MITIGATION OF RISK IN THE CONTEXT OF MOBILE BANKING IN GHANA

Abstract

Mobile banking refers to the mode of making financial transactions through a mobile device, which is cell phone, computer and other digital devices. These financial transactions includes banks sending money to their clients or receiving money from their clients through mobile devices. The introduction of mobile banking has brought efficiency in the financial sector. The digital age has made mobile banking very convenient with many banks offering impressive applications. Notwithstanding these benefits, there are several security concerns and threat for the use of mobile banking. The fundamental objective of this paper was to identify risk associated with the use of mobile banking in Ghana, and to suggest mitigation measures to reduce or curtail these risks. Primary data was gathered through questionnaire in two parts that was direct/physical and online. The total number of responses received for the study were sixty six (66), and this was achieved through direct/physical and online questionnaire. The first part was direct administration of questionnaire to twenty (22) respondents at various points and this represents 33.33% of the total responses. The second part was an online questionnaire through email and WhatsApp. A total of forty four (44) responses represents 66.67 of the total responses were received through WhatsApp, and out of this number five (5) indicated that they have never used internet banking before. Table was used to analyze the data collected.

Eight (8) risks were identified through the use of mobile banking in Ghana. These risks were; receiving of misleading short message services (SMS)

Authors

Mr. Stephen Oteng
Research Scholar
Parul Institute of Commerce
Faculty of Commerce
Parul university
stephen1442003@gmail.com

Dr. Ashwinkumar Patel
Assistant Professor
Parul Institute of Commerce
Faculty of Commerce
Parul university
ashwinkumarpatel528@gamil.com

that could prompt a customer to reveal bank account information, phishing scams email that appear to have come from a customer's bank that include a call to take an action, such as change or reset of password, call from someone reporting to be bank official, needing to verify a customer login details for the purpose of confirming of an identity, mistakenly transfer of money to someone, unauthorized third parties gaining access to a customer bank accounts through using login details that have been stolen directly from mobile phone, lost devices that have mobile banking details saved in a text file, login details stolen over WiFi and hotspots of a bank customer, and delays in bank confirming of successful transaction leading to multiple transfers. The results of this study showed that the quick rise in the adoption of mobile banking services has been accompanied by a subsequent rise in fraud activity by individuals claiming to be associated with the banks. Those who have received misleading short message services (SMS) that could prompt them to reveal bank account information were twenty four (24) representing 39.34% of those who have used mobile banking before and this was the highest risks area identified. This should be a major concern to the banks, other stakeholders, policy makers and the country as a whole.

Keywords: Mitigation, Risk, Mobile Banking.

I. INTRODUCTION

The use of mobile banking has gained popularity as a growing number of people discover the benefits of having instant access to their money and bank account information. As a result of more people having access and owning mobile devices such as phones, tablets, watches , has expand the use and coverage of mobile banking in recent times. According to Okiro and Ndungu, (2013), mobile banking is the provision and execution of banking and financial services through the help of mobile telecommunication device such as the telephone or mobile phone. James C., (2020) also defines mobile banking as the act of making financial transactions on a mobile device, such as cell phone, tablet, and so on. Before the development of the mobile phone devices and its introduction for financial services, banks had its head office and branches to manage. In recent times there are several new channels introduced in the financial sector which includes; mobile banking, automated teller machines (ATMs), online help desks, call centers, point-of-sale (POS) devices, and many more.

Mobile banking had gained grounds on Ghana and it plays and continue to play a major role in how financial institutions interact with their customers. The use of mobile banking requires availability of internet service. Mobile banking represents a breakthrough for remote banking services. The days bank customers used to go to the bank branches to pay bills, check their bank account balances are things of the past. It is worth to note the distinction between mobile banking and mobile financial services. In order to understand the risks associated with mobile banking, it is essential to isolate mobile banking from the wider set of mobile financial services and products.

In a broader since mobile financial services involves the use of mobile devices to transfer money, marketing, banking, or payments for individuals or corporate institutions, however, mobile banking allows customers of a particular bank to conduct banking activities, such as checking balances, receiving accounts alerts, or making bill payments, through a mobile phone.

It is important also to note that mobile financial services which includes mobile banking involves nonbank third parties. This paper focuses mainly on mobile banking services because of its uniqueness and ongoing risks faced by financial institutions that offer these services to their customers. Mobile banking services includes; short message service (SMS) alert, customer accounts balance check, mini statements, phone credit to up, intra account transfer, bill and payment of school fees and many more. Mobile banking has a competitive advantage over traditional banking because it allows customers to perform banking transactions at any place and time. The introduction of mobile banking presents a big opportunity for both banks and customers because of its 24-hour availability, and this helps to reduce the cost of handling banking transactions.

To have proper understanding of mobile banking risk, it is equally important to understand the three most common delivery medium that banks offer to reach their customers. These mediums includes short message service (SMS), mobile enabled internet browser, and mobile applications. Banks usually send financial information to their clients through their mobile phones. It is most often used as an alert and inquiry delivery medium. These SMS are sent to customers in clear text over widely used satellites network without controls in most cases. The use of SMS can make customers susceptible to receiving of misleading messages that could prompt them to reveal vital bank account information. The

use of mobile banking through an internet browser is an extension of the online banking medium. Bank customers usually navigate to a website on their mobile phones in much the same way that they can access a site from their personal computers. Though banking from mobile devices using a mobile enabled internet browser is risky as banking from personal computer, it is harder to see and use security features on a mobile device.

The mobile banking application uses a built-in software fixed on a mobile phone that provides for a more user-friendly interface. However, the mobile application banking introduces risks that may arise if third parties have chances to know the code for these applications. Also there is the possibility that the applications can be compromised if customers install rogue, corrupted, and malicious software. Mobile banking service is regulated and for this reason banks invest heavily in the security of their services, in other to protect their assets and also to comply with various laws and regulations within the jurisdiction they operate. However, the use of mobile banking is associated with various risks of which this paper tried to uncover.

II. HISTORY OF MOBILE BANKING

In the last four decades, the birth of internet had facilitated the use of online banking. In the 1980s, the United American Bank started offering its customers a home banking services. Remote banking services started in New York around 1981. The history of mobile banking has its roots in the late 1990s and early 2000 and its introduction is strictly related to the boom of internet. The first wireless application protocol (WAP) banking appeared in Norway in 1999.The Bank of Scotland indubitably is one of the global mobile banking pioneers. This bank in 2007 announced the world's first mobile banking app for smart phones. Also Polish mobile banking pioneer Raiffeisen provided its customers with the first mobile application in 2004.

The use of mobile banking in Ghana was launched in 2009 by MTN in partnership with universal banks, and this was followed by Airtel and Tigo in 2010 and 2012 respectively. Over the years, a lot has changed in the banking industry and applications. There is no country in the world today that does not have banking application and for that matter the use of mobile banking.

III. OBJECTIVES OF THE STUDY

The objective of this study was to identity risk associated with the use of mobile banking in Ghana, and to suggest mitigation measures to reduce risk associated with the use of mobile banking in Ghana.

IV. PROBLEM STATEMENT

Mobile banking has been adopted by banks in Ghana to reach out to their various customers scattered within and outside Ghana. Mobile banking has become one of the key success factors in the banking industry with its associated efficiency. Notwithstanding its numerous benefits, risks associated with mobile banking has now become a concern for the banks as well as their customers.

V. LITERATURE REVIEW

According to Bank of Ghana, (2023), the year 2022 recorded 2998 of attempted fraud cases for the banking and specialized deposit-taking institutions (SDI) sectors, as compared to 2347 cases in 2021, representing a 27.74% increase. The total loss value recorded in 2022 stood around GH¢56million as compared to approximately GH¢61million in 2021. This shows a 7.88% decrease from 2021. The major drivers of fraud that impacted most of the financial institutions in the sector included forgery and manipulation of documents, fraudulent withdrawals, cheque fraud, cyber/email and cash theft.

The total Electronic-Money related loss recorded by PSPs in 2022 amounted to approximately GH¢26 million, a huge jump of 103% from GH¢12.8million in the previous year, 2021.Cyber fraud also saw an upsurge in the number of cases recorded in 2022. The number of cases recorded rose to 422 in 2022, as compared to 50 cases recorded in 2021, an increase of 744%.

According to Serianu (2016), most of the major mobile banking issues recorded were needless external individuals having access to financial institutional data, credential data tapped over insecure wireless networks, unencrypted data and reverse engineering. In a related study, Mahad et al, (2015), indicated that mobile devices has played and continue to play a critical role in improving efficiency, access and convenience to its users. The use of mobile devices in the banking sector has changed from just checking of account balances, viewing of account transactions and checking of bank statements during the early 2000s to a more complex financial transactions such as funds transfer, bill payments, loan applications among others .

Also in a related study by Joubert and Belle, (2013),the final results indicates that the swift development in mobile technology and its high penetration for the use in the banking sector presents an opportunity for growth especially in the developing countries . Notwithstanding the prospective of the mobile banking in enhancing financial sector inclusion, coupled with reducing cost of banking and increasing convenience and accessibility, He et al, (2015) indicates that mobile banking security threats have been on ascendency in the last 10 years. There is clear evidence from the literature reviewed the existence of risks associated with the use of mobile banking of which this paper seeks to uncover.

VI. METHODOLOGY OF THE STUDY

Primary data was used for collection of data for this study. Primary data was gathered through questionnaire in two parts. The first part was direct administration of questionnaire to twenty (22) respondents at various points and this represents 33.33% of the total responses. The second part was an online questionnaire through email and WhatsApp. A total of forty four (44) responses represents 66.67 of the total responses were received through WhatsApp, and out of this number, five (5) indicated that they have never used internet banking before. Table was used to analyze the data collected.

VII. ANALYSIS OF THE RESULT

1. **Presentation of the Data and Analysis:** The table 1 below showed the data collected on the various risks associated with the use of mobile banking in Ghana. The total number responded to the questionnaire were sixty six (66), and out of this number five (5) indicated that they have never used internet banking before. Their reason was that they do not have bank accounts. Those who have never been fallen victim of using internet banking were thirteen (13), and this represents 19.70% of the total responses received. Those who have been fallen victim in one or the other way were forty eight (48), and this also represents 72.73% of the total responses received. Those who have never used mobile before were five (5) and this represents 7.57% of the total responses received.

   Those who have received misleading short message services (SMS) that could prompt them to reveal bank account information were twenty four (24) representing 39.34% of those who have used mobile banking before. Those who have never been victims to this were thirty seven, and this also represents 60.66% of those who have used mobile banking before. Those who have been victims under this was the highest among the areas of risk associated with the use of mobile banking, and this should be a major concern to the banks, other stakeholders, policy makers and the country as a whole.

   The second highest risk area was phishing scams email that appear to have come from a customer's bank that include a call to take an action, such as change or reset of password. The total number of responses that have been victims under this risk area were 21, and this represents 34.43% of the total responses received who have used mobile banking before. The total responses that have used mobile banking were sixty one (61) and out of this number forty (40) representing 65.57% have never been victim under this risk area for the use of mobile banking.

   Based on the data received, the third highest risk area was, a call from someone purporting to be bank official, needing to verify a customer login details for the purpose of confirming of an identity. Those who have been victims under this risk area were sixteen (16) representing 26.23% of the total respondents who have used internet banking before. Those who have not been victims under risk area were forty five (45) representing 73.77% of the total responses received who have used mobile banking before.

   The fourth highest risk area associated with the use of mobile banking was a bank customer mistakenly transferred money to someone. The total number that have been victims to this risk area were twelve (12) representing 19.67% of the total responses that have used mobile banking before. However, those who have not been victims under this risk area were forty nine (49), and this represents 80.33% of the total responses that have used mobile banking before.

   The unauthorized third parties gaining access to a customer bank accounts through using login details that have been stolen directly from mobile phone was the fifth highest risk area identified under those using mobile banking. Those who have been a victim under this risk area were eight (8), and this represents 13.11% of the total respondents that have used mobile banking before. The data also showed that 86.89% of the total respondents have never been victims to this risk area.

Lost devices that have mobile banking details saved in a text file was also the sixth highest risk area based on the responses received. Those who have been victims under this risk area were four (4), and this represents 6.56% of those who have used mobile banking before. Those who have not been victims under this risk area were fifty seven (57), and this represents 93.44% of the total responses received.

The last but not the least risk area identified was login details stolen over WiFi and hotspots of a bank customer. The total number of respondents who have been victims under this risk area were three (3) representing 4.92%. Those who have not been victims under this risk area were fifty eight (58), and this also represents 95.08% of respondents who have used mobile banking before. A customer indicated that he had a challenge of making more than one transaction due to delays of bank confirming successful transaction. Another customer also mentioned that a scammer was able to detect his bank account details without his knowledge.

Table 1: Number of Risks Associated with Mobile Banking

	QUESTION	YES		NO		TOTAL
		Number	Percentage	Number	Percentage	
1	Receiving misleading short message service (SMS) that could prompt a customer to reveal bank account information	24	39.34%	37	60.66%	61
2	Unauthorized third parties gaining access to a customer bank accounts through using login details that have been stolen directly from mobile phone	8	13.11%	53	86.89%	61
3	Login details stolen over WiFi and hotspots of a bank customer	3	4.92%	58	95.08%	61
4	Lost and stolen devices that have mobile banking details saved in a text file	4	6.56%	57	93.44%	61
5	Phishing scams email that appear to have come from a customer bank that include a call to take an action, such as change or reset of password	21	34.43%	40	65.57%	61
6	A call from someone reporting to be bank official, needing to verify a customer login details for the purpose of confirming of an identity	16	26.23%	45	73.77%	61
7	A bank customer mistakenly transferred money to someone	12	19.67%	49	80.33%	61

VIII. CONCLUSION AND RECOMMENDATIONS

Most at times fraudulent activities by scammers in mobile banking can be difficult to notice, and clients often do not know they were been monitored or targeted until after the event is happened. This situation can lead to bank customers to have doubt of mobile banking services, mainly for clients who have a higher chance of experiencing fraud.

The various literatures that were reviewed and the results of this study showed that the quick rise in the adoption and using of mobile banking services has been accompanied by a subsequent rise in fraud activity by individuals claiming to be associated with the banks.

It is very important of the customers of the various banks to know and understand the various risks associated with the use of mobile banking for business transactions. This can be achieved through continuous education by the various banks. It is advisable also for the customers to download their mobile bank application through their banks websites, and stop using mobile banking through unsecured WiFi networks.

Customers should verify from their respective banks when they receive any messages or calls that is purported of coming from their banks to take any action on their mobile banking application.

Banks must also put in place mechanisms that will ensure the safety for the use of mobile banking by customers. There are various safety measures which the banks can put in place to curtail fraud associated with the use of mobile banking. These safety measures includes; end- to-end encryption such as advanced encryption standard (AES), and full disk encryption solutions, encryption software that convert data into code, the banks should insure the mobile banking operations, banks should send short message service (SMS) notification to the phone number of the customer on every transaction made, the use of biometric identity verification through thumb or facial verification, and finally customers should provide consent letters, for instance when transactions are above a certain threshold.

REFERENCES

[1] Bank of Ghana, (2023), Banks, Specialized Deposit-Taking Institutions (SDIs), Payment Service Providers (PSPs) Fraud Report. https://www.bog.gov.gh› N...PDF
[2] He, W., Tian, X., & Shen, J. ,(2015). Examining Security Risks of Mobile Banking.
[3] James Chen (2020). *Mobile Banking*.https://www.investopedia.com/terms/m/mobile-banking.asp
[4] Mahad, M., Mohtar, S., Yusoff, R. Z., & Othman, A. A., (2015). Factor affecting mobile adoption companies in Malaysia. *International Journal of Economics andFinancial Issues, 5*, 84-91.
[5] Okiro, K., & Ndungu, J., (2013). The impact of mobile and internet banking on performance of financial institutions in Kenya. *European Scientific Journal,9*(13), 146-161.Applications through Blog Mining. *Research Gate*, 1-6.
[6] Seriano,(2016).Kenya,Cyber,Security,Report.https://www.serianu.com/downloads/KenyaCyberSecurityReport2016.pdf.

