ADDIS ABABA UNIVERSITY
COLLEGE OF BUSINESS AND ECONOMICS

SECURITY ISSUES IN MOBILE BANKING SERVICE IN ETHIOPIA

A Project Submitted to the College Of Business and Economics of Addis Ababa University in Partial Fulfillment of the Requirements for the Degree of Master of Business Administration Specialization in Financial Service

By

BIRUK ARGAW

Advisor

MESFIN FIKRE (PHD)

Addis Ababa, Ethiopia
May 2018

ADDIS ABABA UNIVERSITY
COLLEGE OF BUSINESS AND ECONOMICS

SECURITY ISSUES IN MOBILE BANKING SERVICE IN ETHIOPIA

By

BIRUK ARGAW

Name and Signatures of Members of approving and Examining Board

Name	Title	Signature	Date
Lemessa Bayissa(Phd)	Examiner	_____	_____
Tekalign Nega(Phd)	Examiner	_____	_____

DECLARATION

I declare that security issues in mobile banking service in Ethiopia is my own work and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

Biruk Argaw	_____	_____
Name	Signature	Date

This study has been submitted for examination with my approval as university advisor.

Advisor: -**Mesfin Fikre (PHD)**

Signature _____

Date_____

DEDICATION

This study is dedicated to Memory of construction and business bank for giving me a chance of study this MBA program and for my family for the inspiration they gave me during my studies.

ACKNOWLEDGMENT

Next to God, I would like to give special thanks to my advisor Dr Mesfin Fikre, for always being there whenever I need help. The thesis would not have this shape without his professional inputs, criticism, guidance and support.

I would like to use this opportunity to thank the Public Finance agency and construction and business bank that give me full sponsorship for my study, and all banks who cooperate and allow me to gather information and the management staff who took their time and respond to my interview. I would like to say thank you all.

Last but not least, I would like to extend my thanks to my wife, my children and friends for their support, encouragement and pray not only during my thesis work but also all the way during my study.

Table of Contents

LIST OF ACRONYMS

ATM	Automatic Teller Machine
AVR	Automated Voice Response
CBS	Core Banking Solution
E-Banking	Electronic Banking
E-Payment	Electronic Payment
LMTS	Local Money Transfer Service
IT	Information Technology
M-Banking	Mobile Banking
M-Payment	Mobile Payment
NBE	National Bank of Ethiopia
PDA	Personal Digital Assistant
PIN	Personal Identification Number
POS	Point of Sale
SMS	Short Message Service
USSD	Unstructured Supplementary Service Data
WAP	Wireless Application Protocol

ABSTRACT

The mobile banking services is one of the newly introduced services designed to enable customers transact 24 hours in a day and seven days a week without the need to go to the bank's counter. The major challenges for the adoption of mobile banking technologies are customer concerns about security therefore the major objective of this study is, to assess current security practices and customer protection of mobile banking service in Ethiopian banks. The research was conducted by using exploratory research design and focus on qualitative methods like focus group, interview and content analysis approaches have a foundation for the study and data analysis. The paper tried to explore and identify major potential security issues and protection challenges. In order to manage the issue of mobile banking security and enhancing customer protection, the paper tried to conclude and recommend that the banks would have implement best and strong security framework for prevention and detection mobile banking services. This should include customer education and awareness, strong authentication; secure mobile applications, strict account set up and management processes, real time detective services, and 24x7 customer supports.

Keywords

Mobile Banking, Security issues and Customer protection

1. INTRODUCTION

1.1 Background of the Study

A bank is an institution which accepts deposit from businesses, institutions and individuals and engages in investment and consumer lending. Bank helps to mobilize and distribute the idle resources to potentially productive sectors, aiming to raise the level of economic development as a whole. If the banking industry does not perform well, then the effect to the economy could be huge and broad, because, banks are the critical part of financial system, play a pivotal role in contributing to a country's economic development.

According to the guideline of ICT security (2015) of Bangladesh bank the banking industry has changed the way of providing services to their customers and processing of information in recent years; Information Technology (IT) has brought this momentous transformation; Electronic banking is becoming more popular and enhancing the adoption of financial inclusion; Security of Information for financial institutions has therefore gained much importance and it is vital for us to ensure that the risks are properly identified and managed; Moreover, information and information technology systems are essential assets for the Banks as well as for their customers and stakeholders.

Information system has become the heart of modern banking in our world today. The Banking sector in Ethiopia is one of the rapidly growing sectors of the country's economy. In addition, the banking service has shifted from local banks to national and global presence and anywhere-anytime banking. According to Patrick (2011) the Banking business competition has motivated the advancement of services enabled by IT which in turn increased the information security risk. These threats to information and information systems can include purposeful attacks, environmental disruptions, and human/machine errors and result in great harm to the national and economic security interests of the country (Patrick, 2011).

Technology has brought a paradigm shift in the functioning of banks and delivery of banking services the growth of the internet, mobile, ATMs and communication technology has added a different dimension to banking industry; today, some of the transactions (balance enquiry, fund transfer ,bill payment, beneficiary management etc…) can be done from the comforts of one's

home without visiting a bank's branch this indicates that technology is no longer an enabler, but a business driver (IDRBT, 2011).

According to Negalign & Lisanwork (2016) the Ethiopian Banks have been implementing comprehensive Banking software known as Core Banking Solution (CBS) in accordance with the guidelines of the National Bank of Ethiopia (NBE). CBS helps each bank to acquire and implement state-of-the-art centralized banking application software that provides the needs of all branches of the Bank and its Head Quarter. Ethiopian Banking system has been going through transformation processes and technological shifts so as to render services that are modern and up to the expectations of customers. These perpetual transformations are adopting the latest technologies and introduce new services. The mobile banking services is one of the newly introduced services designed to enable customers transact 24 hrs. in a day and seven days a week without the need to go to the bank's counter. Mobile banking service offer a wide range of services to customers such as fund transfer, payments, bill payments, balance enquiry and various information type service.

1.2 Statement of the Problem

The rapidly growing information and communication technology (ICT) is knocking the front door of every organization in the world, where Ethiopian banks would never be exceptional. In the face of rapid expansion of electronic payment (E-payment) systems throughout the developed and the developing world, Ethiopian's financial sector cannot remain an exception in expanding the use of the system (Gardachew, 2010).

Technological innovations play a crucial role in banking industry by creating value for banks and customers, that it enables customers to perform banking transactions without visiting a brick and mortar banking system on the other hand E-banking has enabled banking institutions to compete more effectively in the global environment by extending their products and services beyond the restriction of time and space (Turban, 2008).

According to Federal Reserve Board research of 2015 the two major challenges for the adoption of mobile banking technologies are (1) concerns about security and (2) the possibility of hackers remotely accessing consumers' phones (Consumer and Mobile Financial service, 2012). Generally, now a day the banking industry along with the use of Information technology is expanding dramatically in Ethiopia during recent periods. However, the work done with regard to information security is almost none compared to the expected effort.

Ethiopian Banking system is still underdeveloped compared to the rest of the world regarding electronic payment, Internet Banking, mobile banking and online shopping as noted by different scholars such as Abiy & Lemma (2012), Ayana (2012) and Balcha (2012) the reason for this weak or evolutionary development is being numerous; the main one is security threats or poor implementation of Information system security in the country. However these study doesn't mention to what extent this security challenge hinder the E-Banking service in general and for mobile banking in particular.

Taking these facts into consideration in this study would like to assess the current status and practices of security and customer protection in mobile banking service in Ethiopia Banking industry by taking sample of them. Thus, the study has the following objectives and questions.

1.3 Research Questions

1. What kind of mobile banking security practice employed by the Ethiopian banks?
2. What are the major problems that hinder the security process of mobile banking service in Ethiopian banks?
3. What kind of customer protection mechanism employed by Ethiopian banks to protect their customers in relation to mobile banking security?
4. What kind of awareness creation mechanism used in relation to the security of mobile banking service for the customer

1.4 Objectives of the Study

1.3.1. General Objective

The major objective of this study is, to assess current security practices of mobile banking service and customer protection in Ethiopian banks

1.3.2. Specific Objectives

1. To identify the security practices employed in mobile banking service in the Ethiopian Banks.
2. To identify the predominant problems that hinder the security process in mobile banking service in Ethiopia.

3. To identify the customer protection mechanism employed by banks to protect their customers in relation to mobile banking service
4. To identify the awareness creation mechanism used in relation to the security of mobile banking service for the customer

1.5 Significance of the Study

The researcher believes that this study has the following significance for different parties. These are: The result of this study shows the states of security in mobile banking service; It enables all banks to have a common understanding for the development of security in mobile banking service in Ethiopia; The employees and the customer could be able to get a better practice via a body of knowledge; It also serve as a starting point for practitioners and researchers who want to conduct more comprehensive research in this area from Ethiopian banking sector perspective.

1.6 Delimitation of the Study

The result of the research would be more comprehensive if it covers the entire banks in Ethiopia. However, due to financial and other constraints, it is delimited to some sample banks head quarter and main branches in Addis Ababa. The head quarter and main branch are the place where major information, security resources and facilities and the office of E-payment and IT staffs are sited. These staffs can provide the necessary information about the study better than other staffs who work at branch level.

1.7 Limitation of the Study

The research aims to develop an instrument that measure the level of security when using mobile banking service in the Ethiopian banking context for which there is no prior instrument developed and due to financial and other constraints the research has forced to focus on selected banks headquarters and branches of sampled banks Therefore, the study has a significant constraint to develop a proper instrument and finding those samples that fill the real test each dimensions in mobile banking due to inexperience also be a difficult task and finally finding related secondary data sources have the expected drawbacks for the study.

1.8 Organization of the Study

The research constitutes five chapters. The first chapter deals with the Introduction like background of Ethiopian banks, statement of the problem, research questions, objectives and significance of the study. The second chapter deals with the literature review which provides both conceptual and contextual ground in the existing body of knowledge related to Mobile Banking and the security issues in mobile banking industry. The third chapter presents the research design and methodology used in the study. In chapter four, the data gathered from research participants has analyzed and its results would present and discussion. Conclusion and recommendations would be present in the final chapter which is chapter five.

2. LITERATURE REVIEW

2.1 The Evolution of E- Banking System

Electronic innovation in banking industry can be traced back to 1970, when the computerization of financial institutions gained momentum; however a visible presence of this was evident to the customers since 1980, with the introduction of ATM (Malak 2007).

Innovative banking has grown since then, aided by technological developments in the telecommunications and information technology industry. The early decade of the 1990s witnessed the emergence of automated voice response (AVR) technology. By using the AVR Technology, banks could offer telephone banking facilities for financial services. With further advancements in technology, banks were able to offer services, through PC owned and operated by costumers at their convenience, through the use of intranet propriety software. The users of these services were, however, mainly corporate customers rather than retail ones (Sohail & shanmugham, 2003). The security first network bank was the first Internet banking in the world that was built in 1995 in USA. After that some famous banks introduced their internet banking one after another, such as City bank and bank of America.

2.2 E-Banking System in Ethiopian Banking Industry

The appearance of E-banking in Ethiopia goes back to the late 2001, when the largest state owned, commercial bank of Ethiopia (CBE) introduced ATM to deliver service to the local users. In addition to eight ATM Located in Addis Ababa, CBE has had Visa membership since November 14, 2005. But, due to lack of appropriate infrastructure it failed to reap the fruit of its membership. Despite being the pioneer in introducing ATM based payment system and acquired visa membership, CBE Lagged behind Dashen bank, which worked aggressively to maintain its lead in E-payment system. As CBE continues to move at a snail's pace in its turnkey solution for Card Based Payment system, Dashen Bank remains so far the sole player in the field of E-Banking since 2006 (Gardachew 2010).

According to the annual report of Dashen bank (2011) Dashen bank, a forerunner in introducing E-banking in Ethiopia, has installed ATMs at convenient locations for its own cardholders; Dashen's ATM is available 24 hours a day, seven days a week and 365 days a year providing service to Debit Card holders and International Visa Card holders coming to the country; At the end of June 2009

Dashen bank has installed more than 40 ATMs in its area branches, university compounds, shopping malls, restaurants and hotels. In the year 2011 the payment card services have witnessed significant strides, Dashen's ATM service expanded to 70 and 704 POS terminals.

The annual report of Dashen bank (2011) further discussed that available services on Dashen Bank ATMs are: Cash withdrawal, Balance Inquiry, Mini statement, Fund transfer between accounts attached to a single card and Personal Identification Number (PIN) change; the bank gives debit card service only for Visa cards; Dashen bank clients can withdraw up to 5,000 birr in cash and can buy goods and services up to 8,000 to 13000 birr per day; Expanding its leadership, Dashen Bank has begun accepting MasterCard in addition to Visa cards; Dashen won the membership license from Master Card in 2008.

Harnessing its leadership with advanced banking technology, Dashen Bank signed an agreement with iVery, a South African E-payment technology company, for the introduction of mobile commerce in April 21, 2009. According to the agreement, iVery Payment Technologies has licensed its Gateway and MiCard E-payment processing solution to Dashen Bank. Dashen's Modbirr users can transfer 500 birr to other Modbirr users in 24 hours a day. This would make Dashen Bank the first private bank in Ethiopia to acquire E-commerce and mobile merchant transactions (Amanyehun, 2011). Although Dashen's new technology is one step ahead in that it allows transfer of funds from one's account to others, the first ever E-banking gateway was signed between Ethiopian Commodity Exchange (ECX) and Dashen Bank and CBE. The E-banking system being developed with both banks is designed to give a secure electronic data sharing gateway between clients, banks and ECX, by facilitating a smooth transaction (Abiy, 2008)

By the end of 2008 Wegagen Bank has signed an agreement with Technology Associates (TA), a Kenyan based information technology (IT) firm, for the development of the solutions for the payment system and installation of a network of ATMs on December 30, 2008 (Ayana, 2014).

Zemen Bank, the only Ethiopian bank anchored in the idea of single branch banking, by launching full-blown internet banking, a service which is new to Ethiopian banking industry in the year 2010. The bank tested the venture through its first phase of the online service, and now it is already started the full-fledged version, which enable customers to make online money transfer freely. Previously, the online banking service, delivered by the bank, only gave access to bank statements and exchange rate information. The new and never-been-tried service proposed by the bank is to include free account money transfer, corporate payroll uploading system where employers could

upload payroll to the system and make payments to individual worker's accounts online and online utility bill settlement system, when utility companies are ready (Asrat 2010).

The agreement signed by three private commercial banks to launch ATM and POS terminal network, in February 2009 is welcoming strategy to improve electronic card payment system in Ethiopia. Three private commercial banks - Awash International Bank S.C., Nib International Bank S.C. and United Bank S.C. have agreed in principle to establish an ATM network called Fettan ATM network. If everything goes as planned, Fettan ATM will install over 140 ATM machines and over 340 POSs across Ethiopia. There will be one ATM at every branch of the consortium banks, all domestic airports serviced by Commercial service, shopping complexes and merchants. The agreement is the first significant cooperation between competing banks in Ethiopia, which others should be encouraged to follow as there is no single bank in Ethiopia that can afford to provide Extensive geographical coverage and access (Binyam 2009).

2.3 E-Banking Challenges in Ethiopia

Banking in Ethiopia faces numerous challenges to fully adopt and adapt E-Banking applications and seize the opportunities presented by ICT applications in general. As noted by different scholars such as Gardachew (2010); Ayana (2014) and wondwossen & Tsegai (2005) various Challenges for E-Banking applications in Ethiopia are summarized as follows:

Low level of internet penetration and poorly developed telecommunication infrastructure: Lack of infrastructure for telecommunications, Internet and online payments impede smooth development and improvements in e-commerce in Ethiopia. Most rural areas of the country, where the majority of small and medium businesses are concentrated, have no Internet facilities and thus are unable to engage in e-commerce activities.

Lack of suitable legal and regulatory framework for e-commerce and e-payment: Ethiopian current laws do not accommodate electronic contracts and signatures. Ethiopia has not yet enacted legislation that deals with e-commerce concerns including enforceability of the validity of electronic contracts, digital signatures and intellectual copyright and restrict the use of encryption technologies.

High rates of illiteracy: Low literacy rate is a serious impediment for the adoption of E-Banking in Ethiopia as it hinders the accessibility of banking services. For citizens to fully enjoy the benefits of E-Banking, they should not only know how to read and write but also possess basic ICT literacy.

High cost of Internet: The cost of Internet access relative to per capita income is a critical factor. Compared to the developed countries, there are higher costs of entry into the e-commerce market in Ethiopia. These include high start-up investment costs, high costs of computers and telecommunication and licensing requirements.

Frequent power interruption: Lack of reliable power supply is a key challenge for smoothly running e-banking in Ethiopia.

Lack of awareness creation on the benefits of new technologies: fear of risk, lack of trained personnel in key organizations, tendency to be content with the existing structures, people may be resistant to new payment mechanisms

Cyber security issues: Cyber security is a global challenge that requires global and multi-dimensional response with respect to policy, socio-economic, legal and technological aspects. E-banking applications represent a security challenge as they highly depend on critical ICT systems that create vulnerabilities in financial institutions, businesses and potentially harm banking customers. It is imperative for banks to understand and address security concerns in order to leverage the potentials of ICTs in delivering E-banking applications. In the deployment of E-banking application, attention should be drawn to the prevention of cyber crime (i.e. the use of ICTs by individuals to commit fraud and other crimes against banking transactions).

2.4 Development of Mobile Banking

Mobile Commerce (m-commerce) is defined as a business transaction conducted through mobile communication networks or the Internet (Siau & Shen, 2003). M-commerce can offer value to consumers through convenience and flexibility by enabling time and place independence.

Mobile banking is an application of m-commerce which enables customers to access bank accounts through mobile devices to conduct and complete bank-related transactions such as balancing cheques, checking account statuses, transferring money and selling stocks (Tiwari & Buse, 2007). (Luo, Li, Zhang and Shin, 2010), defined mobile banking as an innovative method for accessing banking services via a channel whereby the customer interacts with a bank using a mobile device (e.g. mobile phone or personal digital assistant (PDA)).

Mobile banking refers to the use of a smart phone or other cellular device to perform online banking tasks while away from your home, such as monitoring account balances, transferring funds between accounts and other.

According to FATF guidance (2013) Mobile Banking as they are offered today is the result of an evolutionary process which started with the spreading of the mobile telephony around the world in late 1990s; The first stage of this evolutionary process can be related to the inherent data communication capability of mobile phones, which caught the attention of banks, prompting them to start launching basic inquiry services like account balance inquiry, and slowly starting expanding the range of functions to also include transaction services such as funds transfer; These sets of services collectively started being referred to as "mobile banking"; This stage is mostly characterized by banks being the main actors in the provision of mobile payments services; Such mobile banking services are distinct from bank-centric mobile payment models where new products or services are delivered to new customers.

2.4.1. Operation Overview

According to Ahmad & Zakarya (2015) Mobile Banking is designed for mobile phone users and offers them services that enable them to conduct their financial transactions through a mobile device such as a mobile phone or tablet. The architecture of the Mobile Banking System is depicted in Figure below, which shows the main functional components, their roles and contribution within the system.

Ahmad & Zakarya (2015) further discussed that the Mobile Banking Equipment is what is at the end–user's hand to access the information and services provided by the system. The Mobile Banking Equipment displays the menu and performs secure short message creation and transmission based on the user's selection. The Mobile Banking Platform is split into two functional blocks, which may be separated and operated by the Network Provider and the Service Provider respectively.

Additionally Ahmad & Zakarya (2015) mentioned that The Mobile Banking Platform transfers the short message received from the Mobile Banking Equipment into conformant commands of a selected banking protocol. Interaction between User and Service Provider system is supported by multilevel dialogs. The Bank Account Server as part of the system provides the respective banking support. It receives the instructions to provide the necessary functions to be performed on the bank accounts and communicates the results and status back to the Mobile Banking Platform. The Mobile Banking System supports communication with other servers, such as Internet Information

Servers. These participate in the environment and contribute other services and information to enhance the service offering to the user.

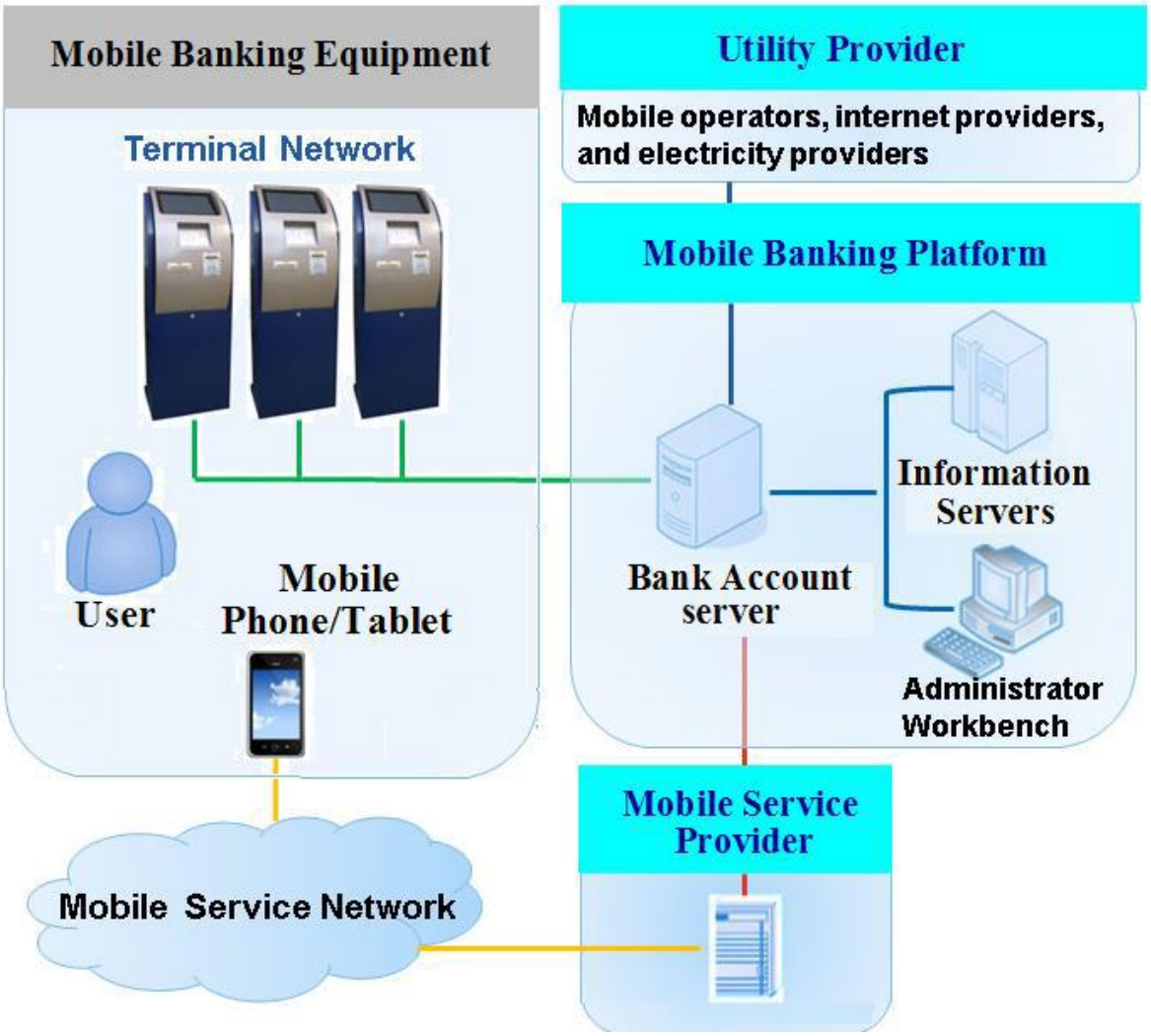

Figure: Mobile Banking System Architecture (Ahmad & Zakarya, 2015)

2.4.2. Trends in the Utilization of Mobile Banking

Mobile banking has the potential to revolutionize the customer experience in personal financial services, with nonbank organizations often leading the way (Keramati et al., 2012; Kesenwa, Oima, & Oginda, 2013). Mobile banking offers great opportunities for financial institutions to expand their market share and for unbanked to participate in the global financial system (Berger & Nakata, 2013; Dikit et al., 2012; Hinson, 2011). Usage of smartphones is increasing, while new applications are proliferating and banks across Europe are mobilizing to respond to the growing mobile opportunity (Berger &Nakata, 2013; Kang & Kim, 2012; Keramati et al., 2012). Embracing of

mobile banking services is on the increase, with an increasing number of mobile phone users enrol in mobile banking services (Berger & Nakata, 2012). As the smartphone users are continuously increasing, so will mobile banking users. Services like mobile banking allow customers to get account facts and do transactions and allow consumers to make payments & transfers (Ahmad & Singh, 2012; Comninos, 2008; Tobin, 2012). Dittus and Klein (2011) confirm that there is an increased use of mobile phones users for mobile banking services since 2010. The presence of mobile banking by 2012 had risen; 28% of mobile phone users and 48% of smart phone users (Hoon et al., 2013). In 2013, mobile disbursement services noted growth with increased access to locations for retail customers (Neil & Pénicaud, 2014).

Mobile banking is a system wherein the customers are allowed to do financial transactions through a device called mobile or personal digital assistant. Mobile banking services are easily accessible to everyone irrespective of their income groups (Keramati et al., 2012). There are various types of mobile financial transactions and services and the services are expanding with the technological advancements.

The mobile banking service in Ethiopia is endowed with huge potential as the sector remains untapped (Getnet, 2014). For the banked customer mobile banking mostly creates convenience and for addressing financial inclusion, mobile money (e-wallet) plays vital role, which may impact expanding access to finance (William & Suri, 2014). As of 2014, there were about 28.3 million mobile phone subscribers in Ethiopia, recording an annual growth rate of 19.2% (Getnet, 2014). The mobile phone subscribers' penetration rate is increasing in each year. In 2014, the mobile phone penetration rate reached at 33.3% (Getnet, 2014). The growth of mobile phone subscribers in Ethiopia presents an opportunity for the development of the mobile banking service.

2.4.3. Types of Mobile Banking Delivery Channel

According to mobile marketing association report in creating a mobile banking solution, financial institutions use a variety of mobile media channels including Short Message Service (SMS), Unstructured Supplementary Service Data (USSD), mobile client applications and mobile web, (XHTML). Each mobile banking media channel has its strengths and weaknesses, and it is important to identify the delivery mode that is most appropriate for each banking service. As yet, no common standard for mobile services has been developed among national and/or global banks. As banking customers rapidly respond to mobile banking solutions, it will be beneficial for banks to

work collaboratively to develop mobile banking guidelines at national and global levels. Each delivery mode has its advantages and disadvantages.

I. Short Message Service (SMS) based Channel

According to mobile marketing association report SMS-based mobile banking was the first channel that enabled customers to interact with their bank using a mobile device. SMS messages are short; typically limited to 160 characters per message, and can be sent and received by all mobile phones. The financial institution and customer use text messages to exchange financial information and instructions within the parameters set by the bank. SMS channel has a variety of advantages and disadvantages for financial applications and services.

The mobile marketing association report further discussed that the advantages are easy-to-use, common messaging tool among consumers, works across all wireless operators, affordable for consumers, compatible with all mobile devices, require no software installation, stored messages can be accessed without a network connection and allow banks and financial institutions to provide real- time information to customers and employees; The disadvantages are make transact with one time password or pin, text-only and limited to 140-160 characters per message and does not offer a secure environment

II. USSD Channel (Unstructured Supplementary Service Data)

According to CBE Mobile Banking user guide USSD (Unstructured Supplementary Service Data) is a Global System for Mobile communication technology that is used to send text between a mobile phone and an application program in the network.

According to mobile marketing association report USSD is a data bearer channel in the GSM network. Like SMS, it transports small messages of up to 160 characters between the mobile handset and the network. Unlike SMS, which is 'store and forward', USSD is session based and can provide an interactive dialog between the user and a certain set of applications. In other words, both sides of the dialogue happen during a session whereas an SMS based interaction is broken into each segment of communication between the client and the service.

According to CBE Mobile Banking user guide USSD is similar to Short Messaging Service (SMS), but, unlike SMS, USSD transactions occur during the session only. With SMS, messages can be sent to a mobile phone and stored for several days if the phone is not activated or within range. E.g. *889# --→ dial in case of CBE

According to mobile marketing association report USSD channel has a variety of advantages and disadvantages for financial applications and services the advantages are high speed, Compatible with all mobile devices, low cost and need only mobile network no need of internet access the disadvantages are low security, Data sent in plain text not encryption.

III. **Smart Client Application Channel** (android iPhone...)

According to mobile marketing association report Technological advancements in mobile handsets will introduce and create a more secure, user-friendly environment with many rich features for both banks and their customer base. However, there are still many issues that need to be overcome before downloading applications to handsets. Mobile client applications are a rapidly developing segment of the global mobile market. Mobile client applications (downloadable, client applications) are common on most mobile phones today and are key to providing user interfaces for basic telephony and messaging services, as well as for more advanced and entertaining experiences such as playing games, browsing and watching videos on mobile phones; This form of mobile banking channel uses a custom-designed software application installed on the customer's mobile device. The application is unique to each device operating system, providing the most user-friendly experience of the four delivery channels. In fact app-based mobile banking is now the fastest growing delivery channel.

The mobile marketing association report further discussed that Mobile client applications can offer powerful and secure application functionality while protecting the consumer and the application data on the mobile handset. Once installed and configured on the mobile handset, the application vendor can easily distribute updates, upgrades, and easily manage the device and application configuration.

The mobile marketing association report further discussed that Mobile client applications have a variety of advantages and disadvantages for financial applications and services the advantages are Offers organizations more control over the user experience, with a rich user interface capability, ability to work even when there is no connection to the wireless network, secure access can be established with applications, support for access to corporate or custom applications, Most applications also provide the ability to provide remote wipe-out of information when device is lost or stolen, highly secure data encrypted, user friendly and low cost The disadvantages are Thousands of different combinations for devices, operating systems and development environments may prevent support for all devices; differing handset capabilities and performance causes inconsistent

user experience when using or downloading an application; Possible increase in customer service and support issues and need internet.

IV. Mobile Web (XHTML) Channel

According to mobile marketing association report the mobile web uses XHTML, a successor to HTML, developed to address the need to deliver content to devices other than desktop computers. Smart phones are devices that have a large screen and a keyboard and are more suited for accessing the mobile web. In comparison, most smaller mobile phones do not have the resources necessary to support a good mobile web experience or the additional complexity of standard HTML syntax.
Smart phone or tablet computer with an embedded browser, customers can visit the institution's online banking Web site from virtually anywhere. This provides customers with an online banking experience similar to what is available on desktop computers. The mobile web allows users to access web sites from their handset. The mobile web is a channel for delivery of web content, which offers and formats content to users in awareness of the mobile context. The mobile context is characterized by the nature of personal user information needs (e.g. updating a blog, accessing travel information, receiving news update), constraints of mobile phones (i.e. screen size, keypad input) and special capabilities (i.e. location, connection type such as 3G or WLAN). Mobile web sites include the well-known .com domain and .mobi, which was created by a consortium of companies including Google, Microsoft, Nokia, Samsung and Vodafone. The mobile web also includes the Wireless Application Protocol (WAP), which is an open standard to enable access to the internet from a mobile device

The mobile marketing association report further discussed that The mobile web has a variety of advantages and disadvantages for financial applications and services. The advantages are user experience of browsing the internet from a mobile device is familiar and offers a rich UI experience, allows end users to access corporate applications, secure connection can be established on most of the mobile browsers, increase security encrypted data. The disadvantages are many non-standard variables including handsets, browsers and operating systems; inconsistent user experience due to varying connection speeds and handset limitations, user needs to have a data plan, which may be a barrier to adoption among price-sensitive demographics, need internet access and No "off-line" (out of the coverage) capability

2.4.4. Types of Service in Mobile Banking

According to CBE Mobile Banking user guideline and brochures of other local banks regarding mobile banking there are various mobile banking service provided by a banks or other financial institution that allows its customers to conduct financial transactions remotely uses a mobile device such as a smartphone or tablet. These typical mobile banking services may include the following:

Account information services: Being able to access account information from anywhere, at any time, is of great value to customers. Initially offered as a competitive differentiator the information such as checking account balances, real time account balance enquiry, Viewing statements and transaction history, mini-statements and checking of account history and alerts on account activity or passing

Fund Transfer or payment services: Mobile banking is usually available on a 24-hour basis. Some financial institutions have restrictions on which accounts may be accessed through mobile banking, as well as a limit on the amount that can be transacted. Transactions through mobile banking may include own account transfer (transfer balance to other account of the owner), Pay to Favorite pre-defined Beneficiary (transfer an amount to under listed beneficiary account), People to People account transfer (Fund transfer to other customer which have an account with in the same bank) and the last but not the list is LMTS (Local Money Transfer Service)

Managing favorites or beneficiary service: customer can have register and manage favorite/Beneficiary customers who have an account with the same bank, register global beneficiary, delete registered Beneficiary, and List Registered Beneficiaries

Other information service: Customer can access various information from the bank through their mobile banking services information's like foreign exchange rates, loan repayment schedule of their loan account, future dated payment, make standing order of various issues, deposit Interest rate, Stop Payment orders, cheque book request for current account, check the states of cheque book ordered, cheque detail and ATM or branch locator

2.4.5. Ecosystem of Mobile Banking

According to Vanessa (2012) the ecosystem of mobile banking is complex and this leads to some of the challenges when addressing issues of security. There are numerous players involved including: Customers, merchants, banks, debit/credit card networks, clearing/settlement

organizations, application providers, 3rd party payment providers, wireless carriers, and handset/chip manufacturers.

Vanessa (2012) further discussed that In order to understand the complexity, it is useful to walk through the different actors involved in credit card payments. The card holder is the consumer who applies for a credit card through some bank. The bank that issues and extends credit to the card holder is called the Issuer or Issuing Bank. The issuing bank assumes the liability of the card holder purchase. The merchant is the place of business whereby the cardholder uses their card to purchase goods or services offered by the merchant. The merchant must obtain a merchant account prior to being allowed to process credit cards and receives this account through a merchant service provider or merchant bank (acquiring bank). The merchant service provider is responsible for all communications and relationships on behalf of the merchant to other players in the ecosystem. Processors provide a point of connectivity for the merchants to authorize and settle credit card transactions through appropriate payment networks. In some cases the merchant service provider and processor are part of the same company. Card associations are companies such as Visa, MasterCard, American Express and Discover. In the case of American Express and Discover they are the issuing bank, the merchant bank and the card association. The other key complexity of the ecosystem is the mobile handset and wireless carrier component of the landscape. The diversity of handset manufacturers is growing and dynamic with some traditional players such and Nokia and Motorola losing market share and new players such as Samsung and Apple gaining significant market share. In addition to the hardware diversity, the variety of operating systems on these devices continues to grow.

2.5 Information Security and Threats

The definition of information security varies across scholars and/or institutes since it does not reach in its maturity level due to technological evolution. However; a broad and internationally recognized definition of information security is given in ISO/IEC 17799 standard as “The preservation of confidentiality (ensuring that information is accessible only to those authorized to have access), integrity (safeguarding the accuracy and completeness of information and processing methods), and availability (ensuring that authorized users have access to information and associated assets when required) of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved (Anene & Annette, 2007).

A threat is any circumstance or event with the potential to harm an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. Threats generally can be classified as Natural and Deliberate or Accidental. These threats, as stated by Michael (2003), include: Act of Human Error or Failure (accidents, employee mistakes), Compromises to Intellectual Property (piracy, copyright infringement), Deliberate Acts of Information Extortion (blackmail of information disclosure), Deliberate Acts of Sabotage or Vandalism (destruction of systems or information), Deliberate Acts of Theft (illegal confiscation of equipment or information), Deliberate Software Attacks (viruses, worms, macros, denial of service) Forces of Nature (fire, flood, earthquake, lightning), Quality of Service Deviations from Service Providers (power and WAN service issues), Technical Hardware Failures or Errors (equipment failure), Technical Software Failures or Errors (bugs, code problems, unknown loopholes), Technological Obsolescence (antiquated or outdated technologies)

In addition to this, technically specking the following major categories will be the cause of information system threats: Malware, Malicious insiders, Exploited vulnerabilities, Careless employees, Mobile devices, Social networking, Social engineering, Zero-day exploits, Cloud computing security threats, and others.

2.6 Key Security Risks in Mobile Banking

A major challenge for the adoption of mobile banking technology and services is the perception of insecurity. In the survey conducted by the Federal Reserve, 48% of respondents cited their main reason for not using mobile banking was "I'm concerned about the security of mobile banking". In the same study, respondents were asked to rate the security of mobile banking for protecting their personal information and 32% rated it as somewhat unsafe and very unsafe, while 34% were not sure of the security. These statistics represent a significant barrier to the use of mobile banking products and services. (Consumer and Mobile Financial Services, 2012)

According to Mobile marketing association report Users will expect at least the same level of security that's available when banking online via their PC. Both the real problem (e.g., eavesdropping, injection and modification) and the "perception" issue (e.g., how security – or lack thereof – affects the financial institution's brand) must be addressed in order to encourage adoption of mobile banking. Data transmission must be secure in this case, the term "secure" addresses

mainly the concept of confidentiality and therefore requires encryption of the connection between the device and the bank. Mobile marketing association report further discussed the following issues:

Application and data access must be controlled: Before users can receive any sensitive information related to their bank accounts, a certain degree of verification must be completed. Ideally, the combination of several authentication factors and the possibility to challenge the user in case of a (potential) security breach should be part of the procedure.

Data integrity must be provided: Any critical data stored on the mobile device must be protected against unauthorized modification. The issue of possible corruption and deletion error of sensitive information should also be addressed.

Loss of device must have limited impact: The mobile banking service should be designed so that there's limited impact when customers lose their handsets. For example, the service could support a remote-locking feature embedded in the software client that prevents a lost phone from accessing the customer's account. Such features also provide the peace of mind that helps encourage customers to try mobile banking.

According to Vanessa (2012) the security risks associated with mobile devices are very similar to any other computing device with a few key exceptions:

- Mobile devices have a smaller form factor and therefore are more susceptible to loss or theft
- Mobile devices are more personal and there will be a tendency for users to use devices in a more personal and confidential way
- Security controls and tools available have not matured to accommodate the constraints of limited processing power and limited battery life

Vanessa (2012) further discussed that the key risks to the mobile device include: Malware, Malicious applications, Privacy violations relative to application collection and distribution of data, Wireless carrier infrastructure, Payments infrastructure/ecosystem, SMS vulnerabilities, Hardware and Operating System vulnerabilities, Complex supply chain and new entrants into the mobile ecosystem and Lack of maturity of Fraud tools and controls.

According to Mobile marketing association report financial institutions should be aware of the types of potential threats that can affect their mobile banking services. These include:

Cloning – Copying the identity of one mobile phone to another, thereby allowing the perpetrator to masquerade as the victim, normally with the intent to have calls and other services billed to the

victim's cellular account. In the case of mobile banking, cloning could give the hacker access to the victim's financial accounts.

Hijacking – The attacker takes control of a communication between two entities, masquerading as one of them. As with cloning, hijacking could give the hacker access to the victim's financial accounts.

Malicious Code – Software in the form of a virus, worm or other "malware" is loaded onto the handset, the SMS gateway or the bank's server to perform an unauthorized process that will have adverse impact on the confidentiality, integrity or availability of financial information and transactions.

Malware – A contraction for "malicious software" that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity or availability of the victim's data, applications or operating system, or otherwise annoying or disrupting the victim.

Man-in-the-Middle Attack – An attack on the authentication protocol exchange in which the attacker positions himself between the claimant and verifier with the intent to intercept and alter data traveling between them.

Redirecting – Intercepting a communication by substituting a fraudulent address or identity, potentially by using a Man-in-the-Middle attack.

SMiShing – A contraction of "SMS phishing," this attack uses SMS to facilitate bogus requests for personal information.

Spoofing – Sending a network packet that appears to come from a legitimate source, rather than its actual source.

Vishing – A contraction of "voice and phishing", in which victims are tricked into disclosing sensitive personal information through a phone call.

Phishing – Tricking a victim into disclosing sensitive personal information or downloading malware through an email.

2.7 Security Challenge of E-Banking

According to Wondwossen & Tsegai (2005) one of the biggest challenges of e-payment is to ensure its security. Securing the payment process involves authenticating both the customer and the merchant and protecting the information to be transmitted from interception. In addition a means must be provided that prevent repudiation both by the merchant and customer once the payment process has taken place. E-payment systems have to take into account the need of multilateral

security i.e. security needs of all participating parties in the e-payment system must be given due attention. An e-payment system that is not secured may not get trust from its users. Trust is one of the crucial factors for the acceptance of e-payment system. The next section discusses major security challenges of e-payment system as per Wondwossen & Tsegai (2005)

Disclosure of private information: -In e-payment there are many ways in which private information may be accessed by attackers.

Counterfeiting: -Counterfeiting is the creation of new data or duplication of existing data, which are technically valid but not legally admissible

Illegal alteration of payment data: -Illegal modification of payment information may result in loss money. This may again results in the loss of customer confidence.

Infrastructure: -The other challenge for e-payment is proper infrastructure. For the effective deployment of e-payment, it is necessary to have a reliable and cost effective infrastructure that can be accessible to the majority of the population.

Wondwossen & Tsegai (2005) further discussed that In Ethiopia the major challenges of E-payment are: Poor telecommunication infrastructure, frequent power disruption, People are resistant to new payment mechanisms, lack of skilled manpower, unavailability of payment laws and regulations particularly for e-payment

2.8 Best Practice for Mobile Banking Security

According to Wu He, Xin Tian & Jiancheng Shen (2015) Some security experts and vendors propose new ways to mediate security risks associated with mobile banking service. Below are some emerging trends that found from the blog mining results.

- Integrating biometrics into mobile banking apps to enhance user authentication. Biometric authentication such as fingerprint scanning and voice recognition offers a promising way for identity and access management (Fatima, 2011). As personal biometric also has vulnerability, it is better to combine personal biometric with other authentication such as one-time password (OTP) and Site Key for stronger personal identification and verification.
- Integrating intelligent behavioral monitoring and analysis technology with mobile banking apps. Webroot (2014) recently developed mobile security SDK which is designed to embed security within a mobile banking app, run in the background and deliver real-time threat intelligence to the bank for further data analysis and action. By employing a behavioral monitoring and analysis approach, banks can detect abnormal behavior more accurately and

early. Specifically, behavior analysis can detect the behavior of the person who is using the mobile app and compare it with previous behavior or usage patterns. If abnormal behavior is identified, alert messages will be sent out.

- Deployment of advanced big data analytics technology for fraud detection and behavioral analysis. Accurate and efficient behavioral analysis requires banks to de-ploy advanced big data analytics to mine enormous volumes of security data to better identify trends of malicious behavior or abnormal behaviors indicative of an attack at the outset (Khosla, 2015).

2.9 Empirical Evidences

Over the past decade, researchers have focused on internet or online banking, whereas research focusing on mobile banking is relatively insufficient and receives little attention (Puschel et al. 2010; Suoranta and Mattila, 2004). M. Hassan, A. Rahman, S. Afrin, & M. Gulam Rabbany (2014) investigated factors influencing the adoption of mobile banking services in Bangladesh and concluded that five factors affects user adoption. These are: perceived usefulness, subjective norm, perceived ease of use, perceived credibility, consumer awareness about mobile banking and perceived risks associated with mobile banking.

Laforet and Li (2005) investigated the barriers to Chinese consumer adoption of online banking. They indicated that security was the most important factor that motivates adoption. Also, they indicated perception of risks, computer and technological skills, lack of awareness and understanding of the benefits, and Chinese traditional cash-carry banking culture as the main barriers to adoption.

Some related studies are conducted by different researchers in different parts of the world. However, there are limited numbers of studies conducted in Ethiopia on the adoption of technological innovation. Specifically, Gardachew (2010) conducted research on the opportunities and challenges of E-banking in Ethiopia. The aim of his study was focused on analyzing the status of electronic banking in Ethiopia and investigates the main challenges and opportunities of implementing E-banking system. The author conducted a survey on the existing operating style of banks and identifies some challenges of using E-banking system, such as, lack of suitable legal and regulatory frame works for E-commerce and E- payments, political instability in neighboring countries, high rates of illiteracy and absence of financial networks that links different banks.

Wondwossen and Tsegai (2005) also studied on the challenges and opportunities of E-payments in Ethiopia; their objective was studying of E-payment practices in developing countries, Africa and Ethiopia. The authors employs interview and on site observation to investigate challenges to E-payment in Ethiopia and found that, the main obstacles to the development of E-payments are, lack of customers trust in the initiatives, Unavailability of payment laws and regulations particularly for E-payment, Lack of skilled manpower and Frequent power disruption. According to Wondwossen and Tsegai (2005), an adequate legal structure and security framework could foster the use of E-payments, which is contradicting with the finding of the previous study.

Among various banking services, mobile banking is one of the most risky fields, which is prone to customer resistance (Laukkanen & Kiviniemi, 2010; Prabhu & Vijaya, 2014). There are also a number of challenges and risks involved with new technology and it takes time for users to become comfortable and embrace the change (Al-Akhras et al., 2011; Amin et al., 2012).

There are many risks in mobile banking as personal and commercial data is transmitted wirelessly and can be seen in some circumstances by third party intermediaries or unauthorized individuals (Chin et al., 2012; Kang & Kim, 2012; Laukkanen & Kiviniemi, 2010). Legal aspects also have a role to play, as the relationship between the bank and its customers appears vague in mobile banking (Darballey & Weber, 2010). The security of financial transactions on mobile banking devices is a prime concern for customers of this service (Darballey & Weber, 2010; Sheng et al., 2011). The risk taking nature of entrepreneurship is also related to the relatively high risk of something going wrong with security in mobile banking systems (Abadi et al., 2013; Agwu & Adele-Louise, 2014). Many financial institutions recommend people take caution with mobile banking due to the security risks and regularly check their banking statements (Boateng & Duncombe, 2013; Dass & Muttukrishan, 2011).

Electronic payments are not currently covered in Ethiopian legal system. Lack of such legal framework may thus hinder the introduction of cost effective modern electronic payment instrument such as ATMs, credit and debit cards, mobile/telephone/internet banking. Similarly the study of Gardachew (2010) revealed that lack of legal frame work is one of the challenges for E-banking system in Ethiopia. In contrary the study of Wondwossen and Tsegai (2005) revealed that an adequate legal structure and security framework could encourage the use of E-payments in Ethiopia. However, the result of survey presented in table 5.3 about legal frame work on implementation of E-banking system revealed that lack of legal frame works and cross country

legal and regulatory difference is considered as barriers faced by banking industries for the adoption of E-banking system in Ethiopia.

Electronic payments are not currently covered in Ethiopian legal system. Lack of such legal framework may thus hinder the introduction of cost effective modern electronic payment instrument such as ATMs, credit and debit cards, mobile/telephone/internet banking. Similarly the study of Gardachew (2010) revealed that lack of legal frame work is one of the challenges for E-banking system in Ethiopia. In contrary the study of Wondwossen and Tsegai (2005) revealed that an adequate legal structure and security framework could encourage the use of E-payments in Ethiopia. However, the result of survey study presented by Ayana (2014) about legal frame work on implementation of E-banking system revealed that lack of legal frame works and cross country legal and regulatory difference is considered as barriers faced by banking industries for the adoption of E-banking system in Ethiopia.

2.10 Identification of Knowledge Gaps

In line with the above empirical studies and theoretical literatures in mobile banking, banks usually provide different mobile banking channel for different devices. Mobile banking makes financial services easily accessible for customers through a handheld device. Mobile banking applications also helped financial institutions cut down the cost of providing banking services to customers. However, security is a major concern for many mobile banking customers. Security on mobile banking is complicated because of the variety of mobile devices and platforms. Mobile devices have a smaller form factor and it has more susceptible to loss or theft. Mobile devices are more personal and there will be a tendency for users to use devices in a more personal and confidential way. Security controls and tools available have not matured to accommodate the constraints of limited processing power and limited battery life. Absence of integrating biometrics into mobile banking service to enhance user authentication. Failure to integrating intelligent behavioral monitoring and analysis technology with mobile banking service and fail to exploitation of advanced technology for fraud detection and behavioral analysis.

3. RESEARCH METHODOLOGY

3.1 Research Design

The research design reflects the purpose of the inquiry and it is needed because it facilitates the smooth sailing of the various research operations, thereby making research as efficient as possible yielding maximal information with minimal expenditure of effort, time and money. Research design stands for advance planning of the methods to be adopted for collecting the relevant data and the techniques to be used in the analysis and keeping in view the objective of the research.

Exploratory research is conducted when there are few or no earlier studies to which references can be made for information and it is most useful to addressing a subject about high level of uncertainty and ignorance about the subject. The aim is to look for patterns, ideas or hypotheses rather than testing or confirming a hypothesis. In exploratory research the focus is on gaining insights and familiarity with the subject area for more rigorous investigation later. The main goal of exploratory research is to identify the boundaries of the environment in which the problem, opportunities or situations of interest are likely to reside and to identify the salient factors or variables that might be found there and be of relevant to the research.

Exploratory study is usually characterized by a high degree of flexibility and lacks a formal structure. Exploratory research is effective in laying the groundwork that will lead to future studies. Exploratory studies can potentially save time and other resources by determining at the earlier stages the types of research that are worth pursuing.

This research would be conducted by using exploratory research design. It uses to obtain information concerning the current status of the security in mobile banking service to describe "what exist" with respect to variables have be identified by the study or conditions in a situation. The research will focus on instrument development as well as empirically investigates the statuses of security in mobile banking service in Ethiopian banks. Therefore, it is a combination of both exploratory and empirical types.

Empirical research relies on experience or observation alone, often without due regard for system and theory, It is data bases research coming up with conclusions which are capable of being verified by observation or experiment.

3.2 Research Approaches

The qualitative method is beneficial because a specific event is described (Marshall & Rossman, 2011). According to Yin (2011), there are five features of qualitative research to gain knowledge from the experiences of others: (a) studying the lives of people under real-world conditions and providing meaning from the information collected, (b) representing the views and perspectives of participants in the study, (c) covering the contextual conditions of the participants' lives, (d) contributing insights into existing or newly emerging concepts by adding insight to the social behavior of humans, and (e) striving to use multiple sources of data and not on a single source alone. Hence, the qualitative method was the most appropriate for this study.

Qualitative – concerned with a quality of information, qualitative methods attempt to gain an understanding of the underlying reasons and motivations for actions and establish how people interpret their experiences and the world around them. Qualitative methods provide insights into the setting of a problem, generating ideas and/or hypotheses. Qualitative research is used to look into phenomena involving qualitative data which could be human experience or belief related to a research topic.

The research used qualitative approaches to assess states of security on mobile banking service delivery. To develop the instrument and related activities the researcher tries to focus on qualitative methods like focus group discussion with group of branch managers and Customer service mangers of selected banks, unstructured interview with the E-payment service mangers of selected banks and analysis of document found in selected banks a document related to Mobile Banking service.

3.3 Sampling Design

Sampling, as it relates to research, refers to the selection of individuals, units, and/or settings to be studied. Whereas quantitative studies strive for random sampling, qualitative studies often use purposeful or criterion-based sampling, that is, a sample that has the characteristics relevant to the research question(s). This strategy adds credibility to a sample when the potential purposeful sample is larger than one can handle.

For this study the sampling design used is purposive sampling. A purposive sample is a nonprobability sample that is selected based on characteristics of a population and the objective of the study. Purposive sampling is also known as judgmental, selective, or subjective sampling. The eligibility criteria for the focus group discussion of the study were: working for the bank within the

last 5 years; exposure to Mobile banking service; and knowledge of the security issues mobile banking system. The sample sizes of focus group discussion were 7 Branch Manager and 5 customer service manager total of 12. In addition to that 5 banks mobile banking service concerned managers (Head of the department) were interviewed. The sample size was sufficient for gaining comprehensive knowledge regarding security issues and customer protection on the mobile banking service.

3.4 Sources of Data and Data collection Methods

The most common methods of collecting qualitative data include observation, interview and focus groups. To collect valid and reliable data for this research, the study use the following research instruments. These are;

Unstructured interview –the researcher conducted unstructured interview with E- Payment service managers' of five banks which are Commercial Bank of Ethiopia, Dashen Bank, Awash Bank, Bank of Abyssinia and Lion International Bank. The objective of the interview is to identify facts that could be exposed to find related information mobile banking security and customer protection.

Two focus group discussions were conducted. The first group discussion is made with seven branch managers of three banks three of them from CBE Two of them from Buna international bank and two of them from Addis international Bank. The second group discussion was set with five Customer service managers of CBE whose have a lot of experience in customer service operation. The major objectives of these group discussions is to gather real case happened in the mobile banking service delivery related to security and customer protection.

Secondary sources: the researcher tries to use different kinds of secondary resources for the research as input such as banks security policy procedures and guidelines, various Mobile banking documents prepared by banks their own, mobile banking service related reports and other source documents like different web sites, journals, and articles.

Data collection process pertaining to the research question resulted from face to face semi structured interviews, handwritten interview notes, and any copies of archival materials, and review statements. The researcher will try a lot to find current and much related secondary information to use them as a stepping board for the research.

3.5 Data Analysis

Analyzing the data contributed to examining the relationships and meaning of the data as well as revealing properties, repeated patterns and expressions. The study use interviewing, observation, document analysis, and other feasible method to assess the issues of security in mobile banking service provide by Ethiopian banks

Qualitative analysis is the analysis of qualitative data such as text data from interview transcripts. Unlike quantitative analysis, which is statistics driven and largely independent of the researcher, qualitative analysis is heavily dependent on the researcher's analytic and integrative skills and personal knowledge of the social context where the data is collected. Qualitative analysis is organized around concepts or key ideas. The size of text units may vary with the type of concept. Hence, coding units does not have to be standardized (to say, a certain length like a paragraph) in qualitative analysis (Bhattacherjee, 2012).

Open coding is a process aimed at identifying, uncovering, and naming concepts that are hidden within textual data, which can later be used to explain a social phenomenon. The researcher examines the textual data line by line to identify discrete events, incidents, ideas, actions, perceptions, and interactions of relevance that are coded as concepts. Each concept is linked to specific portions of the text (coding unit) for later validation. While coding, it is important to identify the recognizable characteristics of each concept, or level, so that similar concepts can be later grouped into broad categories. This coding technique is called "open" because the researcher is open to and actively seeking new concepts relevant to the phenomenon of interest (Bhattacherjee, 2012).

The semi structured interviews and other secondary source of documents formed a foundation for the study and data analysis (Yin, 2014). The researcher analyzed the interview transcripts. The responses of this interview addressed the central research question. The first step is evaluating the collected data, the next step required the organization of the data gathered from the interviews and other resource the final step involved the preparation and development of interpreting the data.

4. FINDINGS INTERPRETATION AND IMPLICATION

According to the Federal Reserve a major challenge for the adoption of mobile banking technology and services is the perception of insecurity. In the survey conducted by the Federal Reserve, 48% of respondents cited their main reason for not using mobile banking was "I'm concerned about the security of mobile banking". In the same study, respondents were asked to rate the security of mobile banking for protecting their personal information and 32% rated it as somewhat unsafe and very unsafe, while 34% were not sure of the security. These statistics represent a significant barrier to the use of mobile banking products and services (Consumer and Mobile Financial Services, 2012).

The main purpose of this study is to assess current security practices of mobile banking service and customer protection in Ethiopian banks. To address this issue of security the study first tries to gather information about the mobile banking operation and its security challenge to get this information focus group discussion held with various banks branch managers and customer service mangers and during our discussion the following cases are raised.

4.1 Bio Data of the Respondents

For the focus group discussion two groups were prepared the first group was the combination of seven branch managers from three banks and they have been working experience of above 10 years and for last 5 years worked as a branch manager and they have Degree and above educational qualification. They have an exposure to electronic banking products, and they have a knowledge of the service nature of the mobile banking system. The second group was arranged with five customer service managers of various branches of commercial bank of Ethiopia and they have above Eight years' work experience in the banking sectors and they have Degree and above educational qualification and they have an exposure to led all branch customer service operation and also have an opportunity to face all customer contact related to mobile banking and other service in addition to this they have also engaged in various challenging cases and experience related to the service

These two groups were sufficient for gaining comprehensive knowledge about the nature of mobile banking service and its security challenge.

The study conducted by making unstructured interview with E- Payment service managers' of five banks which are The Manager-Mobile and Internet Banking Team of Commercial Bank of

Ethiopia, Director of E-Payment of Dashen Bank, E-Banking Manager of Awash Bank, E-Payment manager of Bank of Abyssinia and E-Payment division head of Lion International Bank. All of the managers have an experience of above ten years in banking sector and they have a degree Masters educational qualification. For the interview they spent above an hours with me for discussion and shared their experience and challenges they face in related to mobile banking.

4.2 Observed cases and security issues

During the Focus group discussion with both groups a lot of issues were raised about mobile banking specifically and E-banking in general. From various service issues of mobile banking raised the following are the major issues related to security and customer protection.

1. Double entry of transaction due to system problem

When the user of mobile banking who use mobile banking for transferring money to different customer of his. One day as usual when sending Br 5,000 to his customer and he process all the steps and at the end he presses the ok button the system automatically deposits to the receiver twice in the account by deducting the amount from him. Finally he know that the deposit to the customer twice and go to the bank and ask them to reverse one of the transaction but the bank say that they did not because they are not do anything without the order of the beneficiary account holder

The problem of doubling the transaction entry when making fund transfer in mobile banking happen frequently when there is a problem of network or a problem system failure. This problem happens in most banks and has high frequency. In this case banks did not have any strong legal /security/ background to refund wrong posting made by Mobile banking users due to system or network failure.

To resolve the problem some positive branch managers try to contact the beneficiary and explaining the problem to reverse one of the transactions to make an adjustment the bank need a source document of an order to adjust by the beneficiary account holder by paper.

This problem is comment to all banks and all the participant of the discussion agreed that the issue has increase the tendency of losing the confidence of using mobile banking service

2. **Absence of any source document for the transaction made by mobile banking for reference**

In the traditional banking service all transactions are its own source document for cash deposit the customer get an advice slip from the bank. customer use banking transaction for various purpose for example customer make deposit to other person account to settle their credit to pay monthly house rent to pay tuition fee to the school, to buy various kinds of property of service, to buy shares of the companies, etc for all these activities the customer want an advice from the bank as a source document and reference these all activities can done by mobile banking service however from the mobile banking service the customer does not get any printed source document therefore it is difficult to confirm the transaction is made.

To view this issue the participant of the group discussions raises case happen at merkato which is one of the biggest market in the country that found so many wholesalers and retailers the wholesalers distribute the merchandise item to the retailer in bulk and the retailers sell the merchandise item to the consumer. Most of the time the wholesaler distribute the goods to the retailer after receiving the money through their bank account. Most retailers are deposited to wholesalers account mostly by cash but one of retailer customer of the bank credit to wholesaler account by using mobile banking fund transfer and go to the wholesaler to collect the merchandise goods the wholesaler refuse to give the goods to the buyer because wholesaler want an advice to confirm the transfer by bank even if the wholesaler receive the alert massage through his mobile because the wholesaler have so many retailers deposit the same amount so he need to see the receipt to differentiate and identify who deposit the money.

SMS alert is the SMS massage sent by the bank to its customer mobile when the customer account has any credit or debit transaction which means any kind of deposit or withdrawals activity made in the account this massage is send to any customer who have an account of any kind and have register their mobile number in the customer address data. See the picture below typical massage sample sent by banks to the customer the massage inform the customer about the debit or credit of a specific amount to the account but it does not mention who make the transaction and for what reason the transaction was made.

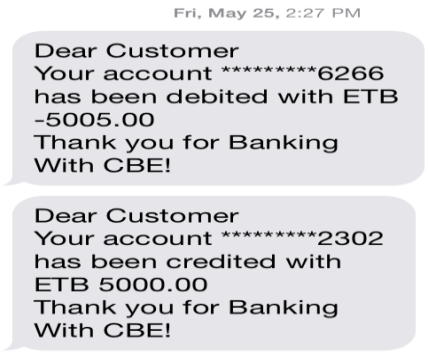

Fig. 1 Type of The SMS alert massage sent by banks

The mobile banking user encounters such kind of issue and come to the bank and asks the bank to give a receipt so in mobile banking transfer the bank did not issue such kind of advice or receipt so the customer encounter such difficulty for period of time until the wholesaler check his account by the bank statement. Therefore the customers refuse to use mobile banking to make such kind of fund transfer. The banks do not have any accepted legal reference document for mobile banking transaction made by customer

3. Difficult to adjust transaction entry made erroneously

In traditional banking when customer want to make a transaction they need to fill the deposit or withdrawal form of the bank and the banks customer service officer post the transaction requested by the customer to the system and process the deposit or withdrawal of money in this process there is a tendency to make an error by both parties the customers or the banks officer due to that all traditional banking transactions are processed though makers checkers and audit arrangement if the incident of error happen and found an adjustment takes by the bank any time but there is no such kind of treatment in the mobile banking service for errors made by the customer.

When a customer try to transfer money to others various errors may happen such as it may try to transfer to wrong account number or it may try to transfer wrong amount money but when he/she comes to the banks to make an adjustment of that transaction the banks has not try to adjust such kind of error without the order of the beneficiary account owner of that the amount is wrongly enter just like the firs issue raised above. In this case bank did not have any strong legal /security/background to refund wrong posting made by customer erroneously and also the customer doesn't have a right to amend such kind of error

4. Time of customer lost his mobile phone

If a customer lost or stolen his/her mobile devices and that device has not locked by pin code or pattern and have mobile banking details saved in a text file, or set to be never forgotten by the

mobile banking app itself or unauthorized third parties gaining access to online bank accounts using login details that have been stolen directly there is a tendency clean out the bank account of the customer in a short period of time without any effect of place and time

If the customer lost their mobile there is a tendency to transfer of money by the person who found the phone if pin is set in the app as unforgotten mode or if the pin saved in text at reminder or note apps. In addition these cases happen at the time of activation the bank performer send the pin and activation code to the customer phone in order to activate. So the customer did not delete their pin from the mobile and found by other person he/she can transfer the money. on the other hand even if when keeping the mobile at workplace or other which is untrusted place and the mobile banking details saved in a text file, or it set as to be never forgotten by the mobile banking app itself or auto saving of mobile banking passwords gives anyone with physical access to the mobile device has an access to the mobile banking service of the customer.

However the participant of the discussions cannot face such kind of case in their work experience and it is rare of a tendency of such kind of issue.

5. There is no way to protect customer that transfer money by force

During the dissociation with the groups I raised the issue of transferring money by force or by hijack the customer. But no one hired such kind of issues in their bank domain but all of them agreed that it was possible to happen.

If a someone force a customer of a bank who use mobile banking service to makes fund transfer some amount of money to other person through mobile banking the bank have no ways to protect such kind of problem because it’s difficult to identify the situation by the bank the only thing that protect the customer is his pin code of mobile banking. Therefore the banks do not give any protection mechanism for safeguarding the customer but until now I cannot found abd hired such kind of cases reported.

6. Weak password or pin protecting strengthens and ease of accessing by others

Mobile banking Uses 4 digit numerical pin code to enter in to mobile banking menu and this password given to customer during activation the bank send to user by SMS and most customers does not delete the SMS after they memorize and save in mind therefor it is a high tendency to view this pin code by others who access the pone. In addition to this the pin code is not case sensitive and week strength.

During the group discussion one of CBE customer service manager share a case happen on the on customer of CBE Gurdshola branch a women who have an account and use the bank's ATM service one day she want to withdraw money from the ATM machine and go to the nearest ATM machine with her son and she insert the card and when the machine request the pin she try to insert the pin code but when she insert the code she also sound the code number at this time the son hired the code and memorize he withdraw money from the ATM Machine so many time without his mother know after so many time she come to the bank to withdraw some money but at that time its insufficient amount when officer tell her it is insufficient she fill that the bank stolen her money but after so money discussion after cooling her when viewing the transaction enquiry it is withdraw by ATM machine and she know it that it is her son fault.

Even if this case is an ATM service case it is related to mobile banking because the mobile banking pin code also 4 digit numeric password which is very week and not case sensitive password now nowadays all smart phones have an alpha numeric keyboards

Possible issues collected from various literatures which is not raised during the group discussions

1. Inadequate disclosure of information to customers

The information disclose through mobile banking service and other electronic midia has a tendency to view by other third party without the knowledge of the customer this creates losing of confidence of their account secrecy. Customers may not fully understand what their right is and obligations are, including for example, any dispute resolution procedure. They may therefore take inadequate precautions in using the product or service. In the developed world Customer may bring legal suit against the bank as a result of losses or disputed regarding information disclosure. A bank may be subject to regulatory or legal sanctions and most of the time customers do not have any ground to get back their losses because there is no clear low of mobile banking that govern and bind Ethiopian banks

2. Difficult to identify suspicious transaction and Money laundering

The transfer of money by mobile banking is now possible. Therefore mobile banking is misused by customers who seek to engage in criminal activity, including money laundering. It affects the banks Legal sanctions for noncompliance with "know your customer" laws this Increase the risk of money laundering and difficult to identify AML and CTF suspected transaction though mobile banking

service due to bulky of transaction which are less in amount but large number of transaction in a day within the banks customers

3. Using Mobile banking by unsecured wireless network

Some customer of banks can use the wireless networks which are hacker-friendly Unlike websites, mobile apps don't properly encrypt information, which means it is not a good idea to access your bank account Via, application base mobile banking when you are on a public or otherwise unsecured Wi-Fi network because wireless network drain out their messages in to the open air how to handle such kind of security issues by banks. Mobile banking apps are connected to wireless networks which are inherently insecure as they broadcast their messages into the open air.

4.3 Summary of Interviews response and banks source document

Key participants in this in-depth interview were the E-payment Managers of 5 commercial bank. The interview questions were tailored to gain the management perspective of the issue of security on mobile banking service in the banks. The main themes that emerged under each interview points are grouped together and the result is presented in summary as follows:

All banks implements different security layer in order to safeguard customers data. Such as the intranet firewall, server side (Arc Mobile) by Page Certificate Authentication (https), on customer side Client Tier User name and password, PIN (4 digit number), One Time Password – expire after a few second during activation of mobile banking service and Session time out.

Regarding the customer protection all interviewed managers respond that there is no any additional protraction mechanism the only customer security has the pin code and it is the responsibility of the customer that keep the pin code in secret way.

In relation to the problem and challenges that hinder the service most bank raise the problem of network and infrastructures and it is also beyond their roll it is the issue of the network provider the Ethio telecom but regarding the customer problem all customer has contact their branch and they treat in their branch according to their case.

Using of technology and innovative financial service delivery channels such as mobile devices have significant contribution in deepening financial service accessibility to the wider section of the population. There is a need to set the minimum standards for risk management and customer protection on the delivery of mobile banking services in doing so the national bank of Ethiopia has issues one directive related to regulation of mobile and agent banking services directives No.

FIS/01/2012 however this directive focuses on agent banking customer protection it lacks detail definition and requirement of banks about mobile banking customer protection and it is the only directive to regulate banks in relation to Mobile Banking service.

On the bank side all banks has their own IT security policy but these security policies focuses on computer password security issues, companies email security, backup security, disaster recovery, database administration and other internal bank system security issues and the systems usage security. However the policy and procedure were not include the issue of mobile banking security and customer protection therefore all banks does not properly address the issue of mobile banking security in their security policy.

When customer apply for the mobile banking service the customer has required to sign the banks prepared term and conditions made for the mobile banking this term and conditions forward the issue of protection of customer in mobile banking service leaved to the customers

According to the term and conditions made by CBE for Mobile banking the following pointes are bind the customer up on mobile banking service delivery:

The customer acknowledges that the mobile banking service is dependent on the infrastructure, connectivity and services provided by the Telecom Service provider.

The customer accepts that timeliness, accuracy and readability of SMS/Bank's Alerts/instructions /Information shall depend on factors affecting the telecom services provider.
The Customer hereby irrevocably agrees, to indemnify and keep the bank indemnified at all times hereafter, from all losses, damages, costs, legal fees, charges and expenses and consequences whatsoever, incurred by the bank on account of any claims, actions, suits or otherwise instituted by the Customer, or any third party whatsoever, in connection with the use of the mobile Banking
The bank makes no express or implied warranty with respect to the Mobile Banking service provided hereunder including, without limitation, any warranties of non-infringement of third party rights, satisfactory quality and fitness for a particular purpose.

The bank shall not be liable to the Customer for any loss or damage whatsoever or howsoever caused arising directly or indirectly in connection with Mobile Banking service.

In case the Customer considers that there has been an error or irregularity in the recording system of the Bank, he/she will be allowed to prove it.

The customer shall be bound by the term and conditions of the contract up on subscribing the mobile banking service.

This shows that all customer protection and security handle by the customer. During the observation this term and conditions does not give to customer it keep at the bank's branch after singing of the customer. In addition it is difficult to know how many of the customers understand this term and conditions. Because there is no way of creating awareness and education to the customer except the media advertisement and customer service officer explanation at the counter it is not well prepared awareness creation and education mechanism for customers that is why the above mentioned cases happened

When customers make any transaction by Mobile Banking they must be confident that it will be processed correctly. In the unlikely event that banks fail to process customers' transaction in accordance to the beneficiary, amount and date specified, Bank must try to reimburse the customer for any late-payment-related charges incurred.

All possible risk of mobile banking service related to the banks side are recorded at the bank and monitor them in the Risk and compliance management process of the Banks. They used various security and management mechanisms to manage the risk emanated from the service to banks own .

4.4 Why Mobile Banking Security is Essential

Banks must have worked hard to deploy effective security frameworks for traditional online banking. However, mobile banking presents its own unique challenges, including growing malware threats that specifically target the mobile channel. As a result, any attempt to leverage existing online banking infrastructure and tools will result in a much higher risk profile, unless steps are taken to adopt mobile-centric security. There are several ways in which mobile banking presents its own unique challenges:

In a relatively short space of time, mobile devices along with house keys and the wallet are the three must-have items when leaving the home. With the use of mobile payments and mobile keys, there is a very real possibility that mobile devices could one day replace physical keys and wallets altogether. This means that mobile security becomes even more important in the event of device loss or theft, but also enables banks to make mobiles a core part of a user authentication strategy, due to the various features they contain. These include GPS, pressure sensors and biometrics.

Mobile usage is all about providing a positive user experience. As such, users expect access to apps, services and content to be seamless with strong security operating in the background as standard. This makes striking the balance between security and user experience more important than ever before.

As a rule of thumb, mobile devices support always-on email, SMS, browsing and a gesture-based approach to using mobile apps. This encourages users to open unsolicited emails and attachments, visit untrusted websites, download third-party apps and reuse the same login credentials across multiple sites. This makes mobile devices vulnerable to a growing array of security threats, including phishing, malware and social engineering.

Increasing use of unsecured Wi-Fi connections, as opposed to traditional wired networks means users are more likely to inadvertently compromise their device's security.

The mobile threat landscape is evolving rapidly, with cybercriminals becoming increasingly insight in their methods. Symantec's 2016 Internet Security Threat Report revealed a 77% increase in the number of new Android mobile malware variants between 2014 and 2015; with malware such as X code Ghost also enabling hackers to target Apple's operating system.

5. CONCLUSION AND RECOMMENDATION

5.1 Conclusions

In today's technological and social environment, security is a very important part of a banking system. Mobile banking is becoming one of the fastest growing segments in banking. A majority of the banks in Ethiopia offer mobile banking services. Using Mobile Banking to access banks and their financial systems made customers do their banking jobs independent of time and location. In addition, it allows customers to take full advantage of the latest technology.

From the bank's point of view, mobile banking reduces the cost of handling transactions by reducing the need for customers to visit a bank branch for non-cash withdrawal and deposit transactions. Mobile banking does not handle transactions involving cash, and a customer needs to visit an ATM or bank branch for cash withdrawals or deposits.

This study was undertaken to identify and create a better understanding about the security issues and customer protection in mobile banking service in Ethiopia. A major challenge for mobile banking technology and services is the perception of insecurity. So banks and customer (mobile banking users) must be concern about the security and protection level of the service. In this paper the study tries to explore and identify major potential security issues and protection challenges.

In order to securely deliver mobile banking services, and to increase user confidence in the safety of banking on their mobile devices, banks must provide multi-layered security. Their solutions must address the potential challenges that can occur throughout the transaction.

This includes challenges at both the front end (consumer devices), the back end (banking systems that recognize and facilitate legitimate user requests through mobile devices), as well as the channel connecting the front and back ends. Bringing this peace of mind to users helps to drive further adoption of mobile banking, thereby bringing added revenue and profits while improving the user experience. At the same time, banks can safeguard themselves from the severe reputational impact that a data breach can have.

5.2 Recommendation

In order to manage the issue of mobile banking security and enhancing customer protection, the banks should implement strong security for prevention and detection mobile banking services. This should include customer education and awareness, strong authentication; secure mobile applications, strict account set up and management processes, real time detective services, and 24x7 customer supports.

1. Customer Education and Awareness

One of the less technical areas of risk mitigation includes an effort around strong customer education and awareness. There should be an established and well understood method of communication with customers. Customers should understand that any deviations from this established communication channel cannot be trusted. This will reduce the risks of customers falling victim to attacks. Customers should also have an established way to communicate relative to suspected fraud and understand how their bank will communicate to them. Customers should be educated on the importance of downloading from reputable sites as well as understanding the behavior of the application in terms of what data is gathered and shared with potentially other services or applications.

Customers should be educated and aware on their options to prevent fraud and what to do if they suspect fraud. Customers should be able to select into strict process rules include limiting transaction value, requiring dual approvers on high risk transactions, and not allowing changes to customer sensitive data such as address or authorized transfer to individuals without strong restrictions. Dual approver is a process that requires one person to initiate the transaction and a second approver on a different device to authorize the transaction. Customers should be encouraged to enroll in predefined alerts that will help in the area of fraud prevention. Other key data points used in fraud prevention include IP reputation, endpoint identity, geo-location, user history and behavior. Additionally, the service should provide controls based on the transactional risk score such as step up authentication where the customer is prompted for additional information as the transaction initiated is more risky.

Education and awareness building collaterals can be created in the form of: leaflets and brochures; Short Messaging Service (SMS) texts; safety tips in account statements and envelopes; educational material in account opening kits; electronic newsletters, DVDs with animated case studies and videos, recorded messages played during waiting period of phone banking halls; preparing talk

shows on television/radio; advertising campaigns though print and TV media; developing common website etc…

2. Authentication

Strong authentication is critical in the mobile space since devices are easily lost and stolen. The most mature and widely deployed method is knowledge based authentication which includes passwords, question and answer (Q&A), and image recognition. Another form of authentication can come from establishing a device identity. There are many methods by which this can be accomplished but the essential element is to authenticate to an ID from that specific device that is derived from attributes (HW and SW) of that device. While authentication through biometrics is not new, it is still challenged with issues related to false positives. With advanced mobile device hardware such as cameras and voice recognition, there will be increased use of biometric authentication in the use of mobile banking.

3. Mobile banking application security

With a marked increase in malware targeting mobile apps, the best security solution should address these safety concerns. Solutions should include debugger detection, emulator detection, tamper detection and code obfuscation detection amidst other mobile application protection methods.

4. Protection is a Shared Responsibility

Protection is a shared responsibility so customer must be sure to understand their role they do play a significant role in keeping their financial information safe. These responsibilities are important to follow and help customers safely access their account and quickly report fraudulent transactions. Customers have different rights and responsibilities For instance it's better to Know and understand about the following issues:

Locking down your mobile device with a PIN code (an okay level of security) or lengthier password (more secure, if you use a combination of letters, numbers, symbols and avoid using common words); Do not share your mobile banking ID and Passcode; Sign off before leaving; Routinely Review your Account Transactions; being aware of your surroundings and who may be watching you either directly or via any cameras in the locale, never allowing any website or app to remember your login details – such convenience could ultimately prove to be very costly, keeping your mobile banking app up to date, along with the device's operating system; looking out for rogue emails that ask you to login to your bank account via an included link – your bank should never ask you to do this; keeping your wits about you if you ever receive a text or phone call from an official claiming there is a problem with your account – no legitimate organization will ever ask

you to confirm all your details so don't give them out; only ever download banking and other apps from official sources, such as Google Play and Apple's App Store, as third party sites have often been known to host rogue versions of popular files; consider installing a mobile security solution – many apps, even from the biggest names in the security industry, are free on mobile platforms; if your bank offers a facility to send a text message whenever a transaction is auctioned on your account, take advantage of it, and check those transactions as and when they come through to ensure they were authorized by you

5.3 Area of Further Research

As for future research, it's better to reach out to mobile banking customers and conduct in-depth interviews with them about their experience, concerns and perception with security and protection level of mobile banking and level of awareness about the service and How do banks develop a security culture for their product and service. On the other hand it's better to asses legal and regulatory aspect of mobile banking service in related to customer protection.

REFERENCE

Abiy Woretaw; Lemma Lessa. (2012). Information security Culture in the Banking sector in Ethiopia. *in proceedings of the 5th ICT Ethiopia Conference.* A.A. Retrieved from http://www.ictet.org/downloads/Inf_L5ww9o_1X7b.pdf

Ahmad S. Mashhour; Zakarya Saleh. (2015). Perception of the Security and Acceptance of Mobile Banking Services in Bahrain: An Empirical Study Community. *International Journal of Advanced Computer Science and Applications, vol. 6, No. 9*.

Aleksandra Svilar; Jože Zupančič. (2016). User Experience with Security Elements in Internet and Mobile Banking. *49*.

Ayana Gemechu. (2014, june). Factors Affecting Adoption of Electronic Banking System in Ethiopian Banking Industry. *Journal of Management Information System and E-commerce, 1, No. 1;*.

Ayenew Wudu;Fekade Getahun. (n.d.). Mobile Banking Framework in the Ethiopian Context. *Journal of Computer Science and Technology, Vol. 1, No. 1*. Retrieved from http://www.hilcoe.net/docs/papers/Volume1N1/V1N1Paper7.pdf

Balcha, R. (2005). *State of Cyber Security in Ethiopia.* Addis Ababa: ETIOPIAN TELECOMMUNICATIONS AGENCY. Retrieved from https://www.itu.int/osg/spu/cybersecurity/contributions/Ethiopia_Reba_paper.pdf

Bhattacherjee, A. (2012). *SOCIAL SCIENCE RESEARCH:PRINCIPLES, METHODS, AND PRACTICES.* Florida, USA: The Global Text Project.

Consumers and Mobile Financial Services. (2012). *Consumers and Mobile Financial Services Reoprt.* Washington: The Federal Reserve Board.

FATF. (2013, June). PREPAID CARDS,MOBILE PAYMENTS AND INTERNET-BASED PAYMENT SERVICES. *GUIDANCE FOR A RISK-BASED APPROACH*. FINANCIAL ACTION TASK FORCE.

Gardachew Worku. (2010). Electronic-Banking in Ethiopia- Practices, Opportunities and Challenges. *Journal of internet Banking and commerce*. Retrieved from http://www.icommercecentral.com/open-access/electronicbanking-in-ethiopia-practices-opportunities-and-challenges-1-8.php?aid=38390

Guideline on ICT Security. (2015). Guideline on ICT Security For Banks and Non-Bank Financial Institutions. *Version 3.0*. Bangladesh Bank.

Institute for Development and Research in Banking Technology (IDRBT). (2011). IT Governance Series:Information Security Governance for the Indian Banking Sector. *Version 1.0*.

James, R. K. (2016). Establishing Mobile Financial Services in Ethiopia. *Walden Dissertations and Doctoral Studies*.

Kopchik, J. M. (2011). Mobile Banking: Rewards and Risks. *Supervisory Insights*.

Krugel, G. T. (2007, August). Mobile Banking Technology Options. *FinMark Trust*. TroyTyla.

Laleh Nosrati; Leili Nosrati. (n.d.). A review of Security Assessment in E- Banking. *Int'l Conf. Frontiers in Education: CS and CE*, p244 - 247.

M. Hassan, A. Rahman, S. Afrin, & M. Gulam Rabbany. (2014). Factors Influencing the Adoption of Mobile Banking Services in Bangladesh: An Empirical Analysis. *International Research Journal of Marketing*.

Malak, J. (2007). Readiness of the Palestinian banking sector in adopting the electronic banking system :exploratory study. *MA thesis*. The Islamic University of Palestine.

Marshall, C. & Rossman, G. (2011). *Designing qualitative research (5th ed.).* Thousand Oaks, CA: Sage.

Mauri, A. (2003, January). Origins and Early Development of Banking in Ethiopia. *SSRN Electronic Journal*.

Mobile Marketing Association. (2009, January). Mobile Banking Overviews(N/A). USA.

Mohamed Gamal Aboelmaged; Tarek R. Gebba. (2013). Mobile Banking Adoption: An Examination of Technology Acceptance Model and Theory of Planned Behavior. *International Journal of Business Research and Development ISSN 1929-0977, 2 No. 1,*, pp. 35-50.

NBE Directives No. FIS /01/2012. (2012). Regulation of Mobile and Agent Banking Services. National Bank of Ethiopia.

Negalign, M. & Lisanwork, A. (2016). The Development of Core Banking System in Ethiopia:Challenges and Prospects (Case Study on Ethiopian Commercial Banks). *Research Journal of Finance and Accounting, 7 (19)*, 32-41.

Patrick, D. G. (2011). Managing Information Security Risk: Organization, Mission, and Information System View. *U.S. Special Publication*.

Shaikh, M. A. (2014, september). Ethiopian Banker's Perception of Electronic Banking in Ethiopia – A Case of Adama City. *International Journal of Scientific and Research Publication, vol.4*(issue 9).

Sohail, S & Shanmugham, B. (2003). E-banking and customer preferences in Malaysia: an empirical investigation,information sciences-informatics and computer Science. *international journal of banking, 150(3/4).*

Ulas Akkucuk; Behcet Teuman. (2016). Assessing service quality in online banking services. *Problems and Perspectives in Management, vol.14*(issue 2), p 182-191.

Vaidya, S. R. (2011). Emerging Trends on Functional Utilization of Mobile Banking in Developed Markets in Next 3-4 Years. *International Review of Business Research Papers, 7. No. 1.*, Pp. 301 – 312.

Vishal Goya; U.S.Pandey; Sanjay Batra. (2012, june). Mobile Banking in India: Practices,Challenges and Security Issues. *International Journal of Advanced Trends in Computer Science and Engineering, 1, No.2,*.

Wondwossen Taddesse; Tsegai G. Kidan. (2005, October). e-Payment: Challenges and Opportunities in Ethiopia.

Yin, R. K. (2014). *Case study research: Design and methods (5th ed.).* Thousand Oaks CA: Sage.

APPENDIXES A: INTERVIEW QUESTIONS

Semi Structured Interview Questions

1. Describe the security futures of mobile banking service in your bank?
2. How to measure the effectiveness of the security mechanism that employed for mobile banking?
3. Describe the problem and challenges that hinders the security process?
4. How to manage the problem that hinder the security process?
5. Do you have any protection mechanism that protects customer from mobile banking fraudulent activity?
6. What kind of security risk happened in mobile banking service? how to management it? and what kind of methodology you have used?
7. How to measure the customer service protection level?

APPENDIXES B: MOBILE BANKING TERM AND CONDITIONS OF BANKS