

An Analysis of the Potential Risk and Fraud Involved in Mobile Money Transaction in Freetown Sierra Leone

Morris Ayodele Peacock¹

¹ PORT LOKO UNIVERSITY COLLEGE

Received: 31 December 2021 Accepted: 26 January 2022 Published: 9 February 2022

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.

Index terms—

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.

1 I. Introduction

obile 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

44 growing across Africa, positioned as the next "big thing" to revolutionize the cash dominant economy of Africa.
45 A recent survey revealed that there are 20 countries in which more than 10% of adults used mobile money at
46 some point in 2011, of which 15 are in Africa. For example, in Sierra Leone, Liberia, Ghana, Sudan, Kenya, and
47 Gabon, more than half of adults used mobile money (The Economist, 2012). From this survey, it is evident that
48 mobile money has become one of the "must offer" services for telecom companies in Africa. For example the
49 top ranked telecommunication companies in Sierra Leone -Orange and Africell all offer mobile money services to
50 their clients and usage statistics are increasing daily.

51 Mobile money was initially made popular by Safaricom and Vodafone's M-Pesa ("M" for "mobile", "pesa" for
52 "money" in Swahili) in Kenya, which started in 2007. The M-Pesa application is installed on the SIM cards of
53 customers and works on all handset brands. It is free to register and the user does not need to have a bank
54 account. Safaricom receives fees for withdrawals and transfers, but keeps deposits into the mobile wallets free.
55 The transfer service was quickly picked up for use as an informal savings account system and electronic payment
56 mechanism for bills, goods and services. With M-Pesa, Kenya is at the forefront of the mobile money revolution:
57 the number of agents across the country increased by 40 percent in 2013. It is now estimated that 24.8 million
58 subscribers use mobile money services, like M-Pesa, in Kenya (Communication Commission of Kenya, 2013).
59 According to the Pew Research Center's 2013 survey report, the number of Kenyans using mobile wallets to
60 make or receive payments is higher than any of the other 24 countries surveyed: 50 percent of the Kenyan adult
61 population uses mobile money services (Pew Research Center, 2013). Mobile money services have spread rapidly
62 in many developing countries. However, only a handful of these initiatives have reached a sustainable scale, in
63 particular GCASH and Smart Money in the Philippines; Wizzit, MTN Mobile Money and FNB in South Africa;
64 MTN Mobile Money in Uganda; Vodacom M-PESA and Airtel in Tanzania; Celpay Holdings in Zambia and MTN
65 Mobile Money, Orange Money in Côte d'Ivoire. The Philippines was one of the earliest adopters of mobile money
66 services when SMART Communications launched SMART Money in 2001. The service, which uses SIM Tool-
67 Kits, enables customers to buy airtime, send and receive money domestically and internationally via mobile, and
68 pay for goods using a card. In 2004, Globe Telecom launched GCASH. This service provides a cashless method
69 for facilitating money remittances, settle loans, disburse salaries or commissions and pay bills, products and
70 services via text message. In South Africa, MTN Mobile Money was launched in 2005 as a joint venture between
71 the country's second largest network operator MTN and a large commercial bank, Standard Bank. In Uganda,
72 MTN was the first operator to launch mobile money services in 2009 and remains, by far, the market leader
73 (Intermedia, 2012). By law, each mobile money provider has to partner with a bank. However, users do not
74 need a bank account to use mobile money services. In Tanzania, Airtel was the first mobile network operator to
75 introduce a phone-to-phone airtime credit transfer service, "Me2U," in 2005 (Intermedia, 2013). Airtel partners
76 with Citigroup and Standard Chartered Bank to provide m-money services, including bill payments, payments for
77 goods and services, phone-to-phone and phone-to-bank money transfers, and mobile wallets. In Sierra Leone 21
78 st June 2012, Airtel Money was launched, the service provides customers with convenient access to affordable and
79 innovative financial services through their mobile phones. The platform allows customers to top up their phones
80 with air time, send and receive money, pay their critical utility bills, and access their Bank accounts. Airtel also
81 partnered with International Banks and Regional banks such as Guarantee Trust Bank, Eco Bank, Sierra Leone
82 Commercial Bank Limited, United Bank for Africa, Access Bank and Zenith Bank to provide customers with
83 access to deposit and withdraw cash, money transfers, banking services and pay bills.

84 2 II. Aim and Objectives of the Study

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

87 3 III. Methodology

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

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

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

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

102 The study was conducted in two (2) mobile telecommunication companies in Sierra Leone. The population
103 sample used was based on two mobile telecommunication companies in Sierra Leone Orange and Africell Mobile

104 Telecommunications Companies. The sample selected one hundred people which include staff, agents and
105 subscribers. These one hundred people were chosen indiscriminately.

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

109 4 IV. Results and Discussions

110 Data analysis and result presentation Questionnaires and interviews were used as the sources of collecting data
111 for this research work. This chapter presents the findings of the data from the questionnaires and interviews
112 conducted.

113 The researchers planned to use 120 questionnaires from the two mobile telecommunications companies, but
114 after the disbursement of the questionnaires, 100 were retrieved in all, representing 83% of the total questionnaires
115 administered. Data presented here mainly covers demographic information of respondents, duration of mobile
116 money usage, fraud and actions susceptible to fraud, and mobile phone security and mobile money security. The
117 following are the data collected from the questionnaires:

118 In all, 53% of the total respondents are male, while 47% are female. With regards to the age groups of
119 respondents, 67% of the total respondents are between 18 and 29 years, 26% are also in the age range of 30 and
120 39 years, while 7% are between 40 and 49 years. None of the respondents fall within the 50 to 59 age group or
121 above 60 years. Majority of the respondents, 34%, have Diploma level educational qualification, followed by 33%
122 respondents with a bachelor's degree. Senior Secondary School (SSS) level education, those with no educational
123 qualification and 2nd Degree holders represents 21%, 7% and 5% of total respondents respectively. The above
124 Table 4-1 explains the duration of using mobile money. The table shows that 31 of the respondents have used
125 mobile money for less than one year, and 33 of the respondents have also used mobile money for over two years,
126 whilst 36 of the respondents used mobile money for over four years respectively.

127 5 Global Journal of Computer Science and Technology

128 Volume XXII Issue I Version I The above Table 4-2 identifies the preferred points of loading money on the mobile
129 money wallet of the respondents. The table shows that 73 of the respondents prefer the service provider's service
130 centre to the other sources available. 12, 14 and 1 of the respondents preferred Banks, Merchants and Peer-to-peer
131 respectively. 4-3 above represents mobile money users' responses to the most convenient mode of transferring
132 money. The available modes presented to the respondents are: performing the transfer on their own phone, using
133 service centres, and visiting merchants to transfer money. Performing transfers on their own phones forms the
134 majority of the responses: 51 out of 100. Using service centres for the transfer is another option available, and
135 43 of the respondents see this medium most convenient to them, and 6 of respondents preferred the merchants.
136 From the above Table 4-4, 22 of the respondents indicated that, yes, they will be bothered if anyone has access
137 to their mobile money, since they believe the person can also have access to their mobile money by just having
138 access to the mobile phone. The general trend that gives these respondents the cause to worry is that they store
139 their PINs and password on their phones, and they believe technology is advanced such that people will have
140 means of accessing their mobile money. On the other hand, 78% of the respondents do not think it is possible
141 for anyone to access their mobile money wallet, if a person has access to their mobile phone. Some of the reasons
142 given for this response are that their mobile money PINs are secured, not easily guessed and known to the users
143 alone. One respondent also gives the reason why he will not be bothered about unauthorized access to his phone:
144 "My password is not easy to guess and there is a threshold to the number of wrong password attempt one can
145 make". This table (4)(5) shows that 49 of the respondents agree that having a secure mobile phone definitely
146 ensures the safety of their mobile money. However, 51% of the respondents do not think having a secure phone
147 makes their mobile money secure in any way. The respondents in this class of thought believed that they would
148 have to take precautions in order to protect their mobile money and not leave this to chance, because they have
149 put in place factors to secure the phone.

150 6 V. Conclusions

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

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

7 VI. RECOMMENDATIONS

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

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

180 7 VI. Recommendations

181 Some of the recommendations made are as follows: ? As PIN sharing was identified as one of the major causes of
182 consumer driven fraud, it is recommended that the service providers must set up password age parameters for the
183 users to change their passwords every quarter. This must further be authenticated through answering personal
184 identification questions. ? It is also suggested that service providers must enhance their awareness about the
185 services available on the mobile money service. ? Service providers must also create awareness to mobile money
186 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.

41

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

Figure 1: Table 4 - 1 :

42

Options	Frequency	Percentage
Service centres	73	73 %
Banks	12	12 %
Merchants	14	14 %
Peer-to-peer	01	01 %
Total	100	100 %

Figure 2: Table 4 - 2 :

43

Options	Frequency	Percentage
Own phone (self)	51	51 %
Service centres	43	43 %
Merchants	06	6 %
Total	100	100 %

Figure 3: Table 4 - 3 :

44

Option	Frequency	Percentage
Yes	22	22 %
No	78	78 %
Total	100	100 %

Figure 4: Table 4 - 4 :

4

5: Does secure phone make MM service

Option	Frequency	Percentage
Yes	49	49 %
No	51	51 %
Total	100	100 %

Figure 5: Table 4 -

-
- 188 [Gilman and Joyce] , Lara Gilman , Michael Joyce . Managing the Risk of Fraud in Mobile Money
189 [Kodjoafanu and Selormmamattah ()] , Eric Kodjoafanu , Raymond Selormmamattah . 2013.
- 190 [Odoyo et al. (2016)] *Challenges facing the use and adoption of Mobile Phone Money Services*, Collins Odoyo ,
191 Samuel Otieno , Benson Liyala , Odongo , - Silvanceabeka . January 2016.
- 192 [María Paula Subia and Nicole Martinez-International Organization for Migration (IOM) ACP Observatory on Migration ()]
193 ‘María Paula Subia and Nicole Martinez-International Organization for Migration (IOM)’. *ACP Observatory*
194 *on Migration* 2014. (Mobile money services: ”A Bank in your pocket. Overview and opportunities)
- 195 [Ismail and Masinge ()] *Mobile Banking: Innovation for the Poor*, T Ismail , K Masinge . www.rrojasdatabank.info/mobilebanking15.pdf 2011. UNU-MERIT (Working paper 2011-074. Available
196 from)
197
- 198 [Mobile Financial Services] *Mobile Financial Services*, A MicroSave Publication.
- 199 [Adedoyin (2018)] *Predicting fraud in mobile money transfer*, Adeyinkam Adedoyin . June 2018.
- 200 [Lake (2013)] *Risk management in Mobile Money: Observed Risks and Proposed Mitigants for Mobile Money*
201 *Operators*, Andrew James Lake . November 2013.
- 202 [Godfried and Adaba Daniel Azerikatoa Ayoung ()] *The development of a mobile money service: an exploratory*
203 *actor-network study*, B Godfried , Adaba & Daniel Azerikatoa Ayoung . 2017.