (Intermedia, 2012). By law, each mobile money provider has to partner with a bank. However, users do not need a bank account to use mobile money services. In Tanzania, Airtel was the first mobile network operator to introduce a phone-to-phone airtime credit transfer service, "Me2U," in 2005 (Intermedia, 2013). Airtel partners with Citigroup and Standard Chartered Bank to provide m-money services, including bill payments, payments for goods and services, phone-to-phone and phone-to-bank money transfers, and mobile wallets. In 2008, Vodacom Tanzania launched the second East African implementation of the Vodafone m-money transfer platform, M-Pesa.

Finally, in Côte d'Ivoire two mobile operators, Orange and MTN, are competing head to head in the mobile money market (CGAP, 2012). Orange Money was launched in 2008 by Orange in partnership with BICICI (BNP Paribas), and MTN Mobile Money was launched in 2009 by MTN in partnership with SGBCI (SociétéGénérale) (GSMA, 2014).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 10, October-2023

In Sierra Leone 21st June 2012, Airtel Money was launched, the service provides customers with convenient access to affordable and innovative financial services through their mobile phones. The platform allows customers to top up their phones with air time, send and receive money, pay their critical utility bills, and access their Bank accounts. Airtel also partnered with International Banks and Regional banks such as Guarantee Trust Bank, Eco Bank, Sierra Leone Commercial Bank Limited, United Bank for Africa, Access Bank and Zenith Bank to provide customers with access to deposit and withdraw cash, money transfers, banking services and pay bills.

AIM AND OBJECTIVES OF THE STUDY.

The aim of this research is to analyze the potential risk and fraud involved in mobile money transactions in Freetown, Sierra Leone.

RESEARCH OBJECTIVES

- to discuss the history of Mobile Money Transfer and the contribution of Orange and Africell the development of people in Freetown the capital city of Sierra Leone.
- to assess the Challenges and risk management in mobile money transfer and issues related to fraud.
- mobile money security
- to determine the potential of Orange and Africell Mobile Money in improving the lives of people in Freetown and on the Sierra Leone monetary policy.

METHODOLOGY

The research was carried out in Freetown, which is the capital and largest city of Sierra Leone. It is a major port city on the Atlantic Ocean and is located in the Western Area of the country. Freetown is Sierra Leone's major urban, economic, financial, cultural, educational and political centre, as it is the seat of the Government of Sierra Leone. The population of Freetown was 1,055,964 at the 2015 census.

The city's economy revolves largely around its harbour, which occupies a part of the estuary of the Sierra Leone River in one of the world's largest natural deep water harbours.

The population of Freetown is ethnically, culturally, and religiously diverse. The city is home to a significant population of all of Sierra Leone's ethnic groups, with no single ethnic group forming more than 27% of the city's population. As in virtually all parts of Sierra Leone, the Krio language is Freetown's primary language of communication and is by far the most widely spoken language in the city.

The city of Freetown was founded by abolitionist Lieutenant John Clarkson on March 11, 1792 as a settlement for freed African American, West Indian and Liberated African slaves. Their descendants are known as the Creole people. The local Temne and Loko people were living in villages in the land that became known as Freetown before the European arrival.

The study was conducted in two (2) mobile telecommunication companies in Sierra Leone. The population sample used was based on two mobile telecommunication companies in Sierra Leone Orange and Africell Mobile Telecommunications Companies. The sample selected one hundred people which include staff, agents and subscribers. These one hundred people were chosen indiscriminately.

The information collected would be analysed using both quantitative and qualitative analysis. Tables and figures that would be used will be followed by interpretation and through discussion of the findings. The researcher will also embark on using pie chart on statistical packages for Social Science to be able to analyse the data

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 10, October-2023

RESULTS AND DISCUSSIONS

Data analysis and result presentation Questionnaires and interviews were used as the sources of collecting data for this research work. This chapter presents the findings of the data from the questionnaires and interviews conducted.
The researchers planned to use 120 questionnaires from the two mobile telecommunications companies, but after the disbursement of the questionnaires, 100 were retrieved in all, representing 83% of the total questionnaires administered. Data presented here mainly covers demographic information of respondents, duration of mobile money usage, fraud and actions susceptible to fraud, and mobile phone security and mobile money security. The following are the data collected from the questionnaires:
In all, 53% of the total respondents are male, while 47% are female. With regards to the age groups of respondents, 67% of the total respondents are between 18 and 29 years, 26% are also in the age range of 30 and 39 years, while 7% are between 40 and 49 years. None of the respondents fall within the 50 to 59 age group or above 60 years. Majority of the respondents, 34%, have Diploma level educational qualification, followed by 33% respondents with a bachelor's degree. Senior Secondary School (SSS) level education, those with no educational qualification and 2nd Degree holders represents 21%, 7% and 5% of total respondents respectively

Table 4-1 Duration of using Mobile Money

Options	**Frequency**	**PERCENTAGE**
< 1 years	31	31 %
1-2 years	33	33 %
3-4 years	36	36 %
Total	**100**	**100 %**

The above Table 4-1 explains the duration of using mobile money. The table shows that 31 of the respondents have used mobile money for less than one year, and 33 of the respondents have also used mobile money for over two years, whilst 36 of the respondents used mobile money for over four years respectively.

Table 4-2 Preferred point of loading money on phone

OPTIONS	**FREQUENCY**	**PERCENTAGE**
Service centres	73	73 %
Banks	12	12 %
Merchants	14	14 %
Peer-to-peer	01	01 %
Total	**100**	**100 %**

The above Table 4-2 identifies the preferred points of loading money on the mobile money wallet of the respondents. The table shows that 73 of the respondents prefer the service provider's service centre to the other sources available. 12, 14 and 1 of the respondents preferred Banks, Merchants and Peer-to-peer respectively.

Table 4-3 Preferred medium of transferring money

OPTIONS	**FREQUENCY**	**PERCENTAGE**
Own phone (self)	51	51 %
Service centres	43	43 %
Merchants	06	6 %
Total	**100**	**100 %**

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 10, October-2023

Table 4-3 above represents mobile money users' responses to the most convenient mode of transferring money. The available modes presented to the respondents are: performing the transfer on their own phone, using service centres, and visiting merchants to transfer money. Performing transfers on their own phones forms the majority of the responses: 51 out of 100. Using service centres for the transfer is another option available, and 43 of the respondents see this medium most convenient to them, and 6 of respondents preferred the merchants.

Table 4-4 Linkage between mobile phone access and risk of exploiting MM service

OPTION	FREQUENCY	PERCENTAGE
Yes	22	22 %
No	78	78 %
Total	**100**	**100 %**

From the above Table 4-4, 22 of the respondents indicated that, yes, they will be bothered if anyone has access to their mobile money, since they believe the person can also have access to their mobile money by just having access to the mobile phone. The general trend that gives these respondents the cause to worry is that they store their PINs and password on their phones, and they believe technology is advanced such that people will have means of accessing their mobile money. On the other hand, 78% of the respondents do not think it is possible for anyone to access their mobile money wallet, if a person has access to their mobile phone. Some of the reasons given for this response are that their mobile money PINs are secured, not easily guessed and known to the users alone. One respondent also gives the reason why he will not be bothered about unauthorized access to his phone:

"My password is not easy to guess and there is a threshold to the number of wrong
password attempt one can make"

Table 4-5 Does secure phone make MM service secure?

OPTION	FREQUENCY	PERCENTAGE
Yes	49	49 %
No	51	51 %
Total	**100**	**100 %**

This table (4-5) shows that 49 of the respondents agree that having a secure mobile phone definitely ensures the safety of their mobile money. However, 51% of the respondents do not think having a secure phone makes their mobile money secure in any way. The respondents in this class of thought believed that they would have to take precautions in order to protect their mobile money and not leave this to chance, because they have put in place factors to secure the phone.

CONCLUSIONS

This research has revealed that the major uses of mobile money service are for purchasing top ups and for local money transfer, as is generally believed to be the uses of mobile money in most African countries. The researchers are of the opinion that as more people have access to mobile phones as compared to bank accounts, and money transfer can be easily done on their mobile phones, this usage is very popular. More so, it is cumbersome for one to open a bank account, as several materials are required, such as government issued identity cards, references from an existing customer, as well as a form of confirmation of users' location.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 10, October-2023

Meanwhile, as compared to having a mobile money account, the process is not as complicated as opening a bank account. It can further be speculated that people are looking for easier and faster ways of sending and receiving money. It can also be argued that, as mobile money transfers are done mostly from the cities to the countryside, where most people do not have a bank account but a mobile phone is easily accessible, this could be a contributing factor for the major use of mobile money for transfer purposes.

As one of the major causes of consumer driven fraud is PIN sharing, it can be seen from this research that this is not a very common practice. However, the 9% that shared their PINs did so with their relations and sometimes with customer agents to help them in transacting one service or the other from their mobile money. It can be seen from this that, PIN sharing could be done based on trust, and if any fraud should be perpetuated through acquiring of the users' PIN, the person carrying out the fraud must first try to win the trust of the user, either by pretending to be a part of the service provider or a relative who is trying to offer a help. To avert this however, the researchers believe that the MNOs must alert users to first verify from them the authenticity of any suspected request before giving out any information that could make them vulnerable to fraud.

Despite users' awareness of their security measures they can take to prevent fraud, the service provider has a major task in securing the mobile money service, since as much as 13% believe the security of the service solely depends on the service provider. The researchers believe this category of users will invariably not put any blame on themselves if any fraud happens, since they believe total protection of the service depends on the service provider. It has also been found that even though there are several services available, such as pay bill and top up airtime, on the mobile money that users can take advantage of, the general usage of these other services are few. The researchers believe this could be as a result of the complex nature of using these services. The general perception that there is no direct linkage between mobile phone protection and mobile money protection could be attributed to the fact that users believe the service provider has put in place adequate measures to protect the mobile money service.

RECOMMENDATIONS

Some of the recommendations made are as follows:

- As PIN sharing was identified as one of the major causes of consumer driven fraud, it is recommended that the service providers must set up password age parameters for the users to change their passwords every quarter. This must further be authenticated through answering personal identification questions.
- It is also suggested that service providers must enhance their awareness about the services available on the mobile money service.
- Service providers must also create awareness to mobile money users that the security of the mobile money service does not only depend on the MNOs, but the users also have a role to play.

REFERENCES

1. Eric KodjoAfanu, Raymond SelormMamattah, 2013 — Mobile Money Security, A Holistic Approach - Luleå University of Technology, Department of Computer Science, Electrical and Space Engineering

2 JoseckLuminzuMudiri- — Fraud in Mobile Financial Services, A MicroSave Publication,

3. María Paula Subia and Nicole Martinez- International Organization for Migration (IOM), ACP Observatory on — Mobile money services: "A Bank in your pocket". Overview and opportunities.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 10, October-2023

Migration, 2014

4. Ismail, T. and K. Masinge, 2011 — "Mobile Banking: Innovation for the Poor",UNU-MERIT, Working paper 2011-074. Available from: www.rrojasdatabank.info/mobilebanking15.pdf.

5. Godfried B. Adaba& Daniel AzerikatoaAyoung, 2017 — The development of a mobile money service: an exploratory actor-network study

6. Andrew James Lake, November 2013 — Risk management in Mobile Money: Observed Risks and Proposed Mitigants for Mobile Money Operators

7. AdeyinkamAdedoyin, June 2018 — Predicting fraud in mobile money transfer

8. Lara Gilman and Michael Joyce — Managing the Risk of Fraud in Mobile Money

9. Odoyo Collins Otieno, Samuel Liyala, Benson Odongo, SilvanceAbeka – January 2016 — Challenges facing the use and adoption of Mobile Phone Money Services

