

Holistic Approach to Mobile Cash Transaction

Abba Hassan^{*}, Bala Yakubu Mohammed, Bulama Mohammed, Mohammed Lamir Isah

Department of Science & Technology, Abubakar Tatari, Ali Polytechnic Bauchi, Nigeria

ABSTRACT

The use of mobile money for transactions in Africa is steadily increasing, with the potential to revolutionize Africa's dominant cashless economy. With the increasing use of mobile money services and the number of daily business use cases, it is essential to develop a comprehensive approach to mobile financial security that reduces security exposure and prevents fraud, as some providers have lost millions of dollars of mobile money to this growing threat. This investigation was a case study on Nigerian mobile financial security and collected qualitative and quantitative data through questionnaires and structured interviews with key Mobile Network Operator (MNO) staff. The main conclusions of the research are the general notion that there is no direct link between mobile phone protection and mobile money security. It has also been found that one of the main causes of consumer-led fraud is PIN sharing. When dealing with mobile money fraud, we recommend that the service provider provide users with mobile money security tips at least twice a year through Short Message Service (SMS) to alert them to the security of their mobile phones.

Keywords: Fraud; Security; Cashless; GSM; PIN

INTRODUCTION

Mobile money is the use of telecommunications platforms or networks by mobile phone subscribers to perform banking services. In short, mobile money allows subscribers to bank directly from their mobile phones, without physically being in a financial institution to pay bills, receive money and trade through virtual mobile accounts known as mobile money portfolios. The use of mobile money for transactions has grown steadily throughout Africa, being positioned as the next "big thing" to revolutionize the dominant African cash economy. A recent survey found that there are 20 countries where more than 10% of adults used money at one time in 2011, of which 15 are in Africa. For example, in Sudan, Kenya and Gabon, more than half of adults have used mobile money [1]. From this survey, it is clear that mobile money has become one of the "must offer" services for telecommunications companies in Africa. For example, Nigeria's top telecom companies - MTN, Glo and Airtel offer their customers mobile money services, and usage statistics are growing every day.

With the increasing use of mobile money services and new use cases, it has become important to research the security practices

of mobile network operators and users to ensure the security of mobile money, to prevent fraud and to understand the user's perception. About the connections between mobile phone protection and mobile money security. Most recently, some mobile money service providers have seen an increase in fraud cases, leading to loss of millions of dollars in revenue. For example, an online newspaper reports a case of mobile money fraud MTN Uganda in which company staff stole millions of dollars from mobile money users [2]. Unfortunately, research on mobile money fraud in Africa has been limited to newspapers such as the CIO of East Africa and there has been little scientific research on this topic. Therefore, the true extent and nature of fraud issues are still fully defined for MNO and mobile users, while it is expected that the mobile money service will be extremely attractive to fraudsters.

Mobile phone sales worldwide are estimated to be worth \$ 617 billion to 448 million users by 2016 [3]. In considering this situation, given the increasing use of mobile financial services, and the use of everyday issues, it is important to design a comprehensive model of mobile financial security that will be minimized. Provide safety evidence and prevent fraud. From the

Corresponding author: Abba Hassan, Department of Science Technology, Abubakar Tatari, Ali Polytechnic Bauchi, Nigeria, Email: zumkas@yahoo.com

Received: December 17, 2020; **Accepted:** January 1, 2021; **Published:** January 8, 2021

Citation: Hassan A, Mohammed BY, Mohammed B, Isah ML (2021) Holistic Approach to Mobile Cash Transaction. J Inform Tech Softw Eng. 11:249

Copyright: © 2021 Hassan A, et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

numerous publications reviewed, it is clear that a large number of authors consider security and privacy a critical factor in the use of mobile money for payments. However, there is no clear focus on security from the start of the trade to its completion using fast cash flow for payment purposes. Most texts emphasize the central or core areas of security such as privacy, integrity, access, authentication and authorization, with no direct link to cell phone security and security.

RELATED WORK

A mobile payment or m-payment is any payment that uses a mobile device to initiate, authorize and declare an exchange of financial value in return for goods and services [4]. In this case it is mobile phones, tablets or any other device that can connect to mobile telecommunications networks and enable payment [5]. Depending on the ways the MNO lends itself to providing the service, a consumer may be restricted to the use of one or all of the other mobile devices mentioned above. M-Payments uses what is known as e-money or m-money to pay for goods and services.

Is m-money different from e-money? Electronic money has been described as a broader concept that refers to payments made using contact cards (NFC) near field communication, credit cards, prepaid cards, debit cards, automatic computers (ATMs), as well as mobile phones. Mobile money is seen as a subset of electronic money that refers to financial services and transactions made using technologies integrated with mobile phones. These services may or may not be directly linked to a personal account or related to debit, prepaid, debit or credit cards [6]. The rapid growth of mobile phone use and the lack of access to formal banking in most African countries are contributing to the rapid growth and adoption of mobile money services across most of the continent. Over one billion customers in developing markets have access to a mobile phone but do not have a formal bank account [7]. Mobile phone penetration in Africa provides the essential platform for contacting poor people in rural areas without having a financial service.

The most basic technology used for long distance transfer is short SMS (SMS) service. Technology is to the next, and use more friendly, unstructured data supplement service (USSD), and give some money transfer activities. These technologies are now among the Mobile Network Operators (MNOs) that provide a service. Another technology used in mobile money services is the latest version of the SIM Tools Application (STK), an application attached to the Card Identity Card (SIM) card, at the bottom. Portable memory used on certain mobile phones, with good network security [6]. Some service providers employ all technological avenues to provide mobile money transfer services to their customers. The basic technology, network, and devices used to provide service and mobile phones changed, years ago. Smartphones are rapidly spreading around the world at low cost, and their enhanced capabilities of mobile cash applications will move beyond the mobile cash channel and move to more competitive areas. Despite the high demand for smartphones and the potential for enhanced transactions, the operation of SMS and USSD will be critical to achieving a larger

customer base [7]. Payment faster than sales sites, NFC, for mobile phones or cards allows the user to pay by transmitting the phone or card to the recipient [6].

METHODOLOGY

Hybrid method was employed in this study, i.e. using both qualitative and quantitative methods. Quantitative approach is normally used for data collection techniques, such as questionnaire or analysis as graphs or statistics that generates numerical data. Qualitative approach, on the other hand is concerned with subjective assessment of attitudes, opinions and behavior of a phenomenon. This approach normally generates results either in non-quantitative form or in the form which does not require rigorous quantitative analysis [8-10]. The objective using this approach is for better interpretation and presentation of findings.

The systems are used in the following ways: questions were used to collect information from mobile users about their views on cell phone security and revenue security. This was further reviewed in order to draw conclusions about their views on these relationships. This process was used because some of the conclusions were presented as informants of the interviewees in order to gain an understanding of the information.

The findings of the study are examining ways in which the mobile money service can be better insured to prevent fraud. This goal is achieved by examining the methods used in the case study and the practices identified by studies on the security of accelerated funds. This study is also informative, as researchers gather data and analyze data to understand and explain what investors believe is the connection between mobile and financial security. The research study selected for this research paper is a case study. This chosen strategy helps the researchers to examine a phenomenon in its natural setting, using multiple data collection methods to gather information from one or a few entities. As case study can be used to explore, describe, or explain phenomena by an exhaustive study within its natural setting [11-14], it gives researchers the chance to employ the chosen research design (exploratory and descriptive) adopted.

The locations for data collection were influenced by the nature of the data required for this study (the responses to the interview/questionnaire from mobile money users and key personnel of the case study company). Mobile money users are based in the company's service centers in Nigeria's ten regional capitals. These service centers are located in various viewpoints along the main administrative cities with easy access to subscribers. Service centers provide mobile voice, data and money services to subscribers. In addition to service centers, there are also mobile money traders that act as a platform for receiving mobile money transfers or transferring funds by non-mobile money users. Finding merchant stores is not easy and they have small subscriber activities and are not suitable for finding mobile money users. The choice of service centers was made because, in general, more mobile money subscribers visit these service centers for other services, which is a great opportunity to find more mobile money users. The company's service centers were also chosen, as most subscribers prefer the company's service centers rather than individual third parties or

outlets. Service centers are usually concentrated in regional capitals. Client supervisory authorities in the service centers applied for the authorization to obtain the place of mobile money users and data collection by the research team.

RESULTS AND DISCUSSION

53% of the total respondents are men, and 47% are women. For age groups of respondents, 67% of total respondents are aged between 18 and 29 years, 26% are also between 30 and 39 years, and 7% are between 40 and 49 years. None of the respondents come in the age group of 50-59 years or over 60 years. Most respondents, 34%, have a diploma-level education qualification, followed by 33% of respondents with a bachelor's degree. Secondary education (SSS), those with no educational qualifications, make up 21%, 7%, respectively 5% of total respondents (Table 1).

Duration of mobile money usage, below shows how long the respondents had subscribed to the mobile money service.

Options	Frequency
<1 year	31
1-2 years	33
3-4 years	36
Total	100

Table 1: Duration of using Mobile Money.

Options	Frequency
Service centers	73
Banks	12
Merchants	14
Peer-to-peer	1
Total	100

Table 2: Preferred point of loading money on phone.

The above Table 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 center to the other sources available. 12, 14 and 1 of the respondents preferred Banks, Merchants and Peer-to-peer respectively.

Options	Frequency
Own phone (self)	51
Service centers	43
Merchants	6

Total	100
-------	-----

Table 3: Preferred medium of transferring money.

Table 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 centers, and visiting merchants to transfer money. Performing transfers on their own phones forms the majority of the responses: 51 out of 100. Using service centers 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.

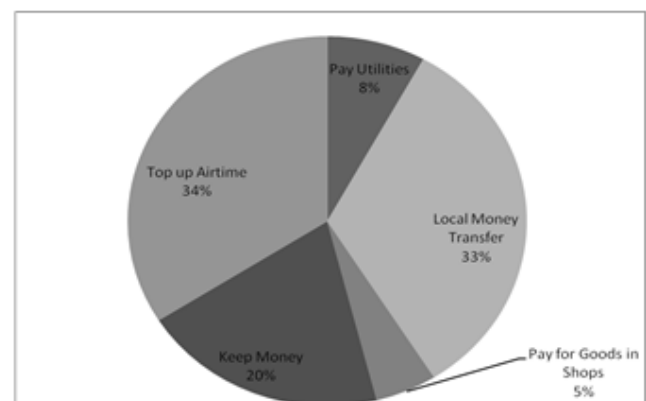


Figure 1: Mobile money usage.

Figure 1, above figure represents the percentage distribution of respondents for the various uses of mobile money. The figure shows that majority of users (34%) use mobile money for top up or the replenishments of phone airtime, followed closely by local money transfer (33%). 20% of respondents on the other hand use mobile money for keeping their money (savings), whilst 8% of respondents use the service for utilities payments and 5% use the service to pay for goods bought at shops.

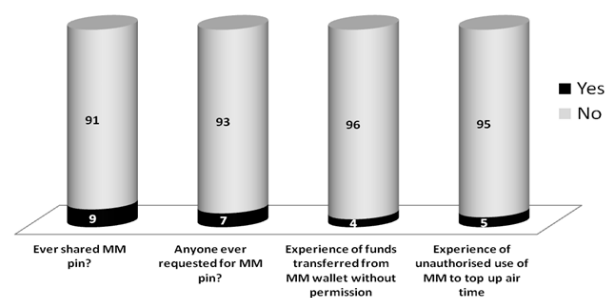


Figure 2: Actions susceptible to fraud.

Respondents were asked to disclose whether they had ever given their mobile money PIN to anyone. As shown in Figure 2, the responses obtained indicate that 9% of all respondents shared their mobile currency PIN, while 91% of users never shared. Some of the reasons why respondents did not provide their mobile money PIN to anyone was that they considered their PIN to be confidential and could not share it, while others said they would not make it public to prevent fraud. Reasons other respondents did not share their mobile currency PIN include:

“I keep money in my mobile wallet as savings, and I can’t allow my account to be ransacked”

“My security will be completely breached if I did”.

On the other hand, it was deduced that the 9% that shared their PINs do so with close relations, such as their spouses and sisters/brothers. Others share their PINS with mobile money merchants because they needed the support of the attendant at the point of transaction.

In response to the question ‘has anyone ever requested for your mobile PIN number?’ 7% of the respondents answered in the affirmative, while the remaining 93% answered in the negative, as seen in Figure 2.

Experience of unauthorized transaction from Figure 2, 4% of respondents experienced cellphone updates from their wallet without their permission, but 96% had no such experience. Similarly, 5% of respondents used money from their mobile wallet to buy unauthorized rescue time, but 95% did not have this experience. This shows that, despite the fact that transactions in users' accounts have been conducted without their knowledge, these events are fairly minimal compared to the percentage of respondents who have had this experience. The purpose of these questions was to find out the number of respondents who went on unauthorized transactions from their mobile phone accounts, which could be the basis for warning of fraud in mobile phones.

CONCLUSION

These studies revealed that the primary use of the mobile phone service is for the purchase of tops and for local transfers, as it is generally considered the use of mobile currency in most African countries. Researchers are of the opinion that because more people have access to mobile phones compared to bank accounts and easy to transfer money to their mobile phones, this use has been very popular. In addition, it is difficult for one to open a bank account as additional content, such as issued credentials, references from current customers and confirmation of user location is necessary. In the meantime, compared to owning a mobile account, the process is not as complex as opening a bank account. It can be further argued that people are looking for simpler and faster ways to send and receive money. It can also be argued that since mobile phone transfers are mainly made from rural cities, where most do not have a bank account, but mobile phones are accessible, it could affect their use. Major carriers of mobile phones.

Since one of the main causes of consumer fraud is the distribution of PINs, this study shows that this is not a very common practice. However, 9% who shared their PINs did so through their communications and sometimes to agencies to assist them in trading one or another service with their mobile money. From this, it can be seen that PIN sharing can be based on trust, and if any fraud is protected by obtaining user PINs, the fraudster must first try to gain the user's trust or by pretending to be part of a service provider or relative who tries to help. To avoid this, scientists believe that MNOs should warn users to first verify the reliability of any suspected claims before providing information that could make them vulnerable to fraud.

REFERENCES

1. One business where the poorest continent is miles ahead. *The Economist*. 2012.
2. MTN Uganda loses over USD \$3m in mobile money fraud. *Online Newspaper. CIO East Africa*. 2012.
3. Gartner CP. *Mobile Payment Market Will Experience Fragmented Service Offerings in the Short Term*. 2017.
4. Seakomo S. *Mobile phone users' information security practices, situation of students in Nigeria*, LTU-EX-2012-41518700, Sweden, 2012.
5. Herzberg A. *Payments and banking with mobile personal devices. Communications of the ACM*. 2003;46(5):53–58.
6. *Mobile Money Study* Washington, DC, 2013. IFC (International Finance Corporation)
7. *Global Mobile Money Deployment Tracker*. GSMA Mobile Money Tracker. 2012.
8. *Information and communications for development 2012: Maximizing Mobile*. World Bank .2012.
9. Saunders MNK, Lewis P, Thronhill A. *Research methods for business students*. Pearson. 2008.
10. Schwiderski-Grosche S, Knospe H. *Information Security Group, UK: Royal Holloway University of London, Egham. Secure M-Commerce*. 2002.
11. Benbasat I. *An analysis of research methodologies, in the information systems research challenge*. 1984.
12. Bonoma T V. *Case Research in Marketing: Opportunities, Problems, and a Process*. *Journal of marketing research*. 1985;22(2):199-208.
13. Kaplan RS. *The role of empirical research in management Accounting*. *Accounting, Organizations and Society*. 1986;11(5): 429-452.
14. Yin RK. *Case study research: design and methods*. Beverly Hills. 2019.