Addis Ababa University Faculty of Business and Economics
Department of Management

FRAUD IN THREE ETHIOPIAN BANKS FOLLOW ON TECHNOLOGY DRIVEN BANKING SERVICES

An exploratory study on E-banking fraud management strategies: Managers perspective from the selected commercial banks in Ethiopia

A Thesis submitted for Partial Fulfillment of the Requirements for the Degree of Master of Science in Management

By: Yonas Worku

January 2020
Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY
FACULTY OF BUSINESS AND ECONOMICS
DEPARTMENT OF MANAGEMENT

FRAUD IN THREE ETHIOPIAN BANKS FOLLOW ON TECHNOLOGY DRIVEN BANKING SERVICES

An exploratory study on E-banking fraud management strategies: Managers perspective from the selected commercial banks in Ethiopia

BY: YONAS WORKU

A Thesis Submitted to the School of Graduate Studies, Addis Ababa University, Faculty of Business and Economics, Department of Management in Partial Fulfillment of the Requirement for the Degree of Master of Science in Management

January 2020
Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY
FACULITY OF BUSINESS AND ECONOMICS
DEPARTMENT OF MANAGEMENT

FRAUD IN THREE ETHIOPIAN BANKS FOLLOW ON TECHNOLOGY DRIVEN BANKING SERVICES

BY: YONAS WORKU (GSE/0536/10)

Approved by the Examining Board

Chairman, Department Graduate Committee	**Signature**
Research Advisor	**Signature**
External Examiner	**Signature**
Internal Examiner	**Signature**

January 2020
Addis Ababa, Ethiopia

DECLARATION

I declare that this thesis entitled "FRAUD IN THREE ETHIOPIAN BANKS FOLLOW ON TECHNOLOGY DRIVEN BANKING SERVICES" is a result of my own investigation, except where otherwise stated. I have undertaken the study independently with the guidance and support of my research advisor. Other sources are acknowledged by citations giving explicit references. A list of references is appended. The thesis has not previously been accepted for any degree and is not being concurrently submitted as an application for any degree in any university.

Signature: __________________________

Yonas Worku

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

Advisor's Signature: _______________________

Mesfin Fikre (PhD)

ACKNOWLEDGMENT

With deepest appreciation, I would like to acknowledge my advisor Dr. Mesfin Fikre for his unreserved assistance and experience sharing as well as guidance to make my study on this topic with thorough follow up in bringing it successful.

I would also like to recognize and forward my gratitude to the commercial banks' officials for their assistance in providing the necessary information throughout my visit to their office with a great appreciation of their willingness to have an access to the secondary data used in the thesis.

Moreover, I would also like to express my genuine appreciation to my beloved family and friends who gave me insight to work hard during my study.

Yonas Worku

January, 2020

Addis Ababa, Ethiopia

ABSTRACT

The study has tried to explore the strategies in use by the selected three banks in Ethiopia to improve their e-banking related frauds management. The study also goes through the types of frauds in brief for which strategies are deployed. The research design undergone on three banks having a total of 57.1 % market share in Ethiopia. Semi- structured Interview and examination of secondary data has been taken as a means of data collection. The qualitative approach with content and thematic analysis method is used to explore the phenomenon of the topic under study. Tangible and concrete outcome of the research is presented in such a way that it can be used by banks in Ethiopia as a source of practice for managing and minimize fraud related risks in complement with their own initiation and strategic direction. In addition to financial institutions, the government as well as the society can benefit from it because of the fund transfers traceability and ease mode of payments respectively can undergo with manageable level of fraud. The findings of the study depicts as banks and their customers are facing different fraud related problems, and those banks are trying to handle it by implementing different strategies at the various stages of the fraud. Based on the findings, it is recommended banks to identify their weakest link and make vulnerability assessment on their system in order to deploy the best and convenient fraud management strategies at hand.

***Keywords**: Financial Institution, Bank Fraud, e-banking services, Ethiopia, cyber security, Cashless Society, electronic or digital banking, banks in Ethiopia, strategy, fraud management. Fraud management strategies*

Table of Contents

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

AAU	Addis Ababa University
ATM	Automated Teller machine
BCCI	Bank of Credit Commerce International
CBS	Core Banking System
CEO	Chief Executive Officer
DOS	Denial of Service
E-Banking	Electronic Banking
E-Business	Electronic Business
E-Commerce	Electronic/Internet commerce
EMV	Europay Mastercard Visa
GSMA	Global System for Mobile Communication Association
IB	Internet Banking
ICT	Information Communication Technology
IMF	International Monetary fund
INSA	Information Network Security Agency
IP	International Police or Interpol
IPPF	International Professional Practices Framework
IT	Information Technology
MAG	Magnetic/Magnetic Stripe
MB	Mobile Banking
NBE	National Bank of Ethiopia
NFC	Near Field Communication
PIN	Personal Identification Number
POS	Point Of Sale
SOC	Security Operation Center

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

Ethiopia’s banking sector has undergone significant reforms since 1991, showing clear steps towards the explosion of privately owned domestic bank institutions (NBE, 2015). The change has led the way for the establishment of 16 private banks, 31 microfinance institutions, and 16 private insurance companies in the country. According to the NBE (2018), all 18 banks in aggregate have opened more than 4,757 branches from which 35.3% of the total is located in the capital city.

Since the beginning, Ethiopian banks focus is on branch network expansion at the expense of e-banking (NBE, 2015). According to the NBE (2015), out of 16.52 million bank account holders, there are only 746,050 e-banking services users. In the year 2019, the number of bank account reaches to double to what it was in the year 2015, but e-banking users is still not more than 6 million.

According to GSMA (2014), creating cashless society will benefit the society and the country as a whole in different ways; and this can be achieved only by the modern banking that can also be called electronic or e - banking. However, the slow diffusion of electronic banking negatively affects the profitability of banking businesses in most of the developing countries. But, there are also many challenges that do not let to create cashless society for the last two decades, and needs to overcome rapidly; the one and foremost problem is fraud.

As defined by Reserve Bank of India, fraud can be loosely described as any behavior by which one person intends to gain a dishonest advantage over another. Fraud encompasses a good range of illicit practices and illegal acts involving intentional deception or misrepresentation. Institute of Internal Auditors' International Professional Practices Framework defines fraud as "Any illegal act characterized by deceit, concealment, or violation of trust". (IPPF, 2009)

E-banking frauds on Ethiopian banks usually are not disclosed officially, as a result, there is little or no information in this aspect. Especially, for this infant stage e-banking services, related fraud and cyber security issues are not being disclosed enough by banks except the use of different fraud management strategies to overcome it. As a result, this study attempted to make the exploration on the frauds and fraud management strategies in use by the selected commercial banks in Ethiopia in relation to E- banking services.

1.2 Statement of the problem

According to Madan (2016), since banks are the engines that drive the operations in the financial sector and growth of an economy; with the growing banking industry in Ethiopia, frauds in banks also are increasing and fraudsters are getting more sophisticated and ingenious. The banking industry in Ethiopia calls rising fraud as "an inevitable cost of doing business."

On the other hand, now a day's going to branch for getting Banking services are unnecessary because, it is already accessible through E-Banking services, you can withdraw, make payment, Transfer money through this Technology but less attention is given to security aspects. (Tsegaye, 2017)

Bambore (2013) identified five major factors that affect implementation of e banking in the Ethiopian banking industry. Those are a) Fraud or security risk, b) lack of trust, c) lack of legal and regulatory framework, d) lack of infrastructure, and e) absence of competition between local and foreign banks.

Fraud, one of the major factors, is a worldwide observable fact that affects all continents and all sectors of the economy. Parties and organizations to get money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage, perpetrate frauds. Fraud affects organizations in several areas including financial, operational, and psychological. While the monetary loss owing to fraud is significant, the full impact of fraud on an organization can be shocking. In fact, the losses to reputation, goodwill, and customer relations can be devastating.

As frauds are often perpetrated by any employee within a corporation or by those from the outside, therefore, it's important to possess an efficient fraud management strategies in place to safeguard organization's assets and reputation (IPPF as cited in Madan, 2016).

In general, always when consumers' wants frictionless, smart and speedy payment processes through e banking services they also need their account to be protected and safe. On the other hand, while banks in Ethiopia are adopting electronic banking, then they are facing one of the identified five major factors that affect its implementation called Fraud or Security risk.

Therefore, from the bank managers' perspective, this thesis covers the exploration of e-banking related frauds and the strategies that are in practice by the selected commercial banks in Ethiopia to improve their fraud management.

The research aims to fill the research gap by disclosing the actual e banking frauds occurred in Ethiopia without affecting the respective banks reputation. Furthermore, in Ethiopian context, since there is little study in relation to the topic, this study explores on e –banking frauds from the respective managers' perspective with deployed strategies to overcome it so that it can be a base for subsequent studies.

1.3 Research questions

1.3.1 The general research question of the study:

- ❖ What strategies do commercial banks in Ethiopia are using to improve e-banking related fraud management?

1.3.2 Specific research questions that the study answers:

- ❖ What is the nature of e-banking fraud and the reasons behind those frauds?
- ❖ What fraud management strategies are in practice?
- ❖ How effective are those fraud management strategies?

1.4 Objectives of the study

1.4.1 The general objective of the study:

- The general objective of the study is to explore the strategies that the selected commercial banks in Ethiopia are using to improve e-banking fraud management by describing the frauds occurred in parallel.

1.4.2 The Specific Objectives of the study:

- To describe actual frauds that occurred on e-banking services of the selected banks
- To identify the fraud management strategies that are in practice by those banks
- To assess the effectiveness of those e-banking fraud management strategies in use

1.5 Scope and Limitations of the Study

1.5.1 Scope of the Study

The scope of the study was limited to the selected commercial banks in Ethiopia, even though there are more than eighteen banks in Ethiopia, for the sake of data availability and longer experience than others, the scope is limited to three banks. The study mainly tried to assess the fraud management strategies and practices in those three commercial banks in Ethiopia. The survey covers two departments of each selected banks, with document review and an interview question to the directors and managers of each department. Although, the term fraud is a broad concept, in this study the present researcher tried to focus on fraud management with special attention to electronic banking services of the banks.

1.5.2 Limitations of the Study

The researcher faces problems such as, shortage of sufficient source documents in Ethiopian context. Moreover, since respondents are bank managers and directors, they were so busy and engaged in meetings. The data collection was also very difficult because banks have already correlated the idea of fraud with their business reputation. Even though there were other constraints arise during the research of this study, the researcher tried to find sound results pertaining to the objectives of the study.

Note: For the sake of the selected three banks business reputation, copies of documents reviewed in parallel with the interview is not attached with annex. However, only for academic purpose, some copies are presented to confirm the reliability and validity of the data used in this thesis.

1.6 Significance of the Study

The study has attempted to show the actual existence of fraud on banks in Ethiopia by which it alert the government as well as the society. Going further on indicating its existence, it describes the strategies that the selected banks are using to improve their fraud management; with that, banks will share their experience to understand the better strategies. It also put some recommendations for effective management of frauds that follow on e-banking services.

Furthermore, the study can be used as further reference for other researchers to conduct further studies in the area and it will benefit the NBE, government banks, private banks, customers and a society as a whole to understand frauds, put caution in place and deploy controlling mechanisms.

1.7 Organization of the Study

The study deals about banking fraud management strategies that occur in relation to e banking services, focusing on the selected commercial banks in Ethiopia. It starts with introductory outlines under which an overview of the topic under study is presented as background of the study and then description is made on the statement of the problem. The research questions, the general and specific objectives of the study, the significance of the study, the scope and limitation of the study and organization of the study are followed along with it. The second chapter is dedicated to the review of related literature. Under this section of the study, a detailed coverage on the concepts of the proposed study is given.

Methodology of the study is presented in chapter three; and analysis of the research findings are presented in fourth chapter. Here an attempt is made to deal with presentation, descriptions, discussions and analysis of data, and findings with the implementation of the study. Finally, the fifth chapter presents the main findings, summary, conclusions and recommendations drawn by the researcher based on the analysis in chapter four. The thesis at the end contains a list of references, and attachments on the interview questionnaire, with few appendixes.

CHAPTER TWO

LITERATURE REVIEW ON BANK FRAUD

2.1 Introduction

A literature review is a systematic way to synthesize earlier works on a particular research topic. A literature review provides a framework for a researcher to build an overview of the phenomenon, thereby helping to identify major controversies and gaps that the research can fill (Walker & Solvason, 2014). My literature search on e-banking service fraud management strategies include information on the development of electronic banking and competitive advantage, frauds registered or occurred so far, strategies to manage frauds, rival theories of the conceptual framework, and a methodology review. Accordingly, this literature review included information on the current research, the significance of the results, and gaps in current knowledge.

Several databases provided source material for the review. I used journal articles, dissertations, and other reference material from the Internet to conduct the literature review. The primary databases searched for this study includes Addis Ababa University Digital Library for research and publications, Journals of Banks in Ethiopia, SAGE Research Methods Online, World Bank, and sources from Google Scholar.

Various keywords and phrases used when conducting the search on scholarly documents includes fraud on banks, cashless society, E-banking, E-business strategy, fraud management, fraud management strategy, cyber security, modern banking, competitive advantage and IT on business alignment etc. I use two methods to search literature: The broad exploratory approach and specific detail approach (Ford, 2012). The broad exploratory approach is used to build a generic overview on the topic by searching information on the Internet. The specific detail approach helps to collect peer-reviewed literature in line with the research topic under this study.

The reference includes books, peer reviewed journal articles, government reports, non-governmental associations, and Internet sources relevant to the research topic, questions, and design.

2.2 Technology and Business

General resources such as high-quality human resource help commercial banks to internationalize their business (Panda & Reddy, 2016). Doherty & Terry (2013) noted information system makes an indirect contribution to improve the competitive organizational position. Organizational resources such as continuous innovation, stakeholder integration, shared visions, and early adoption is vital for Green IT performance (Abdulrahim & Abdulrahman, 2013). Resource-based co-innovation through a platform ecosystem appears a successful strategy for mobile payment service innovation (Zhong & Nieminen, 2015). Intra organizational resources such as top management support and information technology are two vital enablers of supply chain integration and thereby business performance (Xu, Huo, & Sun, 2014). Like many other countries around the world, Ethiopia has embraced ICTs and ICT based services as key enabler for societal and economic development in the nation (Halefom, 2014).

Few scholars, argue that IT could not be a source of competitive advantage (Chi and Sun, 2015). According to Chi and Sun (2015), even though IT can increase performance as well as have a high value for customers, there is no evidence to support it leads to highest business profitability. Carr (2003) argued since IT becomes a commodity, easily acquired and duplicated, the value goes away and no more competitive advantage comes out of it. However, Bhatt and Grover (2005) opposed Carr’s point of view and argued firms can develop distinct capabilities in managing IT. According to Bhatt and Grover, a competitive advantage does not stem from the IT infrastructure itself but the company's capabilities in organizational learning intensity, IT business experience, and relationship infrastructure.

According to Porter (1985), understanding and coping with competition is the key tenet of the strategy process. Porter sees technology as one of the change drivers in industry structure and firms must incorporate it into their strategy so that they can gain a competitive advantage by exploiting the market opportunity. IT is one form of the technologies that affect competitive advantage positively if it is well integrated into firm’s business strategy and enables a firm to achieve a low cost and differentiation through its value activities (Porter, 1985).

2.3 Technology and Banking

According to the international payment schemes; VISA and MasterCard, the international market is still based on a strong use of cash. This represents a tremendous opportunity to growth for electronic payments. Consumers are asking for payment solutions always more; safe and reliable, convenient and innovative. New not traditional players have already entered and are pushing to enter the payments market (e.g. PayPal) in order to offer innovative payment solutions. (Mastercard Academy, 2018)

The banking sector in Ethiopia is one of the rapidly growing sectors of the country's economy (Abiy and Lemma, 2012). Using ICT all banks of today are providing new technology driven services like ATM, POS, Mobile banking, Internet banking and mobile money and very recently ecommerce is on launching stage by many banks.

Bank clients can access financial services (i.e. whether it is transactional or non-transactional) through online channels from anywhere at any point of time (Lie´bana-Cabanillas, Mun˜oz-Leiva, and Rejo´n-Guardia, 2013). E-banking channels enable individuals to make real-time financial decisions conveniently independently of time and location (Sikdar, Kumar, & Makkad, 2015). Mishra and Bisht (2013) pointed out electronic banking enables customers to access financial services without limit in time, place, and the type of agents they use. The core use of online banking, therefore, are convenience and low-cost advantage thereby customer satisfaction (Aliyu, Rosmain, & Takala, 2014; Liébana-Cabanillas et al., 2013).

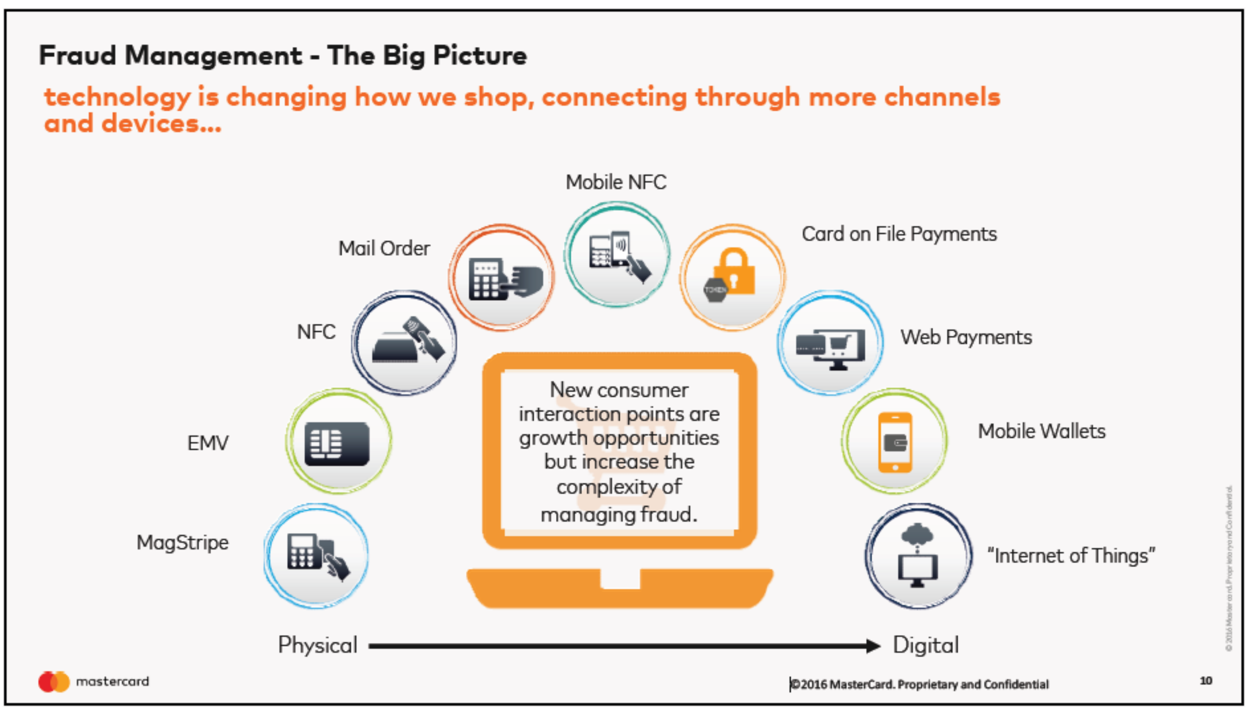

Figure 2.1: Changing Payment Technology **Source: MasterCard Academy**

The provision of electronic banking becomes a lucrative business and the area where companies compete to gain competitive advantage and increase efficiency (Dauda & Lee, 2015). Mobile banking technologies combining with smart technologies create opportunities for Africa to leapfrogging the traditional ways of delivering banking services (World Bank, 2013). It uses as a catalyst to speed up the pace of change in financial services thereby achieve financial inclusion and to overcome geographical barriers (Baptista & Oliveira, 2015). Hence, to tap the unleashed potential of technological innovations, the issue of digital banking becomes a topic of great interest to the business strategists of financial institutions (Liébana-Cabanillas et al., 2013)

2.4 E-Banking and Fraud

Historically, according to An International Multi-Disciplinary Journal, Ethiopia Vol. 4 (3b) July, (2010), Bank of Credit Commerce International (BCCI) $10 billion fraud globally and Japan Fuji Bank $3 billion forgery both happens in 1990. In Japan, the bubble burst in the financial sector in the early 1990s, due to unrealistic valuation of land, share prices manipulation, CEOs fiendish incompetence, uncontrolled poaching of staff, financial engineering, enormous uncollectible bad loans, and issuance of fake certificate. These were reasons for the collapse of Japanese financial segment. As it happened in japan in 1990s, some banks in Africa may face the same tragedy unless they are carful from the current day frauds. For example, most symptoms of those days in Japan are prevalent in the Nigerian financial sector today. It is obvious that, land speculation, weak internal process, blue-chip syndrome, absence of a structured succession plan and poaching staffs are pervading the Nigerian financial sector and all these are agents of fraud.

Some persons have different motivations that are not in line with the use of Information Technology within the confines of proper ethical and sometimes even legal conduct (Dwight as cited in Behabtu, 2015). Unfortunately, not everyone wants to use this advancement for the greater good. Even though the use of IT offers so many advantages to organizations, numerous inherent risks must be mitigated in order to successfully Secure Ethiopian banking sector services. Based on a recent survey, employee fraud in the financial services industry is a widespread problem that is largely attributed to advances in technology. Employees who have access to information systems are usually the ones with the tendency to bargain (Esola as cited in Behabtu, 2015). But the outside environment also bring a lot of fraud risks in relation to cyber security as it already brings a new technology driven banking services too (Behabtu, 2015).

According to Accenture (2015), change in consumers' demography, the expansion of banks into new marketplace, and the implementation of new technologies and channels present new challenge in fraud protection. Rapid technological and social changes alter the relationship between banks and their customers in a way that creates new opportunities for fraudsters (Madan, 2016). It's an endless game of cat and mouse between financial institutions and cyber-criminals. There is a virtual arms battle taking place online between banks and cyber criminals, who as soon as the bank implements a new process or technology to avoid online fraud, they find a weakness to exploit (ACL, 2013; Dzomira, 2014). In addition, customers expect to be protected from fraud, and also want anti-fraud tools to look at them holistically, assessing the fraud risk of transactions by their individual profiles.

There is no single way to squeeze fraud, but by implementing the right mix of different technologies and prevention techniques, bank executives can greatly reduce their organization's risk. As Accenture's Santoro puts it, a solid portfolio of solutions with multiple layers of protection and controls can go a long way toward providing the necessary protection. If you put enough deadbolts at the door, thieves are going to give up and look elsewhere. The information security world has recently started becoming aware of another threat that had more devastating consequences and was substantially more difficult to tackle. This time, the threat was not coming only from external hackers, but from authorized users of IT systems. These users abuse their privileged access rights by committing a series of unintentional or deliberate actions damaging individuals or organizations in many different ways. The global information security survey by PwC (2014) reported that the number of security occurrences increased by 25% in 2013, among which 58% were performed by current (31%) or former employees (27%). Consistently, Verizon (2013) found an increase of more than 10% of reports regarding security breaches committed by insiders.

According to Behabtu (2015), the growing threat of the malicious insider has given rise to a number of long-term research projects on different sectors of the country. The Information Network Security Agency (INSA) identified several critical infrastructure sectors that require special attention in protecting the cyber space from any possible attacks. Some of them are Banking and finance, Information and telecommunications, Energy, Defense base and related technological infrastructures.

Information assets are under serious threats and attacks from insiders day in and out in the government and private Banks. With the advancement of information Communication technology (ICT), Banks collect a lot of confidential information about their, customers, employees and financial status. A lot of the information being collected are processed and stored electronically and with the widespread use of the information technology, the risks of theft and attack are expanding by the day whilst pressure is also being mounted on information security infrastructure. In case any confidential information such as customer's information and trade secrets fall into wrong hands, it will lead to negative consequences like loss of goodwill, customers and profit. In a financial institution such as a bank, likely targets are customer account records or perhaps company accounts, where there is a direct access to funds. (Behabtu, 2015).

Banking and Finance sectors in Ethiopia are now becoming more sophisticated; almost all banks have already implemented CBS (Core Banking Solutions) with the advancement of such technologies enabling services like Mobile Banking. Internet Banking and Card Banking are getting easier and those enablement have simplified almost all operation performed in the Banks.

Security issues are sources of concern for everybody more especially as it concerns banking industry. Electronic banking is prone to security breaches such as fraud, theft of commercially sensitive or financial information, vandalism of web sites or denial of service (DOS) and faults in system design and set up leading to security breaches. All these security violation or breaches have potentially serious financial, legal and reputational impacts. (Kassahun, 2016)

2.5 Fraud management strategies and practices: Empirical evidence

E-banking transactions are significantly growing year by year, at the same time, new fraud techniques, if not contrasted quickly and effectively, can put at risk the reliability of the electronics payments, destroying progressively the Cardholders trust. Consumers' wants for frictionless, smart and speedy payments to process their accounts protected against fraud with speedy resolution of disputed transactions. (Mastercard Academy, 2018)

According to MasterCard Worldwide research, the international experience shows that, across the globe, a number of very clear truths prevail. The truths are fraudsters will operate and survive in every market; fraudsters will migrate to the weakest link. There is no one golden cure that resolves all fraud types, significant losses/risks are often not understood and remain an issue and a high proportion of fraud teams do not understand the negative impact they could and are having on their business revenue and profits.

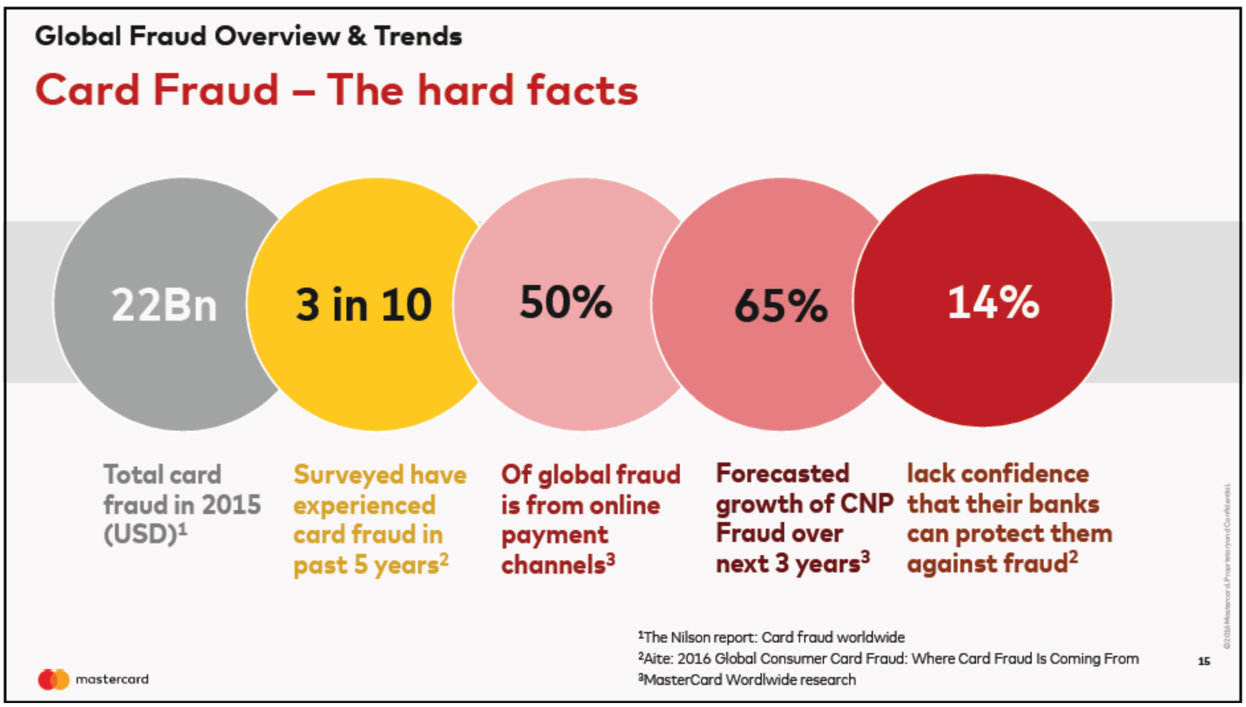

Figure 2.2: Global card fraud- The hard facts **Source: MasterCard Academy**

The current Fraud losses are just the tip of the iceberg. Optimizing fraud management program will provide many opportunities to reduce the full expense of fraud mitigation program while ensuring fraud losses stay on target.

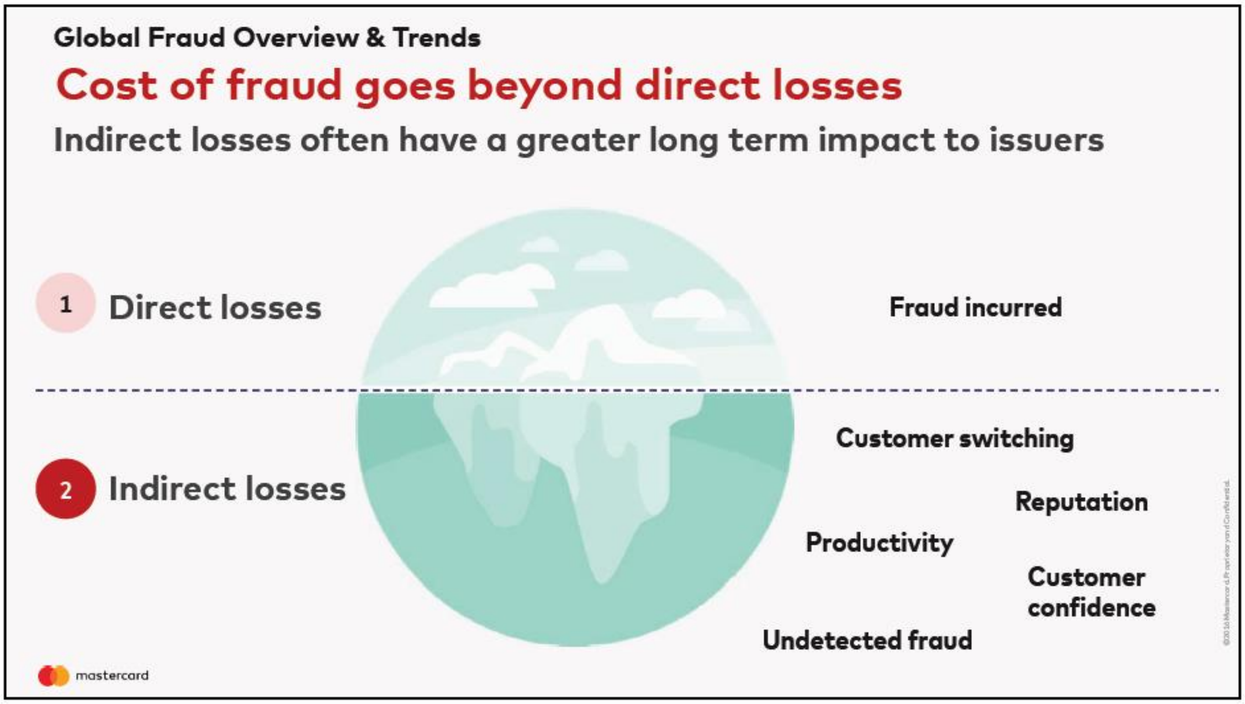

Figure 2.3: Cost of fraud **Source: MasterCard Academy**

According to Evalyne (2018), Fraud Management Lifecycle is made up eight stages, demoralization, expectation, distinguishing proof, control, examination and arraignment. This speculation suggests that the last stage, arraignment, is the summit everything being equivalent and disillusionments in the fraud management lifecycle.

Financial Fraud management practices include internal control, Training, employee and third party screening and whistleblower protection. Effective internal controls are account reconciliation, law enforcement, investigation and law and audit committee and senior management oversight, monitoring systems designed to detect fraud, establishment of internal controls and management review. Additionally, there is proactive data analysis and use of information technology to prevent fraud. (Evalyne, 2018)

Given the prevalence of fraud and the negative consequences associated with it, there is a compelling argument that organizations should invest time and resources towards tackling fraud. There is, however, sometimes debate as to whether these resources should be committed to fraud prevention or fraud detection. Prevention techniques include the introduction of policies, procedures and controls, and activities such as training and fraud awareness to stop fraud from occurring. As fraud prevention techniques may not stop all potential perpetrators, organizations should ensure that systems are in place that will highlight occurrences of fraud in a timely manner. This is achieved through fraud detection. (CIMA, 2008)

It should never just be about minimizing fraud losses or catching the crooks, instead the main objective of optimized fraud management is “Maximize revenue while maintaining an acceptable level of fraud risk.” According to CIMA (2008), an effective anti-fraud strategy in fact has four main components; those are Prevention, detection, deterrence and response.

Payment card fraud is a sophisticated crime carried out by criminals using modern technology, these fraud payments have resulted into losses. Therefore, driving increasing efforts in card fraud prevention and detection as well as implementation of robust card fraud management response strategies such as the new laws which were enacted to compel banks to maintain set security standards and open the card networks to external auditors. (Doody as cited in Allan, 2016)

Fraud management optimization provides opportunities typically include Increase in sales, improved approval rates (e.g. application and transaction), improved portfolio profitability with reduced fraud write-offs, cost-efficiency/Cost Management, productivity opportunities (e.g. improved workflow) and decreased customer impacts and minimized risk exposure with improved customer retention

According to Mastercard Acadamey (2018), at the past, the fraud risk manager's role was seen as very straight forward; they worked to prevent the fraudsters from doing their thing, and focused on managing the cost of fraud losses. Banks have had a tendency to focus on their fraud basis points position, rather than on the impact to sales and other important business drivers. But at the present time and in the future, the roles and responsibilities of fraud management personnel are far more complicated with a broader understanding of and focus on the impacts that their policies, processes and decisions have on the greater business. Moreover, banks must focus on the delicate balance that exists between revenue, customer experience and fraud loss and how changes to one have a direct and significant impact on the others.

Evaluating the true costs of card fraud losses is a complex business. On one hand, it can be split between issuer fraud, acquirer fraud, and merchant fraud. In addition, it can be split between fraud prevention, fraud detection and investigation, and recovery activities. (Cards & Mobile payments industry intelligence, 2015)

2.6 Research Gap

It was discussed on the literature part; most of the studies undertaken are related to Electronic banking and fraud. Different researchers in different research techniques showed different perspective about the use of ICT while commonly agreed about the basics of fraud.

1. Use of ICT or information system is positively concluded by ten researchers as it increases an organization performance and used as competitive advantage and it is not considered as source of competitive advantage by another five researchers.

2. Considering IT with respect to banking services, seventeen researchers have shown as digital/electronic banking positively affect financial sectors profitability and efficiency, and creates convenience to customers. But, no negative effect is found by any of the researchers.

3. Three researchers found out about insider fraud and one researcher explains fraud from the outside environment.

4. The existence of mouse and cat game between financial institution and fraudsters is elaborated by two researchers

5. Three researchers depict the potential loss of fraud but no researcher showed the magnitude of actual fraud happened in Ethiopia.

6. The empirical evidences presented the international digital banking & fraud management strategies, and the amount & types of losses due to fraud globally, but not in Ethiopia.

Even though there are researchers that contradict the use of ICT as a means of competitive advantage and business performance but many of the above stated researchers showed the use of ICT for business. Specific to banking industry, all researchers have concluded the same as digital or Electronic banking has positive effect on the profitability and convenience to banks and customers respectively. Previous researchers have shown as there is fraud both by insiders and outside environment, and described the potential loss of frauds.

On the other hand, there were also items not researched by the above researchers such as the type of e-banking frauds in Ethiopian banks and little attention is given about how do banks in Ethiopia is actually practicing fraud related cases and managing those frauds, thus the researcher is interested in exploring on the type of e-banking frauds. Moreover, in order to fill the research gap, the researcher interest is to study about the Ethiopian banks experience of implementing strategies that are necessary to improve the fraud management practices.

CHAPTER THREE

METHODOLOGY OF THE STUDY

3.1 Research Method

In order to answer the research questions and address the objectives, qualitative research methods were employed. Kaczynski, Salmona, & Smith, 2014 (as cited in Teklebrhan, 2017) described as the qualitative method focuses on understanding participants' perspective, experiences, decision making, and phenomena. In this research, a qualitative approach was chosen in order to directly communicate with the directors and managers of the selected banks and explore from their experience and perspectives. Marshall and Rossman (2014) noted the qualitative method is a better approach than the quantitative method in gaining a better understanding of the complexity of human experiences or phenomena. Moreover, in this research, the selected qualitative method helped to approach the managers and get the necessary information on this complex and sensitive issue of fraud.

Leedy and Ormrod (2015) also mentioned the qualitative method is useful in a situation when variables are unknown, little information exists on a topic, and there is an inadequate or missing relevant theory base. Since the research question is in relation to fraud and banks usually prefers to hold such kind of information confidentially for the sake of their reputation, the qualitative method employed helped the researcher to grasp well on the topic on which little information is out there.

Accordingly, exploration of the actual e-banking frauds focusing on the types of strategies in use by the selected three banks in Ethiopia for fraud management is made in this study using a qualitative approach.

Zahir, Basias, Themistocleous, & Morabito (2013) pointed out qualitative research enables researchers to understand, explain, explore, discover and clarify situations, feelings, perceptions, attitudes, values, beliefs, and experiences. Therefore, in this study, since the topic in relation to e-banking frauds in Ethiopia is studied little, the researcher used qualitative method to explore frauds and fraud management strategies mainly on e- banking services. Exploratory studies help a researcher gain initial insights into a topic that has previously been little studied (Leedy & Ormrod, 2015). It is useful to investigate little-understood phenomena and identify relevant categories of meaning (Marshall & Rossman, 2014).

3.2 Research Design

There are several qualitative designs, but the researcher have chosen phenomenology design. In order to select it, I have considered three popular designs including phenomenology, ethnography, and case study. While phenomenological researchers concentrate on understanding, the essence of participants' lived experiences (Cibangu & Hepworth, 2016), researchers using an ethnography design seek to describe and interpret a culture-sharing group (Lewis, 2015; Simpson et al., 2014). Case study is useful in situations when the research aimed at answering how or why questions and the focus of the study is a contemporary phenomenon. (Leedy & Ormrod, 2015)

Since the purpose of this study is to seek the essence of participants' lived experience i.e. selected banks in Ethiopia and understanding of the phenomenon but not to interpret group's culture. Thus, the phenomenology is found to be more appropriate than ethnography and case study designs for this study, so it used by the researcher.

3.3 Sources of data, Population and Sampling

The necessary data for the study is collected from three banks in Ethiopia. From the selected three banks, electronic payment departments and internal control departments of each bank, with six departments in total, are the specific source of the required information. Cases from all branches are forwarded to the above stated head office organs, so the necessary information that the branches and other departments can provide is also obtained from those departments.

Choosing an appropriate sampling method enhances the trustworthiness of the research (Robinson, 2014). For this study, for the purpose of data availability and experience, the researcher used purposeful sampling technique to select participants from the target population in those departments. By using purposeful data sampling technique, the researcher was able to make the experienced staffs from the selected departments i.e. managers and directors to be part of the necessary source of information.

Regarding the sample size, there is no single formula or criterion to use in the qualitative study rather depends on the research objective, method, and available resources (Boddy, 2016). Moreover, Sauro (2015) described the five types of qualitative approaches methods related to focus, sample size and data collection methods as stated below:

Table 3.1 Five types of qualitative methods

Methods	Focus	Sample size	Data collection
Ethnography	Context or culture	0	Observation
Narrative	Individual experience and sequence	1-2	Stories from individuals and documents
Phenomenological	People who have experienced a phenomenon	5-25	Interviews
Grounded Theory	Develop a theory from grounded in field data	20-60	Interviews, then open and axial coding
Case study	Organization, entity, individual or event	-	Interviews, documents, reports, and observation

By evaluating the different types of qualitative approaches, the researcher has chose to use phenomenological type approach. Based on that, interviewed 12 different level leaders at the respective departments of the selected three banks. With this sample size, the researcher were able to include all directors and responsible managers of all the six departments.

3.4 Data Collection Methods

The qualitative researcher is expected to draw upon multiple (at least two) sources of evidence; that is, to seek convergence and corroboration with different data sources and methods. Apart from documents, such sources include interviews, participant or non-participant observation, and physical artifacts (Yin, 2014). Therefore, for this study, from the primary source of data, semi-structured interview is used for retrieving participant perceptions as the principal data collection method to assess the banks lived experience in fraud management strategies. In addition, from the secondary source of data, document review is used as a supplementary source over the semi-structured interview in order to explore the actual frauds that occurred on the selected banks.

In qualitative studies, a researcher is the primary instrument of data collection, analysis, and reporting (Frels & Onwuegbuzie, 2013; Leedy & Ormrod, 2015). For this research, the researcher direct participation in the collection of the necessary data helped to explore and get the necessary explanation as required. A qualitative interview is a suitable method for a more flexible response (Comi, Bischof, & Eppler, 2014). According to Nguyen (2015) researcher can collect accurate data using semi-structured interview if there is trust between the researcher and participants. So, by properly approaching the interviewees, the researcher was able to build trust that helped to collect convenient information from the semi-structured interview as well as reviewing of documents.

3.5 Data Analysis Methods

Qualitative data develops concepts that help to understand social phenomena in natural settings rather than experimental, by giving appropriate importance to the meanings, experiences and views of the participants (Cibangu & Hepworth, 2016). In this research, data collected using a semi-structured interview and document review is analyzed using thematic analysis and content analysis methods. The themes used in interview transcripts are applied to the content of the documents reviewed. Themes they generate serve to integrate data gathered by both methods.

Thematic analysis is a form of pattern recognition within the data, with emerging themes becoming the categories for analysis (Fereday & Muir-Cochrane, 2006). The process employed for this research involves a careful, more focused re-reading and review of the data collected by both methods. The reviewer takes a closer look at the selected data and performs coding and category construction, based on the data's characteristics, to uncover themes pertinent to a phenomenon.

Since several methods are available to analyze qualitative data, the researcher has revised and checked the convenience of the below most commonly used data analysis methods before selecting content and thematic analysis:

Content analysis: This is one of the most common methods to analyze qualitative data. It is used to analyze documented information in the form of texts, media, or even physical items. When to use this method depends on the research questions. Content analysis is usually used to analyze responses from interviewees.

Narrative analysis: This method is used to analyze content from various sources, such as interviews of respondents, observations from the field, or surveys. It focuses on using the stories and experiences shared by people to answer the research questions.

Discourse analysis: Like narrative analysis, discourse analysis is used to analyze interactions with people. However, it focuses on analyzing the social context in which the communication between the researcher and the respondent occurred. Discourse analysis also looks at the respondent's day-to-day environment and uses that information during analysis.

Thematic analysis: is a form of pattern recognition within the data, with emerging themes becoming the categories for analysis

Grounded theory: it uses qualitative data analysis to explain why a certain phenomenon happened. It does this by studying a variety of similar cases in different settings and using the data to derive causal explanations. Researchers may alter the explanations or create new ones as they study more cases until they arrive at an explanation that fits all cases.

Document analysis is often used in combination with other qualitative research methods as a means of triangulation ‘the combination of methodologies in the study of the same phenomenon’ (Denzin, 1970). Therefore, for this study, by examining information collected through different methods, the researcher was able to verify findings across data sets and thus reduce the impact of potential biases that can exist in a single study. According to Patton (1990), triangulation helps the researcher guard against the accusation that a study’s findings are simply an artifact of a single method, a single source, or a single investigator’s bias. Therefore, as described above, by triangulating the data, the researcher attempts to provide a confluence of evidence that breeds credibility.

In qualitative data analysis the steps starts from being familiar with the data, coding into themes, searching for patterns and connections finally interpretation of the data and drawing conclusions.

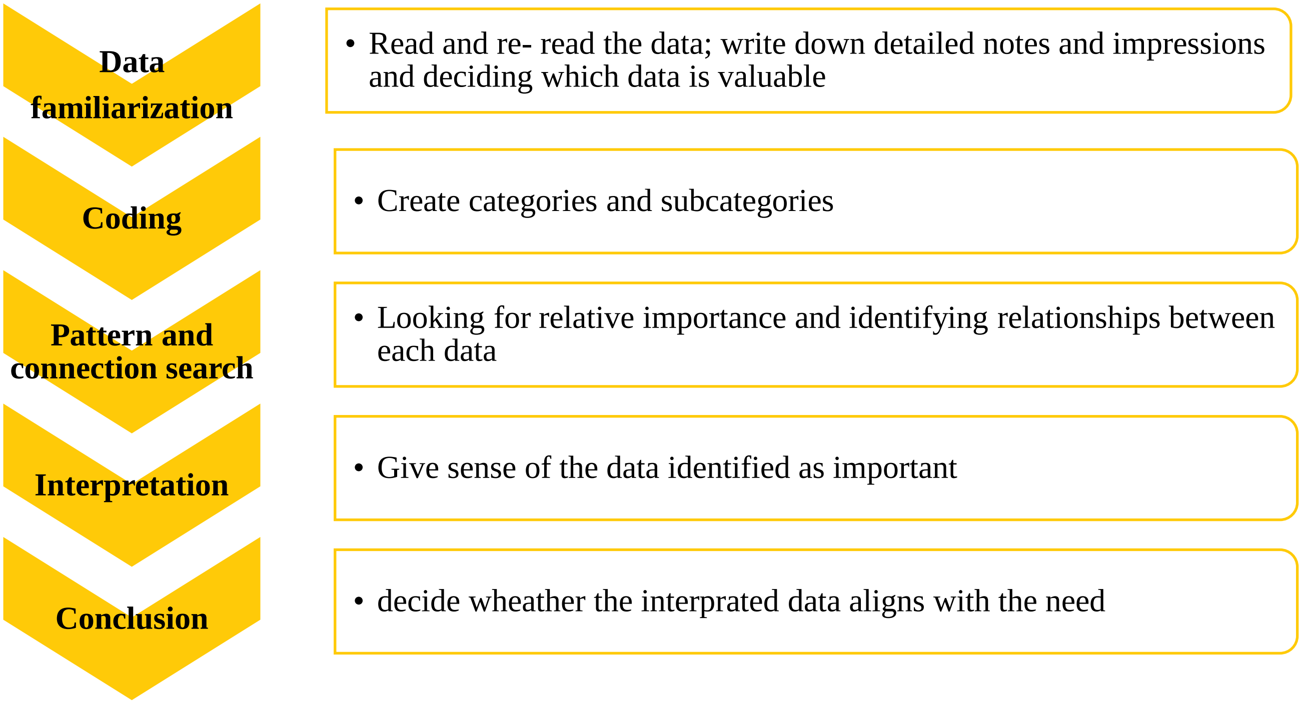

Figure 3.1: data analysis steps

The document analysis employed involves skimming (superficial examination), reading (thorough examination), and interpretation. This iterative process helped the researcher to combine elements of content analysis and thematic analysis. By using the content analysis method the researcher was able to organize information from document review into categories related to the central questions of the research. It entails a first-pass document review, in which meaningful and relevant passages of text or other data are identified.

CHAPTER FOUR

DATA ANALYSIS AND FINDINGS

4.1 Introduction

In this part of the paper, the researcher attempted to analyze the data collected through semi-structured interview and document analysis using thematic and content analysis methods. For this purpose, the researcher has interviewed six department directors and six unit managers i.e. Total of twelve leaders of the selected three banks in Ethiopia. Various documents like procedures, correspondence letters and interdepartmental memos from internal control and electronic banking departments of the selected three banks are also reviewed as a supplementary source of data and analyzed all together accordingly.

4.1 Analysis and Findings

The main research question that guided the study was: What strategies do commercial banks in Ethiopia are using to improve e-banking related fraud management. Thoroughly, questions like the following are answered; what is the nature of e-banking fraud and the reasons behind those frauds? What fraud management strategies are in practice? Moreover, how effective are those fraud management strategies?

Therefore, I was able to obtain relevant information and data for the study by purposefully sampling two departments in those selected three commercial bank in Ethiopia. The sample size for the study and method triangulation was used to achieve data saturation (Fusch & Ness, 2015).

Participants met the research criteria of being leaders in the selected departments of commercial banks and experienced in devising and implementing fraud management strategies for several years. The participants lived in Addis Ababa, Ethiopia. A total of twelve bank directors and managers are participated in the semi-structured interviews. I sent an authorization request letter to the banks' Human Resource development departments for permission and have access to relevant documents for the study before communicating the participants. Subsequently, I contacted each participant to participate in the study. I conducted all interviews in two-week period, and each interview lasted not more than 40 minutes. After the transcription of each interview, I interpreted the participants' responses and conducted member checking by requesting personal feedback from each participant during and after the interview to enhance the validity of the results.

Document analysis is often used in combination with other qualitative research methods as a means of triangulation 'the combination of methodologies in the study of the same phenomenon' (Denzin, 1970). As a qualitative researcher, I have drawn multiple (two) sources of evidence; that is, to seek convergence and corroboration with different data sources and methods. So apart from the Semi-structured interview, document analysis is made with the thematic analysis of the Semi-structured interview.

I used an assigned code from P1 to P12 to identify each participant. Before the completion of the interviews, I reviewed documents about the nature of e-banking fraud and the reasons behind those frauds to ensure methodological triangulation. In the following section, I have presented the key themes and the findings from each interview question and document review.

Based on the central research question and according to the empirical evidences as indicated in section 2.5 (Fraud management strategies and practices: Empirical evidence) data analysis of participants' responses led to the identification of three core emergent themes: a) Prevention b) Detection and c) Resolution

The next component includes a detailed analysis of each theme. The themes emerging from this study reflects a common set of characteristics and strategies that commercial banks are using.

Theme 1: Prevention

Ensuring prevention mechanism is at the core of the bank's e-banking fraud management strategy. Prevention is referred the most up-to-date fraud prevention tools and services to minimize fraud incidents. A thematic analysis of the participants' answers to interview questions 2, 3 and 4 showed as prevention is a key strategic resources to improve the management of e-banking fraud (Table 4.1).

Table 4.1: Fraud Prevention *(Interview Question 2, 3 and 4)*

Participants' answers to interview question #2, #3 and #4	**Interpretation and analysis**	**Emergent themes**
P1 "….our customers are protected based on the Policy set by the board of directors and top management and for that they are willing to use e-banking services" P2 "… guidelines we are using, that are necessary to avoid fraud are not maintained up-to-date even though it is necessary to improve e-banking fraud	Several participants related legislations, policies and guidelines are necessary for fraud protection and helps to improve e-banking fraud management	Fraud prevention using Legislation, Policy and guidelines as a means for e-banking fraud management

management ” P5 “…. In order to improve the e-banking service the local and international legislations should be properly respected …. Those are also controls to prevent fraud…		
P3” …regular review of merchant contracts helps to fill gaps and protect customers against fraud which let customer service to be more convenient and…” P5 “…contracts that clearly outline responsibilities and regular visit to merchants helps us to minimize fraud and improve the POS services”	Merchant contract management is one of the fraud prevention mechanism	Fraud prevention using Merchant contracts as a means of for e-banking fraud management
P4” … compliance with physical card production process requirement is our key method to prevent fraud… customers will be safe…” P6 “ ...card design let customers to be attracted and this will improve the service but the main point is access control, storage of plastic cards,	Standard card production process is one means of fraud prevention	Fraud Prevention using standard card production to improve e-banking fraud management

destruction of damaged and waste cards are critical points in preventing fraud”		
P5” … We use different card holder education methods like initial awareness, card security training and ongoing education, this help customers to use our services and also to be protected from fraud” P6”… always customers’ confidence increases with much education and awareness sessions we prepare…” P11”…Merchants awareness creation sessions were fruitful in increasing successful transaction rate of the bank”	Creating awareness on customers used for improved service delivery and also it makes customers to be protected from fraud	Fraud prevention by awareness creation in managing e-banking frauds
P2” … PIN generation options that we are using is random and fully automated.” P4”… the pin mailer is fully sealed by the machine and it is accessible for customers only, this makes our customers to feel safe and it is also a	PIN generation and delivery is one of the service improvement means with fraud protection in parallel	Fraud prevention by means of secured pin generation helps for e-banking fraud management

means of fraud protection"		

In the data analysis, I have used word clustering and tree projection of the dominant perceptions of participants on the role of various strategies used to improve fraud management. Prevention, the first core themes from data analysis revealed the following five perceived strategies for the participants involved in the study: Legislation, Policy and guidelines, Merchant contracts, Standard card production, Awareness creation and Secured pin generation. (Figure 4.1)

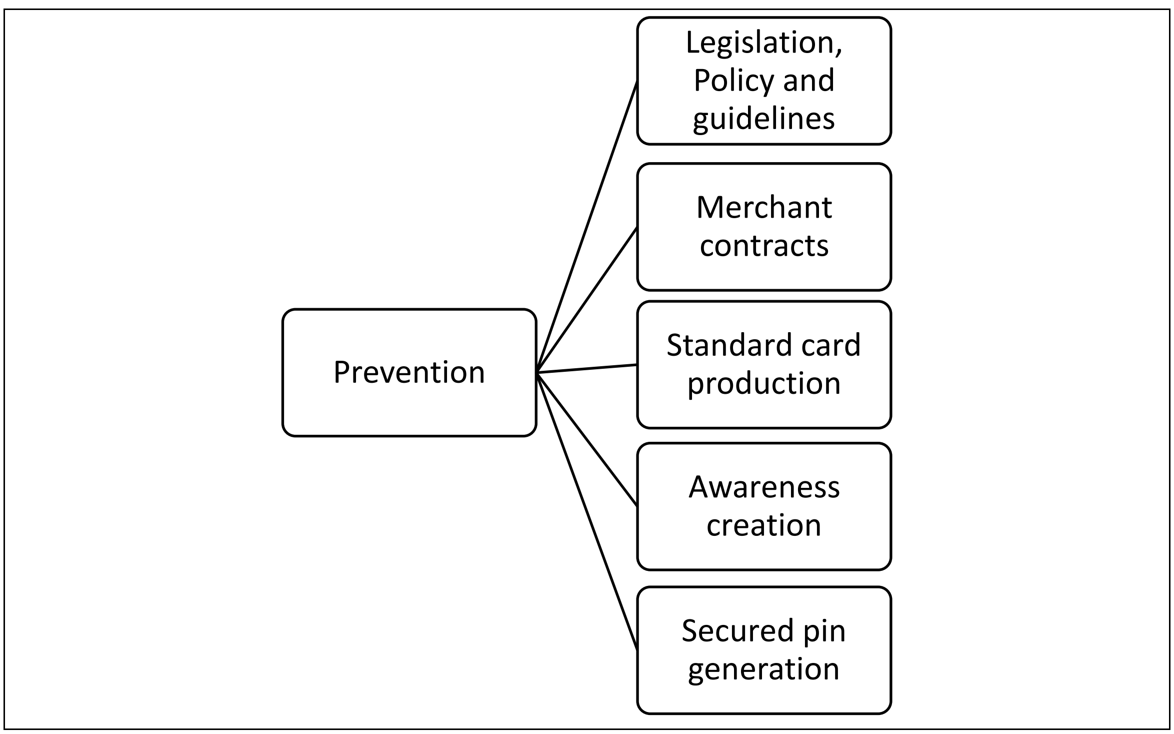

Figure 4.1: Word clustering on fraud Prevention

Twelve participants (Table 4.4) representing the highest frequency of occurrence, perceived strategy of using legislation, policy and guideline led to successful fraud management. The perception of these 12 participants is congruent with the view of Haag and Cummings (2008). Haag and Cummings argued strategy drives technology decision, not the reverse. According to Haag and Cummings (2008), ensuring alignment between strategy and selection of technology enable the organization to achieve its business objectives. The issue of leading through strategy and ensuring strategic alignment is the highest priority of the bank's leadership.

Sixty-Seven percent of the participants (Table 4.4) claimed that the bank's contract with merchants who receive payment for transactions through POS machines is one means for improving e-banking fraud management. P3, for example, stated, "Regular review of merchant contracts helps to fill gaps and protect customers against fraud".

From the documents reviewed, Manual card or card not present transaction on POS is the one that create a great opportunity for fraudsters. Due to this card absent transaction, banks in Ethiopia has lost huge amount of money by charge back requests. Starting from 2017, for the last three years, 115 transactions amounting of 10,779,995.21 are fraud related chargeback. (Table 4.2)

As per international payment facilitator VISA and MasterCard, the main reasons for chargeback have been categorized in to four broad parts; namely, Customer disputes, Fraud, Processing errors and Authorization issues.

From both MasterCard and Visa international card transaction, starting from 2017 more than 28,368,408.45 birr and 409 numbers of transactions made on 126 merchant sites of the selected three banks raised a dispute and those banks have lost most of the disputed amount. Customer disputes, fraud, processing error and authorization issue mainly cause those chargeback requests. The below chart indicates that the number of transaction and amount of chargeback with their type which was appear in the selected three banks in Ethiopia.

Table 4.2: Charge back amount and number of transaction

Common reason	Amount	Transaction No.
Authorization issues	15,602,624.64	53
Fraud	10,779,995.21	115
Processing errors	1,134,736.33	151
Customer disputes	851,052.25	90
Total	28,368,408.43	409

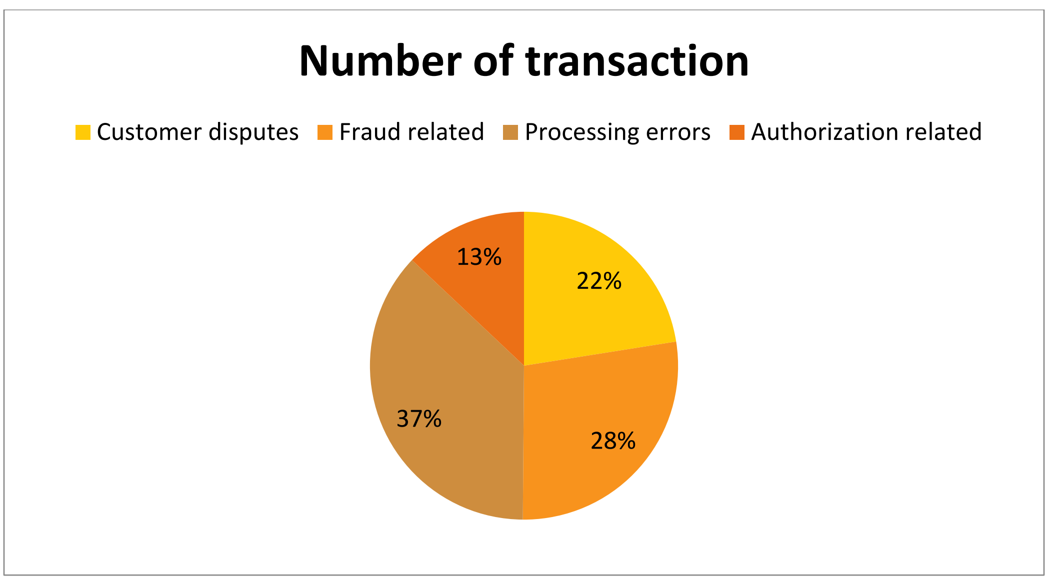

Figure 4.2: Charge back number of transaction

The lion share of both number of transaction and amounts are goes to fraud related chargeback. As per the data presented above, fraud related chargeback results 38% of the total chargeback amount and 28% of the total number of transaction. (Figure 4.2)

These happen due to fraud card present environment and fraud card absent environment. However, as per visa international and MasterCard, fraud related chargeback usually occurs due to when a customer did not swipe the card through a magnetic-stripe reader or insert EMV, i.e. Manual card/card absent transaction.

Even though it has huge risks and banks have lose a lot as stated above, still the selected banks in Ethiopia provides this service for merchants with a binding contract considering some eligibility criteria, the criterions set includes; Merchants' business type, only Hotels, supermarkets and duty free shops are qualified business types to be granted for manual card transaction.

On the other hand, from the documents reviewed (table 4.3), there are five significant amount cases at the hand of the legal offices of the selected three banks since 2018 regarding fraudulent POS transactions; four of them are ongoing while one is closed case, the winner of the closed case is the bank. This is because of the contract binds the merchant to take full responsibility over the fraudulent transaction.

Table 4.3: Court case status and amount

Case	Status	Amount
Case 1	Closed	1,329,807.59
Case 2	Ongoing	277,812.08
Case 3	Ongoing	84,600.00
Case 4	Ongoing	958,638.30
Case 5	Ongoing	120,847.66
Total		**2,771,705.63**

Therefore, the claim of these eight participants is the running of the e-banking business with help of contracts as a means of fraud prevention as explained above.

Seven participants (Table 4.4) believed the use of standard card production enabled banks' to improve their card banking fraud prevention. For example, according to P4" PCI-DSS (Payment card Industry Data Security Standard) is one of the best standard to comply in the e-banking industry. So, compliance with physical card production process requirement is our key method to prevent fraud"

According to the documents analyzed, from the card types, Mag stripe cards is the old technology, so can be easily copied. Frauds like card skimming that significantly affect banks in Ethiopia has happened because of Mag stripe cards are in use. The amount of money lost because of card skimming fraud is more than ETB 500,000 and it affects 52 customers only from one of those selected banks. Even though some banks have quit or minimally use mag stripe cards in parallel with smart cards, but the selected banks in Ethiopia are now moved to the smart cards technology with a standard production mechanism, which is latest and more secured than mag stripe cards.

The claim of nine participants, 75% of the total participants is about awareness creation as a method of preventing frauds in e-banking industry. About this method the participants elaborated from multiple stakeholders perspective in the e-banking business i.e. bank, merchant and customers. For example, P11 stated, "Merchants awareness creation sessions were fruitful in increasing successful transaction rate of the bank"

As per the document review on the banks' assessment report about their merchants' awareness level before the trainings they deliver, merchants didn't perform proper customer and card identification for POS transactions. They didn’t hold their POS password properly, and didn’t know what types of functionality their POS has and some merchants even didn’t know how to operate transaction on their POS. Moreover, because of this gap, they were vulnerable for phishing or social engineering types of frauds; for example, a single fraud makes one merchant to lost ETB 200,000.

P5 Explained, “We use different card holder education methods like initial awareness, card security training and ongoing education, these help customers to use our services and also to be protected from fraud”. Therefore, participants perceive awareness creation on cardholders, as it let customers to be protected from fraud and it is an enhanced means of fraud management in e-banking business.

Six participants (Table 4.4) that comprises 50% of the total participants have perceived as secured pin generation is one means of fraud prevention in improved fraud management strategy for e-banking industry.

P4, for example, stated, “The pin mailer is fully sealed by the machine and it is accessible for customers only, this makes our customers to feel safe and it is also a means of fraud protection”. Even though payment cards are lost, unless the PIN is all-together, customers are still safe. For that, as elaborated by P4, there is one day gap between card delivery and pin delivery to the branches and will be in custody by different personnel. Finally, the card and pin come together only on the hands of customers.

P2 explained another experience in the card and pin delivery system to branches. I.e. the card and pin delivered to branches all together but it will be activated only when it is delivered to the customer. Therefore, even though card and pin are put together, since the card is not activated, no fraud can be perpetrated.

Table 4.4: Frequency distribution of fraud Prevention Strategy

Prevention Strategies	**Total Number of Response**	**% of participants**
Legislation, Policy and guidelines	*12*	*100* %
Merchant Contracts	*8*	*67* %
Standard card production	*7*	*58* %
Awareness creation	*9*	*75* %
Secured pin generation	*6*	*50* %

Theme 2: Detection

The second strategic pillar, having a detection mechanism is at the core of the bank's e-banking fraud management strategy. Detection is referred the recognition of transactional risk information to identify fraud trends and patterns. A thematic analysis of the participants' answers to interview questions 1, 2, 3 and 6 showed as detection is a key strategic resources to manage e-banking fraud (Table 4.5).

Table 4.5: Fraud Detection *(Interview Question 1, 2, 3 and 6)*

Participants' answers to interview question #1, #2, #3 and #6	**Interpretation and analysis**	**Emergent themes**
P9 …one of the means of addressing fraud by our bank is timely identification of the	Customer and merchants report is a means of	Contact center to detect fraud and improve e-

fraud…frauds like card skimming are reported by customers …through our short code phone number… P2 … if customers card is stolen then there is no way to know unless they informs us through our contact center … P12… our merchants know our lines, so when Card Not Present transaction occurs to them they will call us…	detecting fraud by which they regain their confidence	banking fraud management
P10…in collaboration with INSA we have built standard security operation center (SOC) … using Tivoli which is system monitoring application/software made by IBM P11…cyber-attacks are detected by the latest technology we have deployed…	Monitoring systems are a means of detecting frauds by which the safety of entire systems and customers' transaction is identified	Technology/software to detect fraud and improve e-banking fraud management
P10…in collaboration with INSA we have built standard security operation center (SOC) by which we monitor our systems 24 hours, … P12… there is a department called IS Operation, this department is fully engaged in monitoring the health status of	The monitoring team is the one that usually detect frauds and escalate before it significantly affect	Transaction monitoring to detect fraud and its assistance in e-banking fraud management

customer transactions… P12… since we monitor transactions regularly, some frauds like denial of service (DOS) are addressed even before our customers recognize it…		
P3… trainings by the international schemas like VISA lets us to know recent frauds occurred internationally … P12 ...usually memorandums issued by Interpol discloses the very recent types of fraud	Other countries experience helps to understand the patterns of fraud and ease the fraud detection	Industry experience to detect fraud and its assistance in e-banking fraud management

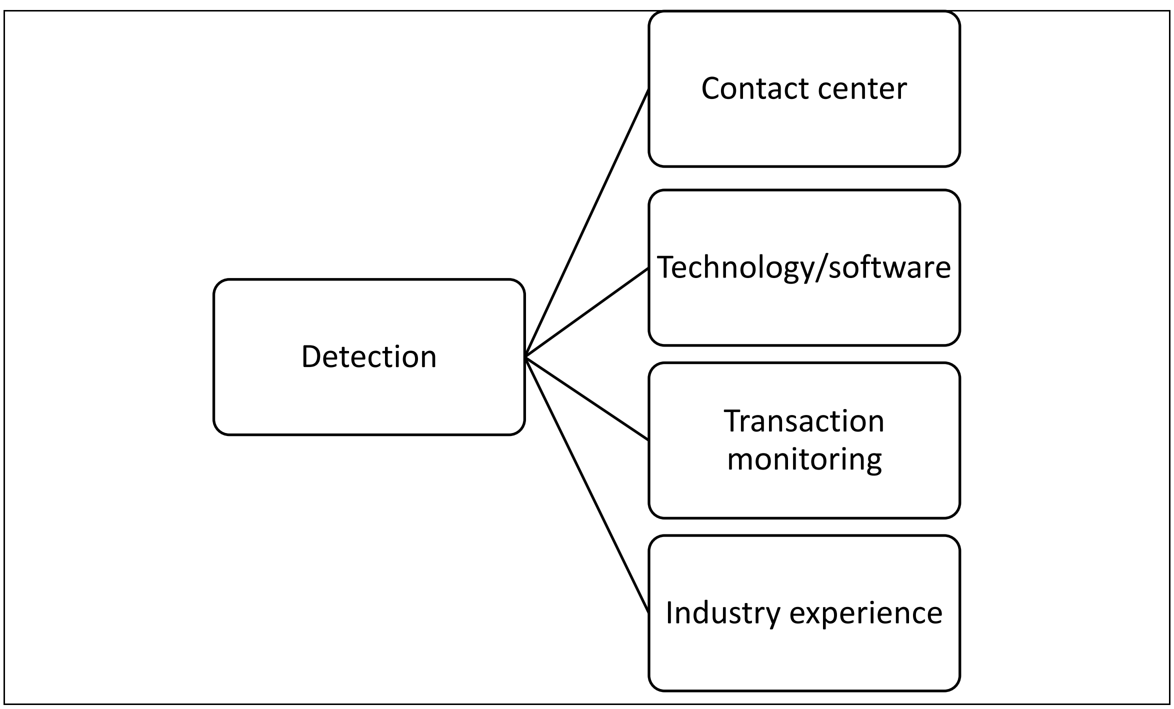

Figure 4.3: Word clustering on fraud Detection

Ninety two percent of the participants, i.e. 11 out of 12 agreed as most of the fraud types are detected through their contact centers they made available for customers (table 4.6). Even some types of frauds in e banking cannot be detected by banks without having contact center. P2, for example, stated, “If customers card is stolen then there is no way to know unless they informs us through our contact center”

Moreover, it stated by P9 as “frauds like card skimming are reported by customers, through our short code phone number”. As explained before from the document review, fraud perpetrated by card-skimming device affects 52 customers only from one of those selected banks. So, this fraud is detected by banks through their contact center following the calls from affected customers.

The deployment of the latest technology products or software applications is perceived by 83% of the participants as a means of fraud detection for improved fraud management in e banking. For example, P11 stated, ”Cyber-attacks are detected by the latest technology we have deployed”

From the document review, because of ransomware virus attack 70 branches and 201 ATMs have stop service for various range of days, until two weeks maximum. As explained by P11, in order to take action the first part, detection or identification of such kinds of frauds is made by the latest technology products.

Ninety two % of the participants perceived as in addition to technologies deployed, uninterrupted monitoring of systems is a significant part of fraud detection. P10, for example, stated, “in collaboration with INSA we have built standard security operation center (SOC) by which we monitor our systems 24 hours”. Furthermore, P12 explained, “Since we monitor transactions regularly, some frauds like denial of service (DOS) are addressed even before our customers recognize it”

The other fraud detection strategy used for e-banking fraud management is the sharing of an international industry practices. P3, for example, stated, “Trainings by the international schemas like VISA lets us to know recent frauds occurred internationally”. This perceived by eight participants comprising 67% of the total participants.

As per the document review on the correspondence letters and electronic messages from the Interpol and international payment schema respectively, all recent and new fraud types are shared for those banks so that they can easily detect it. P12, for example, stated, “Usually memorandums issued by Interpol discloses the very recent types of frauds”.

Table 4.6: Frequency distribution of fraud Detection Strategy

Detection Strategies	**Total Number of Response**	**% of participants**
Contact Center	*11*	*92%*
Technology	*10*	*83%*
Transaction Monitoring	*11*	*92%*
Industry Experience	*8*	*67%*

Theme 3: Resolution

The third strategic theme for the improvement of e-banking fraud management is resolution. Resolution is referred the support, services and tools to assist with resolving all or major fraud cases swiftly. A thematic analysis of the participants’ answers to interview questions 2, 3, 5, 7 and 8 showed as resolution is a key strategic resources to manage e-banking fraud (Table 4.7).

Table 4.7: Fraud Resolution *(Interview Question 2, 3, 5, 7 and 8)*

Participants' answers to interview question #2, #3, #5, #7 and #8	**Interpretation and analysis**	**Emergent themes**
P8… ICAM is a monitoring tool that capture Image of customers while they perform transaction on ATM…those images are used by police … P3….police officers uses transaction logs on the central systems interpreted by system administrators…..	Monitoring systems are source of evidence to give a solution to some fraud…	Tools for fraud resolution in e-banking fraud management
P8… software companies usually gives us an update and patches regularly… P3… international card schemas provides an advisory service about resolving fraud…P7… Ethiopian government through its police officers provides a service to resolve fraud incidents on customers	Different Services by different organizations as means of resolving frauds after its occurrence	Different organizations services for fraud resolution in e-banking fraud management
P10…INSA provides us information security advices to resolve some fraud types P9…our 24/7 contact center provides support to customers in handling any e-banking related fraud perpetrated on them…	Support as means of resolving frauds after its occurrence	Support for fraud resolution and e-banking fraud management

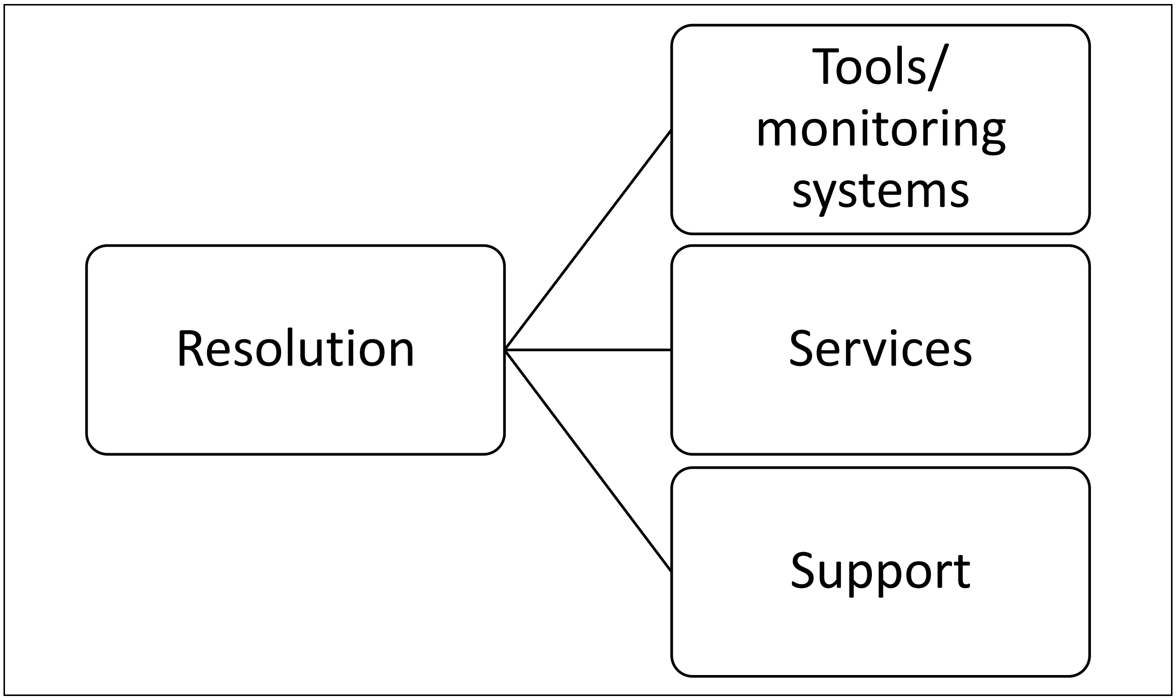

Figure 4.4: Word clustering on fraud resolution

All participants of the interview, 100%, perceived as most of the cases are resolved in collaboration with police offices for that the output of some tools in use are basic for the resolution of the case (table). One of the result of the tools is photo or image evidence that are captured at the time of transaction on ATMs.

P8, for example, stated, "ICAM is a monitoring tool that capture Image of customers while they perform transaction on ATM and those images are used by police" in addition to the images there are other evidences necessary to resolve the case by police, for example, P3 stated, "police officers uses transaction logs on the central systems interpreted by system administrators"

From the documents reviewed, the correspondence letters between branch and head offices, and between different banks, frauds that end up on ATM, like stealing of card and pin then withdraw money from the ATM, fraud by employees who withdraw money from the ATM by customers' card etc. are resolved with the help of cameras on the ATM.

On the other hand, nine participants that comprises 75% of the total participants perceived as services provided by different organizations and business partners as one of the fraud resolution strategy. P8, for example, stated, “software companies usually gives us an update and patches regularly”

According to the documents reviewed, a type of fraud happened on one of the three selected banks. i.e. fraudsters that know the vulnerability of ATMs with special functionality of exchanging foreign country currencies, requests the ATM to pay odd amounts, then since the ATM was not get fixed to handle such kind of strange requests, it pays the approximate amount of money and lets the customer account to be reversed as if the transaction is not successful. So, based on the software service agreement, this fraud is resolved by applying the latest fix to the ATM obtained from the service provider.

Forty two percent of the participants have claimed, as support by other organizations is one means of fraud resolution strategy. P10, for example, stated, “INSA provides us information security advices to resolve some fraud types”; the other participants also claims as support that banks providing for their customers as another means of fraud resolution. P9, for example, stated, “our 24/7 contact center provides support to customers in handling any e-banking related fraud perpetrated on them”

Table 4.8: Frequency distribution of fraud Resolution Strategy

Resolution Strategies	**Total Number of Response**	**% of participants**
Tools/ monitoring systems	*12*	*100%*
Services	*9*	*75%*
Support	*5*	*42%*

CHAPTER FIVE

FINDINGS SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Summary of key Findings

In this section of the chapter, the basic findings obtained by using the semi-structured interview and document review from the selected three banks are described. The key findings are presented from data analysis and findings section in chapter four.

5.1.1 Nature of e-banking frauds and the reasons behind

1. **Fraud and Payment Card types**

Some banks are not using the latest technology that help to manage frauds on some of their services. For instance, the researcher has found that, frauds like card skimming that significantly affect banks in Ethiopia has happened because of Mag stripe cards are in use. Mag stripe cards is the old technology that can be easily copied and insecure. However, still banks in Ethiopia are using this card type alone or in parallel with the smart card technologies.

2. **Fraud and POS Transaction types**

The researcher have found that, banks are taking fraud risks to run their business by deploying the fraud management strategies. Manual card transaction is the one that create a great opportunity for fraudsters. Though it has huge risks and banks have lose a lot, still banks in Ethiopia provides this service for merchants with some eligibility criteria., the criterions set includes; Merchants' business type like Hotels, supermarkets and duty free shops that are assumed to be qualified business types to be granted for manual transaction.

3. Fraud and awareness level or skill gap

Whatever the type of technology banks are using, unless the required knowledge to lead, administer and use the technology is available, its adverse impacts will be high. The researcher has found the below findings with respect to each stakeholders of the e-banking services.

Because of the skill gap, the following are findings from the bank, merchants and customers perspective:

- ❖ Some banks do not compile and assess the level of fraud appeared in their bank at corporate level, that was necessary to assess their preparedness level
- ❖ Some banks do not apply fraud control mechanisms like physical security for ATMs and surveillance camera because of this, for instance, one of the three banks have lost ETB 300,000 to ETB 400,000 because of damaged ATM due to fraud.
- ❖ Merchants are vulnerable for phishing or social engineering because of this, for example, one merchant has lost ETB 200,000
- ❖ Some customers still do not hold their payment card and pins securely; participants mention the number of customers affected and the amount of money lost due to this fraud as significant.

4. Fraud and ATMs hardware and software status

The respondents described, as a strategy, the technologies in use should be latest and up to date in order to improve the fraud management. Therefore, ATM hardware and software is also expected to be the latest and up to dated. However, from the document review, the following are findings in this regard:

- ❖ Even though the world has moved to Windows 10, all selected banks software is running on Windows 7 operating system
- ❖ Some ATMs do not have camera that capture images during transaction
- ❖ Some ATMs do not have anti-skimming device on the card reader that is necessary to protect card skimming fraud
- ❖ Forex ATMs software was not patched, because of this money is stolen

5.1.2 E-banking fraud management strategies and its effectiveness

- ❖ According to the participants response, even though the procedures and way of practice is different, all selected banks are using a similar types of e-banking fraud management strategies
- ❖ Prevention, Detection and Resolution are found to be the key strategic pillars used by the selected banks for improved e-banking fraud management
- ❖ By using merchant contracts, legislation, policy and guidelines with technology results of standard card production and secured pin generation,

the selected banks are trying to insure the implementation of the first strategic theme, prevention. Moreover, awareness creation is also a means of e-banking fraud prevention used by the banks.

- ❖ The second strategic pillar, detection, used by the selected banks to improve e-banking fraud management is being implemented using the banks contact center, technology products, industry experience and transaction monitoring. In this regard, the researcher has found that most of the fraud types to be detected by contact center with customers call.
- ❖ Resolution, the third strategic pillar, is in practice by the selected three banks by using tools/monitoring systems, services and supports of various stakeholders like police. But, there is no formal session for knowledge and experience sharing between police offices and banks, except data exchange after the fraud has happened
- ❖ All reports in relation to frauds are very specific and incident oriented, there is no corporate level aggregate report that in compasses all fraud types managed by different departments.
- ❖ Some of the e-banking fraud management strategies, like detection strategies, are effectively implemented by the selected banks, for example, frauds are detected or identified by one or other detection strategies effectively.
- ❖ On the other hand, some of the fraud types currently occurring on Ethiopian banks and customers are frauds happened on the first world country a long time before like for example loss of card and PIN together. On the other

hand, some of the fraud types described in the analysis section are actually happening even after the implementation of the described strategies. This entails the effectiveness of some of the fraud management strategies in use are still on the developing stage.

- From the document analysis, as stated on section 5.1.1, some of the strategies mentioned by the respondents are not actually put in practice. As a result, some of the fraud management strategies implementation has a long way to go or it is ineffective.

5.2 Conclusions

E banking services can be delivered through different channels that banks are currently using, for example Core-Banking (Branch), ATM, POS, Mobile (Mobile banking, Mobile money) and Internet (Internet banking, E-commerce).

According to the analysis of the study, there are different types of frauds that happened in various forms and magnitude on e-banking services. According to the findings summarized above, different types of fraud have happened on banks in Ethiopia. Fraud on card banking is more frequent than the other types of frauds happened on mobile banking, mobile wallet, internet banking and e-commerce platform. But, from the international practices, cost of fraud aligns with the iceberg concept, even though the occurrence of one fraud type is more frequent than the others but the reputation and other consequences of fraud might be bigger on the less frequent fraud types.

As a result banks have implemented various strategies in managing e-banking related frauds. Those various strategies fall in to three pillars called prevention, detection and resolution. In this regard, the selected three banks are using similar strategies even though the detail of its implementation is different from one bank to the other bank.

Some of the fraud types described in the analysis section are actually happening even after the implementation of the described strategies. These shows as the effectiveness of the strategies in use are still needs improvement.

5.3 Recommendations

Based on the findings and conclusions made above in this study, the researcher identifies and proposes the following recommendations for banks to have an improved fraud management.

- As part of fraud management strategies, banks in Ethiopia have to acquire and implement the latest and more secured card types like EMV chip and contactless cards.

- Banks shall improve the merchant recruitment criteria for manual card entry types of service on one hand and provide all the necessary training to merchants about how to identify genuine customers on the other hand.

- In order to fill bankers awareness gaps, providing the necessary and up to date training, experience sharing between the senior and junior staffs, participating on webinars to share international practices are very necessary for all banks. Moreover, banks should work more on customers' awareness creation strategy, tailoring the training type they give to the status of their customers.

- Banks in Ethiopia should have an agreement with vendors and software providers in such a way that regular latest updates can be easily acquired and applied before significant damage happens.

- Realizing once gap and vulnerability assessment helps to put mitigation plans in to practice, so banks are supposed to scan their system consistently, identify the gap and fill with appropriate strategies.

- To get insight and make correct strategies at organization level on the fraud management system, banks should arrange fraud related data, documents and reports to be holistic and centralized.

- Ethiopian banks should reconcile their status and readiness towards fraud both by learning from other countries earlier experiences and should come up with the 21^{st} century technologies to overcome both out dated and new fraud types.

- It is suggested the strategies that are not yet well implemented to be put in practice by the banks as earlier as possible

- The strategies that are actually implemented for fraud management shall be attentively monitored and regularly updated by the banks.

REFERENCES

Abdulrahim, R. E., & Abdulrahman, A. (2013). Applicability of resource-based environmental studies in green IT. *Journal of Systems and Information Technology, 15*, 269–286. Retrieved from https://doi:10.1108/JSIT-02-2013-0003

Abiy Woretaw and Lemma Lessa (2012). Information security culture in the banking sector in Ethiopia. Retrieved from https://docplayer.net/12528591-Information-security-culture-in-the-banking-sector-in-ethiopia.html

Accenture Analytics Innovation Center (2015*), protecting the Customer: Fighting Bank Fraud in a New Environment*, *1-9. Retrieved from* https://www.accenture.com

ACL Services Limited. ―Fraud Detection using Data Analytics in the Banking Industry. Discussion paper, 1-8. *Retrieved from* *https://www.acl.com/bankingfraud*

Aliyu, A. A., Rosmain, T., & Takala, J. (2014). Online banking and customer service delivery in Malaysia: Data screening and preliminary findings. *Procedia – Social and Behavioral Sciences, 129*, 562–570. *Retrieved from* *https://*doi:10.1016/j.sbspro.2014.03.714

Allan Maina Gakuru (2016). Card Fraud detection techniques on performance of commercial banks in Nairobi, Kenya. *Retrieved from* https://ir-library.ku.ac.ke/bitstream/handle/123456789/19086/Card%20Fraud%20Detection%20.pdf?sequence=1&isAllowed=y

An International Multi-Disciplinary Journal, Ethiopia Vol. 4 (3b) July, (2010). Fraud and Fraudulent Practices in Nigeria Banking Industry (Pp. 240-256). Retrieved from http://www.afrrev.com

Bambore, P. L. (2013). Customer satisfaction and electronic banking service on some selected banks of Ethiopia. *International Journal of Research in Computer Application & Management, 3*(6). Retrieved from http://ijrcm.org.in/comapp/

Baptista, G., & Oliveira, T. (2015). Understanding mobile banking: The unified theory of acceptance and use of technology combined with cultural moderators. *Computers in Human Behavior*, *50*, 418–430. *Retrieved from* *https://*doi:10.1016/j.chb.2015.04.024

Behabtu Amare (2015), Assessment of Insider Threat in Ethiopian Banking Industry, *Retrieved from* http://etd.aau.edu.et

Bhatt, G. D., & Grover, V. (2005). Types of information technology capabilities and their role in competitive advantage: An empirical study. *Journal of Management Information Systems*, *22*, 253–277. *Retrieved from* *https://*doi:10.1016/j.protcy.2014.10.019

Boddy, C. R. (2016). Sample size for qualitative research. Qualitative Market Research: *An International Journal*, *19*, 426–432. Retrieved from https://doi.org/10.1108/QMR-06-2016-0053

Cards & Mobile payments industry intelligence (2015). Card Fraud Report 2015. Retrieved from https://www.paymentscardsandmobile.com/wp-content/uploads/2015/03/PCM_Alaric_Fraud-Report_2015-1.pdf

Carr, N. G. (2003). IT doesn't matter. Retrieved from https://hbr.org/

Chen, B., Zhang, T., Bond, T., & Gan, Y. (2015). Development of a quantitative structure-activity relationship (QSAR) model for disinfection byproduct (DBP) research: A review of methods and resources. *Journal of Hazardous Materials*, 299, 260–279. Retrieved from https://doi.org/10.1016/j.jhazmat.2015.06.054

Chi, J. Y., & Sun, L. (2015). IT and competitive advantage: A study from a micro perspective. *Modern economy*, *6*, 404-410. *Retrieved from* *https://*doi:10.4236/me.2015.63038

Cibangu, S. K., & Hepworth, M. (2016). The uses of phenomenology and phenomenography: A critical review. Library & Information Science Research, vol 38, 148–160. Retrieved from https://doi.org/10.1016/j.lisr.2016.05.001

CIMA (2008). Fraud risk management - A guide to good practice. *Retrieved from* https://www.cimaglobal.com/Documents/ImportedDocuments/cid_techguide_fraud_risk_management_feb09.pdf.pdf

Comi, A., Bischof, N., & J. Eppler, M. (2014). Beyond projection: Using collaborative Visualization to conduct qualitative interviews. *Qualitative Research in Organizations and Management: An International Journal*, *9*, 110–133. Retrieved from https://doi.org/10.1108/QROM-05-2012-1074

Dauda, S. Y., & Lee, J. (2015). Technology adoption: A conjoint analysis of consumers′ preference on future online banking services. *Information Systems*, *53*, 1–15. *Retrieved from* https://doi:10.1016/j.is.2015.04.006

Denzin, N. K. (1970). The research act: A theoretical introduction to sociological methods. New York: Aldine.

Doherty, N. F. & Terry, M. (2013). Improving competitive positioning through complementary organizational resources. *Industrial Management & Data Systems*, *113*, 697–711. *Retrieved from* *https://*doi:10.1108/02635571311324151

Dzomira, S. (2014), Electronic Fraud Risk in the Banking industry, Zimbabwe, Risk, Governance & Control: Financial Markets & Institutions, 4(2), 17-27. *Retrieved from* *https://www.irss.academyirmbr.com*

Evalyne Wayua Ngui (2018), Effect of Financial fraud management practices on profitability of state corporations in Kenya. *Retrieved from* http://erepository.uonbi.ac.ke/bitstream/handle/11295/105164/Ngui_Effect%20of%20Financial%20Fraud%20Management%20Practices%20on%20Profitability%20of%20State%20Corporations%20in%20Kenya.pdf?sequence=1&isAllowed=y

Fereday, J. & Muir-Cochrane, E. (2006). Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. International Journal of Qualitative Methods, 5(1), 80–92. *Retrieved from* http://www.ualberta.ca/~iiqm/backissues/5_1/pdf/fereday.pdf.

Ford, N. (2012). The essential guide to using the web for research how to do a literature review. *Sage Publications Ltd*. *Retrieved from* *https://*doi:10.4135/9781446287927

Frels, R. K., & Onwuegbuzie, A. J. (2013). Administering quantitative instruments with qualitative interviews: A mixed research approach. *Journal of Counseling & Development*, *91*, 184–194. *Retrieved from* https://doi.org/10.1002/j.1556-6676.2013.00085.x

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *Qualitative Research*, *8*, 137-152. *Retrieved from* https://doi:10.1177/1468794107085301

GSM Association (2014). State of the industry mobile financial services for the unbanked. *Retrieved from* https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2015/03/SOTIR_2014.pdf

Haag and Cummings (2008). Management information systems for the information age (7edi). 1221 Avenue of the Americans, NY: McGraw-Hill Companies, Inc Thousand Oaks, CA: Sage.

Halefom Hailu, (2015). The state of cybercrime governance in Ethiopia https://www.researchgate.net/publication/319644987_THE_STATE_OF_CYBERCRIME_GOVERNANCE_IN_ETHIOPIA_-_MAY_2015_THE_STATE_OF_CYBERCRIME_GOVERNANCE_IN_ETHIOPIA

IMF (2013). The Federal Democratic Republic of Ethiopia. *Retrieved from* https://www.imf.org/external/pubs/ft/scr/2013/cr13309.pdf

Jeff Sauro (2015). Five types of qualitative methods. *Retrieved from* https://www.measuringu.com/qual-methods

Kassahun Girma (2016), Challenges and Opportunities of Electronic Banking in Ethiopian Banking Industry, retrieved from http://etd.aau.edu.et

Leedy, P. D., & Ormrod, J. E. (2015). *Practical research: Planning and design*. New York, NY: Pearson Education, Inc.

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health Promotion Practice*, *16*, 473–475. Retrieved from https://doi.org/10.1177/1524839915580941

Liébana-Cabanillas, F., Munoz-Leiva, F., & Rejón-Guardia, F. (2013). The determinants of satisfaction with e-banking. *Industrial Management & Data Systems, 113*, 750-767. *Retrieved from* *https://*doi:10.1108/02635571311324188

Madan Bhasin, 2016. Role of Technology in Combatting Bank Frauds: Perspectives and Prospects. Universiti Utara Malaysia, 22-23. Retrieved from *https://www.researchgate.net/publication/293826828* *and* *https://www.irss.academyirmbr.com*

Marshall, C., & Rossman, G. B. (2014). *Designing qualitative research*. Thousand Oaks, CA: Sage Publications.

MasterCard Academy (2018). Principles of fraud management for issuers and acquirers.

Mishra, V., & SinghBisht, S. (2013). Mobile banking in a developing economy: A customer-centric model for policy formulation. Telecommunications Policy, 37,503–514. *Retrieved from* *https://*doi:10.1016/j.telpol.2012.10.004

National Bank of Ethiopia (2018). Annual report. Retrieved from http://www.nbe.gov.et/publications/annualreport.html

National Bank of Ethiopia (2015). Annual report. Retrieved from http://www.nbe.gov.et/publications/annualreport.html and

http://www.nbe.gov.et/pdf/annualbulletin/Annual%20Report%202014-2015/Annual%20Report%202014-15.pdf

Nguyen, T. Q. T. (2015). Conducting semi-structured interviews with the Vietnamese. *Qualitative Research Journal*, *15*(1), 35–46. Retrieved from https://doi.org/10.1108/QRJ-04-2014-0012

Panda, D., & Reddy, S. (2016). Resource-based view of internationalization: Evidence from Indian commercial banks. *Journal of Asia Business Studies*, *10*, 41–60. *Retrieved from https://*doi:10.1108/JABS-10-2014-0082

Patton, M. Q. (1990). Qualitative evaluation and research methods (2nd ed.). Newbury Park, CA: Sage.

Porter, M. E. (1985). *Competitive advantage: Creating and sustaining superior performance*. New York, NY: Free Press.

PwC (2014), Global Economic Crime Survey 2014. *Retrieved from* http://www.pwc.org.

Robinson, O. C. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. *Qualitative Research in Psychology, 11*, 25-41. Retrieved from https://doi.org/10.1080/14780887.2013.801543

Runfola, A., Perna, A., Baraldi, E., & Gregori, G. L. (2016). The use of qualitative case studies in top business and management journals: A quantitative analysis of recent patterns. *European Management Journal*. *35*(1), 116-127. Retrieved from https://doi.org/10.1016/j.emj.2016.04.001

Sikdar, P., Kumar, A., & Makkad, M. (2015). Online banking adoption: A factor validation and satisfaction causation study in the context of Indian banking customers. International Journal of Bank Marketing, 33, 760–785. *Retrieved from* https://doi:10.1108/IJBM-11-2014-0161

Simpson, A., Slutskaya, N., Hughes, J., & Simpson, R. (2014). The use of ethnography to explore meanings that refuse collectors attach to their work. *Qualitative Research in Organizations and Management*, *9*, 200–183. Retrieved from https://doi.org/10.1108/QROM-01-2013-1133.

Teklebrhan Woldearegay Gebreslassie, E-Business Strategy to Adopt Electronic Banking Services in Ethiopia (Walden University, 2017). Retrieved from https://pdfs.semanticscholar.org/5d1c/f55a0444c715c51908289f68c9cce997d9c3.pdf

Tsegaye Nire (2017), Constructing a predictive model for Real-Time ATM CARD Fraud Detection. *Retrieved from* http://etd.aau.edu.et

Verizon. (2013).Data Breach Investigations Report. Retrieved from http://www.vormetric.com/InsiderThreat

VISA (2015). Chargeback Management Guidelines for Visa Merchants. Retrieved from https://studylib.net/doc/18571147/chargeback-management-guidlines-for-visa-merchants

Walker, R., & Solvason, C. (2014). Success with your early year's research project. *SAGE Publications Ltd*. *Retrieved from https://*doi:10.4135/9781473913875

Wang, Y., Bhanugopan, R., & Lockhart, P. (2015). Examining the quantitative determinants of organizational performance: Evidence from China. *Measuring Business Excellence*, *19*, 23–41. Retrieved from https://doi.org/10.1108/MBE-05-2014-0014

World Bank (2013). Banking in Africa. Retrieved from http://econ.worldbank.org.

Xu, D., Huo, B., & Sun, L. (2014). Relationships between intra-organizational resources, supply chain integration, and business performance: An extended resource-based view. *Industrial Management & Data Systems*, *114*, 1186–1206.*Retrieved from https://*doi:10.1108/IMDS-05-2014-0156

Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences. *European Journal of Education*, *48*, 311–325. Retrieved from https://doi.org/10.1111/ejed.

Yin, R. K. (2014). *Case study research design and methods* (5th Ed.). Thousand Oaks, CA: Sage Publications, Inc.

Zahir Irani, P., Basias, N., Themistocleous, M., & Morabito, V. (2013). SOA adoption in e-banking. *Journal of Enterprise Information Management*, *26*, 719-739. Retrieved from https://doi.org/10.1108/JEIM-07-2013-0042

Zhong, J., & Nieminen, M. (2015). Resource-based co-innovation through platform ecosystem: Experiences of mobile payment innovation in China. *Journal of Strategy and Management*, *8*, 283–298. *Retrieved from* https://doi:10.1108/JSMA-03-2015-0026

APPENDIX A

Addis Ababa University

Faculty of Business and Economics

Department of Management

Interview Questionnaire: To be answered by directors and managers at the selected banks internal control and e-banking departments

The following interview questions are designed to collect information about e banking fraud and fraud management strategies in Ethiopian banks. The information shall be used as primary data in my research that I am conducting as a partial requirement of my study at Addis Ababa University for completing my MSc in Management under faculty of Business and Economics. The research is to be evaluated in terms of its contribution for assessing fraud that exist or occurred on banks in Ethiopia in relation to e banking services and the strategies of managing those frauds. Therefore, your genuine, honest, and prompt response is a valuable input for the quality of and successful completion of the research. Since the tangible and concrete outcome of this research will be present in such a way that it will be used by banks in Ethiopia and National bank of Ethiopia as a source of practice for a minimal fraud related risks in complement with their own initiation and strategic direction. Therefore, I will be willing to submit a copy of my final report to you if desired when it is ready.

List of interview questions:

1. How do you know when fraud occurs on your bank in relation to e banking services?
2. What are the mechanisms you use to improve the safety or security of your e banking services?
3. What are the key features of your safety measures on fraud management?

4. What barriers you encountered while implementing the fraud management mechanisms for the e banking services?
5. How do you address those barriers after implementing the strategy to control frauds?
6. How do you rate the usefulness of your fraud management strategies?
7. What factors were critical in your success regarding the implementation of those strategies?
8. What other additional information would you like to add?

APPENDIX B

Note: For the sake of the selected three banks business reputation, copies of documents reviewed is not attached with annex. However, only for academic purpose, some copies are presented to confirm the reliability and validity of the data used in this thesis.