Addis Ababa University

College Of Law And Governance

School Of Law

Liability Of Banks And Their Officers In Ethiopia For Fraudulent Withdrawal Of Money By Third Parties

By:

Dinka Dereje Asefa

A Thesis Submitted In Partial Fulfillment For The Requirement Of Masters Of Degree In Business Law (LLM)

Advisor: Solomon Abay (Ph.D, Associate Professor Of Law)

May 2021

Addis Ababa, Ethiopia

Approval Sheet

Liability of Banks And Their Officers in Ethiopia for Fraudulent Withdrawal of Money

By: Dinka Dereje Asefa

Approved By Board of Examiners

----------	----------	----------
Advisor	**Signature**	**Date**
----------	----------	----------
Examiner	**Signature**	**Date**
----------	----------	----------
Examiner	**Signature**	**Date**

DECLARATION

A Thesis titled “Liability of Bank officers in Ethiopia for Fraudulent Withdrawal of Money by Third Party” is my original work and has not been submitted for an award of degree at any other University and all Materials Used in this research have been duly Acknowledged.

Declared by:

Dinka Dereje Asefa

Signature ----------

Date ----------

Confirmed by:

Solomon Abay (Ph.D, Associate Professor of Law)

Signature ----------

Date ----------

ACKNOWLEDGMENT

First and foremost, I would like to thank Almighty God for His endless help and eternal love throughout my life.

Next, I am heartily thankful to my advisor Dr. Solomon Abay (Associate professor) for his precious comments and guidance from the start of the paper to its end.

I also owe special thanks to all persons who have cooperated me especially my brother Dr. Fekadu Dereje who stood beside me in many aspects.

Finally, I owe incredible gratitude to my family for their persistent love, support and patience they showed me during busy time of my research work.

Thank you All!

LIST OF ABBREVIATIONS

ATM: **A**utomated **T**eller **M**achine

CATS: **C**ustomer **A**ccount and **T**ransaction **S**ervices

CBE: **C**ommercial **B**ank of **E**thiopia

CDD: **C**ustomer **D**ue **D**iligence

KYC: **K**now **Y**our **C**ustomer

KYE: **K**now **Y**our **E**mployee

NBE: **N**ational **B**ank of **E**thiopia

PIN: **P**ersonal **I**dentification **N**umber

OTP: One Time Password

UV: Ultra Violet

GSMA: Global System for Mobile Communications

TABLE OF CONTENTS

ABSTRACT

Banking frauds are the real challenges adversely affecting the trust between banks, their customers, and the national economy amid the seamless nature of banking technologies. The study is to analyze liability for fraudulent withdrawal of money by third parties in Ethiopian bank systems, employing a doctrinal research method through collecting primary and secondary data from different legal documents and cases that are purposely sampled for the analysis. The finding of the study indicated that Ethiopian banks system is becoming highly vulnerable to such frauds, and the problem is further exacerbated by poor data system, low understanding of the risk by the bank customers and loose standards governing the bank employees, banking technologies and infrastructure. Yet, absence of clearly stipulated laws on who should bear the liabilities sustained by such acts made preventive measures and the retribution less effective. As the result, the study recommends mass education for the bank customers on the types and extent of vulnerabilities to such bank frauds and strong and updated laws to solve disputes related to liability, and employing banking technologies with updated and multilayer security features.

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND OF THE STUDY

Financial institutions in general and banks in particular play significant roles in economic development. An improved financial system fosters the efficient mobilization of domestic savings and allocates resources to their optimum usage.[1] Levine pointed out that "the level of financial development is a good predictor of future rates of economic growth, capital formation and technological change or the lack thereof affects the speed and pattern of economic development.[2]

Bank is business entity that collects funds from the public in the form of savings and distributes it to the community in the form of credit in order to improve the living standard of people by providing credit facilities.[3] It mobilizes funds from, within and outside the country and channels such funds to various sectors of the economy.

Growing use of new payment channels increased access points and changed traditional paper-based payment system to e-payment system. Such growth of using contactless tap-and-go technology, the popularity gained to use such payment systems and the use of mobile to complete electronic payments increased the risk of payment frauds. Payment fraud is an activity that uses confidential information to obtain unlawful gain without the consent of the payer through activities such as counterfeiting, deception, altering payment instruments, hacking, and data interception. It is constantly evolving from day to day as criminals continued discovering new ways to thwart the efforts of financial institutions to protect transaction data. Fraudsters

---

[1] Admasu Bezabeh & Asayehegn Desta, 'Banking Sector Reform in Ethiopia', International Journal of Business & Commerce, vol 3, p 28

[2] Ibid p 29.

[3] Faisal Santiago, *Pengantar Hukum Bisnis*, Jakarta; Mitra Wacana Media (2012), p 43

employ different techniques to overcome new protection measures.[4] Such payment fraud includes Identity fraud, cheque fraud, phishing fraud, Automated Teller Machine (ATM) fraud, Fund transfer Letter fraud and E-banking fraud. It is the leading headache for financial institutions in general and for banks in particular that can happen at any point along the transaction processing chain.[5] Thus, the need for such innovation and the means of addressing the possible risks should be balanced and regulated.

Contractual relationship between banker and customer imposes an obligation of Know Your Customer (KYC) and Customer Due Diligence (CDD) on the banker to identify for whom the latter is giving service. KYC and CDD is an effort banks should make to identify for whom they are giving service by using reliable, independent source documents, data or information.

When payment fraud occurs, liability must be clearly assigned so that end-users of the payment system are made whole and their trust in the overall architecture and integrity of the system is maintained. [6] However, due to the faster change in technology, payment systems change faster than laws and regulations governing them. Therefore, tailored laws are required to protect the right of customers in banking sector and appropriate remedy should be stipulated by law in case such fraudulent acts are committed.

Therefore, the research tries to find out the liability of bank officers in case money is fraudulently withdrawn from account of others through payment frauds mentioned above. The researcher analyzes legal lacunas that impair courts and legal professionals from deciding who should be held liable and whether the existing laws address these issues. Besides, the study analyzes Ethiopian laws, if any, to determine the liability of banks and bank Officers. Furthermore, it also examines what the practice in the courts looks like.

---

[4] Sandeap Dhameja, Kat Jacob, and Richard D. Porter, *Clarifying Liability for Twenty First Century Payment Fraud*, (Federal Reserve Bank of Chicago 2013), P.109

[5] Ibid

[6] Ibid, P108

1.2 STATEMENT OF THE PROBLEM

The cassation division of the Federal Supreme court decided that bankers are liable to the customer who claimed refund of money withdrawn from their account fraudulently only where such money was withdrawn due to the failure by the bankers to follow the regular working procedures of banks or it was proved that the bank was defrauded. [7] In another case, it was decided that banks should refund the money fraudulently taken because it is bank that is defrauded and not the customer.[8] Thus, regarding fraudulently withdrawn money, similar cases are decided differently by the Cassation Division of the Federal Supreme Court, triggering the question which decision should lower courts follow to dispose similar cases that come before them. This dissimilarity of decisions on similar cases is mainly due to lack of clear law addressing the issue.

Therefore, the liability of banks and their officers in case money is withdrawn fraudulently, and the issue of the degree of care required from bank officers in discharging their duty requires proper analysis. Besides, the current increase in innovation of various payment systems necessitate the analysis of existing laws, if any, to infer whether they can sufficiently address payment frauds committed through daily changing technology.

1.3 RESEARCH QUESTIONS

Are bank and their officers liable in Ethiopia for fraudulent withdrawal of money by third parties through identity fraud, cheque fraud, ATM fraud, fund transfer letter fraud and E-payment frauds?

In order to answer the above main question, the following specific questions are considered;

[7] Commercial Bank of Ethiopia vs. Glory PLC [2010], Federal Supreme Court Cassation Division, [41535]

[8] W/o Nejiha Dewale vs. Awash International Bank, Federal Supreme Court cassation decision, [38289]

- Are the Ethiopian banks and their officers aware of their liabilities in fraudulent withdrawal of money by third parties?
- What are the legal practices in solving disputes related to fraudulent withdrawal of money by third parties in the Ethiopian banking system?

1.4 OBJECTIVES OF THE STUDY

The major objective of the study is to analyze the liability of bank and bank officers to customers whose deposit or transfer is withdrawn or transferred fraudulently by third parties through various payment frauds and examining how courts are dispensing facts brought before them.

The study has few specific sub- objectives. Therefore, the study is conducted:-

- To examine the liability of banks and bank officers to their customers in fraudulent withdrawal of money by third parties
- To analyze the legal provisions employed to settle disputes related to fraudulent withdrawal of money by third parties between banks and their customers
- To examine the measures to prevent fraudulent withdrawal of money by third parties?
- To examine the legal practices in courts to decide on fraudulent withdrawal of money by third parties

1.5 METHODOLOGY OF THE STUDY

The research is qualitative doctrinal research. It applies the analytical approach of what legislation related with the liability of bank and bank officers to their customers provide and how courts are applying such laws. The analysis focuses on legal regime dealing with liability of bank officers in case money deposits are withdrawn or transfer is made fraudulently through identity fraud, check fraud, fund transfer letter fraud, ATM or electronic payment fraud.

So, the primary sources of the research is commercial code, civil code, proclamations, regulations, directives, circulars and guidelines of National Bank of Ethiopia (NBE), and other relevant legislations of Ethiopia. The secondary sources include articles, text books, commentaries, cases and the like both from domestic and foreign sources. The researcher also conducted an interview with bank employees to assess how bank officers are generally discharging the obligation of KYC. Purposive selection method was employed to keep flexibility to get volunteers and the right person. Then legal analysis was conducted to examine the aptness of existing law with regard to liability of bank officers to their customers.

1.6 SIGNIFICANCE OF THE STUDY

The finding of this study enables customers to know the extent bank officers and bankers take liability when there is fraudulent withdrawal and the degree of care bank officers are supposed to take during the carry- out of its functions. In addition, it enables the legislature to see legal gaps in governing the issue in Ethiopia. This study will also be a foundation for further research by those who are interested in the subject matter. The research will enable the legislature to consider the changing nature of payment frauds from time to time and enact updated laws regulating them.

1.7 SCOPE OF THE STUDY

This study focuses on liability of bank officers in fraudulent withdrawal of money deposits through various payment frauds. Thus, to limit its scope, the research focuses only on civil liability of bank officers arising from money withdrawn from customers' account through fraudulent acts. It will not cover liabilities other than this.

1.8 LIMITATIONS OF THE STUDY

The challenges that the researcher encountered in the study are mainly inaccessibility of materials related with the subject matter in Ethiopia either as text books, journals or online

materials. As these problems were not given attention they deserve, the researcher encountered short of reading materials used in the literature review. Likewise, some of persons selected for interview were not available and voluntary at the time needed.

1.9 ORGANIZATION OF THE STUDY

The study consists of four chapters. The first chapter deals with introductory matters such as overview of the background of the study, statement of the problem, research questions, research objectives, methodology, scope, significance and limitations of the study. The second chapter deals with payment fraud in banks. Under this chapter, the type of payment frauds and the degree of customer due diligence in each type of payment frauds are reviewed. The third chapter addresses civil liability of banks and its officers in fraudulent withdrawal of money by third parties. Under this chapter, decisions of cassation division on cases brought before them are examined. Finally, the study ends with conclusion and forwarding recommendations.

CHAPTER TWO

PAYMENT FRAUD IN BANKS

2.1. OVERVIEW OF BANK FRAUD

History has shown us that as we invent new technologies, criminals are waiting on the periphery to use them …[9]

Financial institutions in general and banks in particular play a critical role in the emerging markets like Ethiopia. They are intermediaries between depositors and borrowers thereby promoting savings that later result in capital formation which is the basis for economic progress in the country and a way out from abysmal poverty.[10] In Ethiopia, banking has dominated the financial sector with approximately 80% of the total financial sector assets, while insurance and microfinance sector account for 10% each.[11]

Despite the significant role banks play in economic development, their failures have been well pronounced. The dictionary of economics and commerce confirmed that 200 banks failed in England between 1815 and 1850 in just a period of 35 years, and one of the reasons attributed to their failure is Fraud.[12] According to an International Multi-Disciplinary Journal, Bank of Credit and Commerce International (BCCI) globally lost $10 billion due to fraud and Japan's Fuji Bank suffered $3 billion loss due to forgery that happened in 1990.[13]

---

[9] Rajev Saxena,"Cyber Laundering the Next Step for Money Launderers?", St. Thomas Law Review, (1998) Vol.10, P.688

[10] According to annual report of NBE 2019/20 for instance, the amount of deposits mobilized by the banking sector reached 677.1 billion birr whereas, new loan of 271.2 billion birr was distributed. NBE annual report 2019/20, P.45

[11] Gebrehiwot Ageba and Derk Bienen, *Ethiopia's Accession to the WTO and the Financial Service Sector*, *Ethiopian Business Law Series*,(Faculty of Law 2008), A.A., Vol.2, P. 7

[12] Owolabi.S.A., "Fraud and Fraudulent Practices in Nigerian Banking Industry", (2010), Vol.4, An International Multi-Disciplinary Journal. Ethiopia, p.241

[13] Ibid, ,P. 242

The problem of fraud in banking industry is not limited to banks existing in a specific country. It is a general phenomenon that the banking industry all over the world faces in one way or another. Nwankwo explained bank fraud in the banking industry of Nigeria as:

> "The crises of confidence in Nigerian banking industry is not a new one, it has been with us for quite a long time. It occurred in the1930s when all indigenous banks, except one (National Bank), collapsed. It occurred again during the banking 'boom and crash' of the late 1940s when all but four indigenous banks escaped the liquidators hammer". Also between 1952 and 1954, 16 out of 21 indigenous banks failed. In the late 1990s, 26 failed banks were liquidated at once while others went through various surgical operations ranging from, restructuring, renaming, acquisition and complete sales to new investors. One thing that is constant in all the reforms was that fraud was a prominent factor in the major failures."[14]

Ethiopia is not an exception to bank fraud. CBE has lost more than $314,000 at its headquarter in December 2012 only due to bank fraud. In March 2016, $852,000 is transferred from customer account to fake account that was deliberately created. [15] Fraud generally takes place in a financial system when safeguards and procedural checks are inadequate or when they are not scrupulously adhered to, thus, leaving the system vulnerable to the perpetrators.

Currently the change of the traditional cash-based payment system to electronic payments has changed the mechanism the fraudsters use in the commission of their illegal acts. It enabled those fraudsters to discover new ways to thwart transaction and overcome protection measures of financial institutions by using better technology. 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.[16] Moreover, change in consumers' demography, the expansion of banks into new marketplace and the widespread use

---

[14] Ibid

[15] Bob Koigi (2016), https://africabusinesscommunities.com accessed on 18/4/2021

[16] Shewangu Dzomira, *Risk Governance and Control: Financial Market and Institutions*,(2014) available at https:/www.researchgate.net

of e-payment systems has heightened the vulnerability of banks to fraud. [17]This is mainly due to the opportunity created for fraudsters enabling them to use of increasing innovative and creative ways to manipulate any perceived weaknesses in banks. It is sometimes described as an endless game of cat and mouse between financial institutions and cyber-criminals. Therefore, fraud prevention measures need to constantly evolve to ensure handling the threat.

Banks provide their services by dealing with public money and their employees should exercise due care and diligence in handling the transactions in banks because the current rise in bank frauds calls for tightening of security mechanism. [18] Thus, in order to prevent fraud, there are obligations imposed by the directives of NBE on employees of bank. The failure of the employee to discharge these responsibilities will entail liability if money is withdrawn fraudulently from account of customers.

Therefore, in this chapter, the researcher addresses the various types of fraudulent acts, their causes, impacts and the obligations imposed by law on the employees to prevent or minimize fraudulent acts. However, before embarking on tackling the above-mentioned issues, the researcher defines what fraud is.

2.2. DEFINITION OF FRAUDS

According to NBE report (2014), "Fraud means an act or omission by shareholders, directors, employees and customers committed with the intention of gaining dishonest or unlawful advantage for the party committing fraud or for other parties".[19] "Fraud" is a generic term meant to describe an act of deliberate deception aiming at gaining some benefit without any legitimate right when safeguards and procedural checks are inadequate, or when they are not adhered to in financial systems. It encompasses act of dishonestly, illicit practices and illegal acts at any stage

[17] Ibid

[18]Ashu Khanna and Bindu Arrora, International Journal of Business Science and Applied Management, (2009), Vol.4 p.2

[19] Licensing and supervision of banking Business Fraud Monitoring Directive, directive no. SSB/59/2014,National Bank of Ethiopia, art. 2.5

of transaction processing chain involving intentional deception or misrepresentation including but not limited to misappropriation of the identity of another person, forging his signature without his knowledge or consent in order to gain an advantage he could not otherwise have gained through lawful or just means.

2.3. CAUSES OF FRAUD

"Trusted persons become trust violators when they conceive of themselves as having a financial problem which is non-shareable, are aware that this problem can be secretly resolved by violation of the position of financial trust, and are able to apply to their own conduct in that situation verbalizations which enable them to adjust their conceptions of themselves as trusted persons with their conceptions of themselves as users of the entrusted funds or property."[20] Cressey outlined three factors pushing a person to commit fraud.

The first factor is pressure on the employee due to "non-shareable" financial problems. Pressure includes factors that motivate employees to commit fraud. It develops from personal conditions to get money to satisfy financial problem. According to Cressey, these non-shareable problems are associated with status seeking or status maintaining activities. [21]

The second factor is Opportunity. A non-shareable problem by itself will not lead an employee to commit fraud.[22] The employee must also perceive that he/she has the opportunity to commit the crime without being caught. While the position of trust may provide an opportunity for the solution of a non-shareable financial problem, Cressey (2013) found that many trusted people did not at first see in their positions of trust the opportunities which such positions offer, and thus did not engage in fraud by using entrusted funds to solve their non-shareable problems.[23] Opportunity is established by ineffective control or poorly designed structure that leads employees to participate in unethical behavior or to commit fraud.

---

[20] Donald R. Cressey, *Other people's money*, (2013), p30.

[21] Ibid

[22] Joseph T. Wells, "Why Employee Commit Fraud", (2001, .Journal of Accountancy, p 43.

[23] Cressey (n 20).

The third factor is Rationalization. Rationalization is a means by which the fraudsters justify their dishonest action inacceptable to internal moral compass. It is the real reason(s) which the person has for acting in a fraudulent manner. Rationalization is, therefore, part of the motivation to commit fraud and is often abandoned after the criminal act has taken place. [24] Trusted person does not invent a new rationalization for his violation of trust, but rather applies to his own situation a verbalization which has been made available to him by virtue of his having come in contact with a culture in which such verbalizations are present.[25] The fraudulent individual acquires such verbalizations from other persons who have had prior experience with situations involving positions of trust and trust violation which is suggested as differential association theory that an individual learns crime from their association with persons already exposed to it. Examples of such ideologies that seek to justify the crime are: "some of our most respectable citizens got their start in life by using other people's money temporarily"; "all people steal when they get in a tight spot"; "my intent is only to use money temporarily so I am 'borrowing', not 'stealing'; "I have been trying to live an honest life, but I have had nothing but troubles so 'to hell with it"[26] Employees who take organization funds for their own purposes have been known to consider themselves as borrowers rather than criminals.

2.4. IMPACTS OF FRAUD

Fraud affects reputation of banks

Customers deposit their money in banks with trust that banks will safely protect their money from external or internal threat including bank fraud. Thus, when money deposited in a bank is withdrawn due to fraud, customers lose trust in banks. This, in turn, will damage the reputation and good will of the banks in addition to monetary loss. Monetary loss is associated with the cost incurred by employees or the bank to refund the customer. Reputational risk is, therefore, the risk of failure to meet expectation of customers or stakeholders as a result of any event that cause stake holders to form negative perception. It is customers' loss of confidence in the integrity of the institution. As a result, the customers trust and confidence on the concerned bank will

[24] Wells (n 22).

[25] Cressey (n 20).

[26] Cressey (n 20), pages 102-107, 110, 118, 124

gradually decline from time to time and thus customers, legitimate investors, borrowers and depositors cease doing business with such institutions which will eventually affect the banks' financial activity and their relations with their customers.

Fraud Undermines Integrity of Financial Institutions

Fraud can badly harm the soundness of a country's financial sector as a whole and the stability of individual financial institutions in multiple ways. In addition to reputational risk seen above, fraud will also result in Legal risks. This risk is associated with suing of legal actions for reimbursement of monetary loss incurred by the customer. This inevitably affects the reputation of financial institutions and forces investors to invest in countries that are less vulnerable to bank fraud.

Fraud reduces bank's profitability

Fraud leads to loss of money belonging either to the bank or customers. Such losses will reduce the profit which would have been obtained by the bank. It will also constrain the capacity of banks to extend loan and advance their money to profitable operations thereby reduces the profit they get from interest and their activities. The cumulative effect of these constraints impair the financial health of banks.

2.5. TYPES OF FRAUD

Bank fraud has been one of the main challenges many banks encountered in history. Based on the relation of the perpetrator to the bank, fraud can generally be classified as external or internal. Fraud is said to be external when it is perpetrated by a customer or other third party or with collaboration of an employee with external party. It is committed by outsiders who have strong relation with the bank or by new customers including competitors, suppliers, and sister company employees. Fraud is said to be internal when it is carried out by bank employees. Internal frauds refers to the act of a bank. However, the main focus of this paper is on external fraud and thus the researcher will try to address types of external fraud widely seen; that may include identity fraud, cheque fraud, ATM fraud, online banking fraud, and fraud with fund transfer letter.

2.5.1. IDENTITY FRAUD

Identity fraud is the most common financial fraud in bank industry. In this kind of fraud, the fraudster obtains personal detail information from different sources in order to impersonate and defraud the victim. It is the use by one person of another person's sensitive personal information such as their names, identity number, bank account information, PIN number or credit card number without authorization of such person. Identity fraud includes all types of acts or crimes in which someone wrongfully obtains and uses another person's personal data without permission of the rightful person. They acquire enough information to satisfactorily answer the questions asked by the financial institution. They steal personal belongingness containing sensitive information such as wallet, bag, credit card, book accounts and others. Then they will use all personal information obtained to defraud banks. Confidential information shared to close relatives, friends or family members are also sometimes used to withdraw money fraudulently.

Identity theft is usually committed by preparing forged ID cards. The identity thief will first acquire all information related with the sender such as his name, address, amount sent, the day sent, the branch etc. and prepares the forged Id in the name of the true recipient. Then, he will present himself as the legitimate recipient and receives the money. This type of fraud is also common in cheques to be paid to specified person. After stealing the cheque from the rightful holder, the fraudsters will prepare forged ID cards in the name of the true payee and present the check for payment as if they are the rightful payee.

The other identity theft usually seen in banks is financial identity theft. Criminals use the stolen personal information through phishing or cold calling to take over financial accounts and withdraw money from the account of legitimate person. Phishing is a type of email scam where the sender poses as a real company, organization or agency and asks to enter personal information. In "Cold Calling", the fraudster calls pretending to be a bank, real company or organization and ask into providing them with personal information. This type of fraud is

common in online banking where the fraudster acquires PIN number of the legitimate holder and sends money online to his own/another persons' account holder.

2.5.2. CHEQUE FRAUD

A cheque is an unconditional order to a bank to pay certain amount of money to the bearer or to the person named on the cheque. It is the most common means of payment among traders transacting in huge amount of money which is difficult to carry and pay in cash. Despite a reduction in cheque use following the innovation of electronic fund transfer payments, cheque fraud remains a problem in payment system. Cheque fraud refers to making of unlawful use of cheques in order to illegally acquire or borrow funds that do not exist in the account balance or under account holder's legal ownership. According to the AFP Report (2011), 14% of the victims of the organization suffered financial loss due to check fraud.[27] According to the American Bankers Association's 2011 Deposit Account Fraud Survey, 73 percent of banks reported that they suffered check fraud losses totaling approximately $893 million in 2010. However, attempted check fraud against bank deposit accounts resulted in around $11 billion in actual losses and expenses incurred to avoid losses in 2010. That figure was just below the $11.4 billion figure recorded in 2008. [28] As Ethiopia is not an exception to the global reality, though its degree may vary whether it be higher or lower, cheque fraud is practiced and thus there will be loss which necessitates its examination.

Besides, development of Electronic cheque also contributed the volume of cheque frauds as fraud can be easily committed through scanner, printer and desktop phishing software.

There are various forms of cheque fraud. Among them the most widely seen are:-

Counterfeit:- is a cheque created on non-bank paper to look genuine relating to the genuine account and written by fraudster. [29] Under this type of fraud, forged checks are prepared by

[27] Australian Federal Police report of 2011

[28] Dhameja (n 4) p 112.

[29] https://www.chequeandcredit.co.uk › information-hub accessed on 18/4/2021

fraudsters in the name of any person or organization they know having current account and check books in specific bank, then affix falsified signature on them and present for payment. Such type of fraud is committed by persons who have close relationship with the holder of check books, who know the bank and the branch at which the check holder has current account, the serial number of the cheque paper, the exact name by which the current account is opened, the account number of the current account, the signature of the cheque holder and other necessary details regarding the cheque. In one criminal case brought before Federal High Court Lideta Bench, the accused prepared a forged cheque in the name of one organization and wrote 450,000 birr (four hundred fifty thousand birr) to be paid from the account of the organization to a named person in the cheque.[30] Before preparing the cheque, the accused prepared a forged ID with a name other than his real name. Thereafter the accused presented the cheque for payment. The bankers cross checked the name on the ID and the name on the cheque, they verified the signature of the drawer and found it to be similar with the genuine one. However, as the amount indicated in the cheque is quite high, they made a phone call to the drawer of the cheque before payment for confirmation. Then the drawer responded that there is no cheque written for this person. When they realized this, the guards of the bank took him to the nearest police station and he was finally accused for corruption, fraudulent misrepresentation and for using forged document.

Forgery:- This is the most common cheque fraud where the fraudsters present forged cheques by falsifying the signature of the person issuing the cheque. The cheque is a genuine bank paper cheque. However, the signature is not that of the account holder but forged signature signed by the fraudster. Usually this type of fraud is committed when cheque books are placed somewhere easily accessible by another person. The person who obtained the cheque book may write a cheque by using falsified signature of the legitimate person with a view to get undue advantage therefrom.

Fraudulently Altered:- in this type of cheque fraud, a genuine bank paper cheque from a genuine customer is issued but the cheque is altered by the fraudster before it is presented for

[30] The researcher prefers not to disclose of the name of the accused and its file no. because the case is not yet decided.

payment. The alteration may be on the amount indicated on the cheque or recipient's name with the intention to receive the altered amount, not the amount written by the drawer. Altering the contents of cheque will be made either by chemical washing or by erasure, and after all of which a cheque will no longer be genuine.

Conversion of clearing Instruments: - This is kind of fraud becomes common when a Cheque drawn in favor of one person gets into the hands of a wrong person by any fraudulent means and the wrong person in possession of the cheque enjoyed the value on the instrument. In other words, such type of fraud comes into picture when a to order cheque is issued for the benefit of one person or another person, obtaining the cheque in any manner, presents the cheque for payment by using forged ID prepared in the name of the person named on the cheque. Here, banks after verifying the ID and the name on the check will pay to the person appeared. Under such circumstance, the question of who is responsible to pay the indicated amount to the legitimate payee of the cheque is very important. Especially this fraud becomes apparent when a cheque is accepted by a bank for which it cannot fully guarantee collectability until the institution on which such cheque is drawn has confirmed that funds are available to cover them.

Suppression of Clearing Instruments: - This is fraud perpetrated by paying a Cheque drawn on account having no sufficient balance upon issuance or when presented for payment. Issuing cheques having no sufficient balance or cover is a criminal act.[31] But, it can be understood that this type of fraud is committed by individuals against another individual and there is no issue as to whether bank should be held liable or not. Rather it will be the interest of both the fraudster and the defrauded person that claims his right civilly and/or criminally. The same is true with those persons who issue cheques after its account is closed.

2.5.3. FRAUD RELATED TO AUTOMATED TELLER MACHINE (ATM) FRAUD

With the development of electronic banking in the banking industry, the use of ATM has become prevalent now-a-days. ATM is an electronic banking that allows customers to complete basic transactions such as cash withdrawals, deposit and checking their accounts without the aid of a

[31] Criminal Code of FDRE,2004`, proclamation no. 414, Neg. Gaz. , Article 693

branch teller simply by inserting ATM cards. [32] ATM related fraud is fraudulent activity whereby the fraudster uses ATM card of another person in order to withdraw money from the account of another without the latter's consent.[33]

> "ATM related fraud is caused by the manipulations of unauthorized third parties, sometimes because of the incautious behavior of the cardholder, where the loss of a card is exacerbated as a result of the PIN being recorded with the card in some way. However, ATM fraud has increased from time to time with development of different technology that guess the PIN of the card holder. The negligence of banks in taking precautions may also cause such fraud to happen. For example, if banks fail to provide an effective shield to terminals or refuse to record a transaction with the use of video or CCTV or fail to provide for increased program code and internet safety, the fraudster may use these drawbacks as an opportunity to commit fraud. Criminals will go to the extent of renting flats across ATMs by using binoculars, telephoto lens, mini-spy-cameras, or by transmitting the PIN to an external personal computer where the ATM has been manipulated by the criminal to obtain the PIN when the PIN is entered." [34]

ATM fraud can be perpetrated through:-

Card Shimming: This kind of fraud is done by installing a skimming device, on the ATM machine for getting electronic data from the card's chip. The installed skimming device will capture magnetic strip equivalent data. Then the fraudsters use the stolen electronic data in order to imitate the card completely and withdraw money using the imitated card. The commission of this type of fraud is known by the customer only after money is withdrawn from their account.

Debit card skimming: A machine or camera is installed at an ATM to pick up card information and PINs when customers use their cards. Then the fraudsters get ATM card in any means and use the information they picked up to withdraw money. [35]

---

[32] https://www.investopedia.com accessed on 20/4/2021.

[33] https://www.bajajfinserv.in accessed on 20/4/2021.

[34] Gerwin Heyback, "Civil Law Liability for Unauthorized Withdrawal at ATM in Germany", Digital Evidence and Electronic Signature law Review, Vol. 6 (2009) p.57

[35] Ibid (n 33)

Card Trapping: This includes stealing the ATM card by installing a device at the ATM machine by the fraudster. Then due to the installed machine, the card will get trapped in the cash dispenser. When the card holder leave the ATM to receive help from bank officers for getting his card out, the fraudster will enter and withdraw money. [36]

Jamming of Keyboard: The fraudster will jam important buttons on the ATM machine keyboard such as Cancel and Enter buttons so that the transaction is unsuccessful and the customer may leave the ATM to get help. The fraudster then enters the ATM to withdraw money immediately from the machine as the details are already entered.[37]

Obtaining PIN code- The other ATM fraud is when unauthorized third party withdraws money after stealing and obtaining the pin code. This is caused mostly by breach of secrecy, spying to obtain the PIN and guessing the PIN. Breach of secrecy is violation of contractual duty to care from their card and PIN by customers. Some banks impose express obligation upon the customer to keep his PIN confidential and never to pass the PIN to others. For example, in Germany both the prevailing opinion as well as the conditions for the use of the Maestro Card oblige the card holder to keep his PIN confidential and never pass the PIN to others. In particular, the PIN must not be noted on the card or otherwise stored together with it, even in an altered form. Should the card holder keep the Maestro card and code close together, they undermine an important component of the Maestro safety system.[38]

Where a third person obtains the PIN or ATM card, it is assumed that the card holder has been engaged in careless behavior, despite the ease by which a PIN can be obtained by a third person. Card holders are bound to keep the PIN safe, and are not entitled to inform anybody voluntarily of the PIN. The card holder can physically carry the card as well as the PIN but must not write the PIN down on the card or otherwise store together, to avoid a thief obtaining the PIN if the card is stolen. Both card and PIN must be strictly separated even in private rooms and any loss sustained due to the breach of this obligation will result on non-imbursement of the amount withdrawn by fraudsters.

[36] Ibid
[37] Ibid
[38] Ibid (n 34)

2.5.4 ONLINE BANKING FRAUD

The rapid development of technology and internet over the past years in the 1990s and subsequent evolution of e-commerce have given rise to a dynamic business environment where a large volume of transactions take place without face to face interaction through e-payments. 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 e - banking. 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.”

Several e-payments systems have been developed and are increasingly used in e-business. Its development has facilitated the rise of many online shoppers which in-turn provided fast, reasonably safe and relatively low cost operations. However, the digitization of the financial and other data gave an opportunity for E-payment fraud by fraudsters. E-Fraud is “a deception deliberately practiced to secure unfair or unlawful gain where some part of the communication between the victim and the fraudster is via a computer network and/or some action of the victim and/or the fraudster is performed on the computer network.” [39] It may also be defined as “a fraud scheme that uses one or more components of the Internet – such as chat rooms, e-mails, message boards, or web sites – to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institution or to other connected with the scheme” [40]

However, the development of e-payment methods have expanded and with it the fakery has inevitably kept pace. A recent study found-out that more than 7 million consumer complaints have been received during the period from 2007 to 2011and a total of 990,242 of these complaints were related to frauds. [41] Consumers have reported paying over $1.5 billion in those fraud complaints. Additionally according to the report from Cyber-Source (2012), it was found

[39] Bergman B, “*E-fraud -state of art and counter measures*” (2005)

[40] USA department of justice report

[41] Lina Fernandes, ‘’Fraud in E-Payment transactions; threats and Counter-measures”, (2013), Vol.2, Asia Pacific Journal of Marketing and Management Review, P.24

out that merchants have reported losing an average of 1.0% of the total online revenue to Fraud in e-payment transaction in a global problem.[42] It also enables the fraudsters to develop more sophisticated and effective ways to scam online. For instance, Commission of European Committee (2008) report summarized the fraud problem by saying "Fraud against payment fraud remains a threat to the success of the internal market for payments. Payment fraud affects the consumer confidence in non-cash means of payment and ultimately the real economy." According to the report from Association for Financial Professionals AFP (2012), percentage of organizations subject to attempted and/or actual payments fraud has shown an increase from 2004 to 2009.

E-fraud can be committed in a number of ways. Among these the prominent ones are:-

Account Hacking: Hacking includes gaining illegal entry into a person's computer (PC) system. Fraudster use compromised customer credentials to hijack the origination system and use it in the lawful account holder's name.

Phishing: Phishing is a well-known technique for obtaining confidential information from user by posing as a trusted authoring. Phishing is an attempt by fraudster to get banking details through emails with attachment or hyperlinks. The e-mail appears to be sent from legitimate organization to trick people in order to reveal sensitive information. On clicking the attachment or the hyperlink, the computer system gets infected with malware. During the next online transaction, the malware activates and steal private and personal financial information, including credit card numbers, PIN number which is used by fraudster to steal money from the account. [43]

Spoofing or Website cloning: This is an act of creating a hoax web-site or to say duplication of a website for criminal use. The fraudsters use legitimate companies name, logos, graphics and even code. This usually take form of chat room or trade sites where people would innocently give out personal information to criminals or make a fake purchase of a non-existent product. [44]

[42] Ibid

[43] Ibid, P. 27

[44] Ibid

2.5.5. FRAUD WITH FUND TRANSFER LETTER

In this type of fraud, the fraudsters prepares forged letter with the header of the organization and forges the signature of the manager of the organization. Then, they prepare and send a letter containing the order that a certain sum of money is transferred from the account of the organization to the account of some other person indicated in the letter usually to fictitious account opened beforehand with fake and incomplete documentation so that once bank is defrauded they go underground and may not be traced with the fake address and documentation provided at the point of account opening. This type of fraud may also be committed by the employee in collaboration with the outsiders. Such fraudsters present forged articles and memorandum of association, trade license and all other documents necessary to open an account in the name of fictitious company.

2.6. FRAUD PREVENTION AND DETECTION

It is observed that the trend at which fraudulent withdrawal is increasing is alarming and thus calls for a serious check. Fraud prevention is taking appropriate measures to stop fraud from occurring. It reduces the opportunity of potential offenders to commit fraud. It includes the introduction of policies, procedures and controls, and activities such as training and fraud awareness to stop fraud from occurring.

APPLYING KNOW YOUR CUSTOMER (KYC) PRINCIPLE

Security is a fundamental and increasingly important issue in today's banking industry.[45] Over the last few years, the number of fraudulent transactions committed by third parties have arisen tremendously. Consequently, fraud prevention has become a central concern to banks, customers, and public policy makers. [46]

[45] Kanniainen, "Alternative for Banks to offer Secure Mobile Payments", (2010), Vol. 28 no. 5, International Journal of Bank Marketing, p.433-44

[46] Sullivan, R.J, "The changing nature of U.S. card payment fraud: industry and public policy options", Economic Review, Vol. 95 No. 2, (2010) pp. 101-33.

Barlington (1997) stated that "as a bank's policy, banking commences from customer identification to create a good business relationship and this is the most important norm of KYC concept.'' KYC is the basic tenet of all anti money laundering legislations and regulations whereby various procedures are laid down by banks for opening and operation of accounts. KYC policy is an integral part and prerequisite for the banking business to ensure the proper implementation of due diligence to identify their clients and ascertain relevant information as detailed as possible to do business with them.[47]

KYC policy is very important because once followed, one is able to prevent frauds, identify money laundering and suspicious activities. It provides a mechanism to identify the true identity and beneficial ownership of accounts, source of funds, the nature of customer's business and reasonableness of operations in the account of one's business so that banks know the customer with whom they are dealing and minimize the risk of being exploited by money launderers and fraudsters.[48] Thus, banks should establish anti-fraud procedures and culture, covering working practices and business ethics communicated to employees so that employees are aware of a zero-tolerance attitude to criminal breaches of business practices within the banks. Thus, minimum documents/information must be obtained from customers at the time of opening of accounts to prevent openings of fictitious accounts. Further, additional document/information may be obtained on case to case basis where considered necessary.

Fraud monitoring directive issued by NBE imposes an obligation on banks to have a well-defined fraud monitoring and control policies approved by boards, and procedures for fraud detection, mitigation and reporting.[49] . Similarly, some banks in Ethiopia adhere to KYC and KYE policy that enable them to detect suspicious activity in a timely manner and compliance with all banking laws thereby minimize the risk and protect their good reputation.

[47] Global Bank Limited, Know Your Customer Policy, (Dec. 2006), P.1

[48] Ibid

[49] (n 18), art.4

In CDD directive issued by NBE, it can be deduced that bank employees are obliged to verify customer's identity using as much as possible reliable and independent sources, documents, data or information. For this purpose, the identification criteria for natural persons are provided under Art 4(5) of the directive.[50] Accordingly, the minimum requirements for natural persons are; given or legal name, permanent address, date and place of birth, nationality, occupation, public position held and/or name of employer; type of account; and signed statement certifying accuracy of the information provided.

The sufficiency question is raised in countries like Ethiopia where documentation and data retention systems are poor to make things easy for identity fraud. Therefore, further efforts such as requiring other original documents, checking for telephone directory or home/office visit according to the situation, asking the provision of recent utility bill or tax assessment are recommended to verify the identity of those persons and to avoid identity fraud.

With regard to legal persons, the NBE directive stipulated the necessary requirements to identify legal person and the natural persons behind it.[51] It shall also be verified that the person who represents a company is authorized signatory with powers to open and operate the account and is actually authorized by the organization. Thus, banks shall take reasonable measures to understand the ownership and control structure of the customer; b) verify that any person purporting to act on behalf of the customer is so authorized, and identify and verify the identity of that person; c) verify the legal status of the legal person or legal arrangement at a minimum by obtaining proof of incorporation or similar evidence of establishment, existence of the legal personality of the organization.

In practice, in order to strengthen their internal controls and protect the bank from illegal activities, many banks have developed anti-fraud policy, anti- money laundering, payment card policy and procedure and different internal audit manuals. However, not all employees have

[50] Customer Due Diligence bank Directive, directive no. SBB/46/2010, National Bank of Ethiopia, art. 4(5)

[51] Ibid article 4(6)

sufficient awareness as to how to implement these policies.[52] It is also understood that banks are not giving timely training related to ethics and fraud to their employees.[53] The researcher further explored through interview that the employees carry-out their functions using the past experiences, and training on updated challenges of fraud are not given on time. The awareness and training practice related to fraud is weak in banks. [54] Further, the responses of interviewees shows that there is fraud risk in the bank and the controlling mechanism of banks has not been strong enough in the past but effective measures are being taken recently.

In order to identify their customers banks examine in detail, upon opening of account or making transactions. In Business organizations, certificate of incorporation and business registration, memorandum and articles of association, board resolution and documents showing identity of principal shareholders. Banks also monitor and report concerned authority of suspicious transactions. ATM Card, Cash, Cheque, specimen signature card and other stocks are kept under safe custody and controlled dually. Banks also use automatic SMS alerts that notifies customers when there is any transaction made on their account."[55]

However, controlling mechanisms to detect fraudulent activities such as: systematic signature verification, UV light and different machines that detect forged cheque, foreign and local cash, checker maker structure and online audit are not fully implemented. [56] Lack of emergency call center in the bank that receive complaints in case there is fraudulent act is also a challenge in their anti-fraud policy. [57] The use of Mag stripe cards, an old technology that can be easily copied, has also created an opportunity to widespread frauds like card skimming.

[52] Interview with undisclosed name, customer service officer at Awash Bank, Addis Ababa, April 5, 2021

[53] Interview conducted with name undisclosed, service officer at commercial bank of Ethiopia, Addis Ababa, April 1, 2021

[54] Ibid

[55] Cited above at note 43

[56] Interview with name undisclosed, customer service officer at Debub Global Bank, April 7, 2021

[57] Ibid

CHAPTER THREE

LIABIITY OF BANK AND THEIR OFFICERS IN ETHIOPIA FOR FRAUDULENT WITHDRAWAL OF MONEY BY THIRD PARTIES

3.1 INTRODUCTION

Banks are custodians of money deposited by customers. Hence, bank directors and bank officers are required to carry-out their functions in accordance with safe and sound banking practice with all the fiduciary duty of care imposed by law. Loss of money are sometimes subjected to constant agitation due to perpetration of tremendous fraud by outsiders and/or bank employees. The fact that customers lost funds implies that there are some officers in banks that fail to carry-out their activities prudently.

The Delaware Supreme Court described the duty of loyalty as:

> *"*a rule that demands a corporate officer or director, peremptorily and inexorably, the most scrupulous observance of his duty, not only affirmatively to protect the interests of the corporation committed to his charge, but also to refrain from doing anything that would work injury to the corporation, or to deprive it of profit or advantage which his skill and ability might properly bring to it, or to enable it to make in the reasonable and lawful exercise of its powers. The rule that requires an undivided and unselfish loyalty to the corporation demands that there shall be no conflict between duty and self-interest."[58]

Principles of, loyalty or safety and soundness is, therefore, an important source of bank directors' and bank officers' duties. The failure of discharging duties and responsibilities in the spirit of these values will entail liability on the bank and bank officers. Bank officers must exercise standard of care more than ordinary care and prudence in the affairs of a bank depending on the subject to which it is to be applied in view of all the circumstances surrounding the case. Indeed, the conduct that amounts to ordinary care in other affairs may not amount to ordinary care in the

[58] Heidi Mandanis Schooner, "Bank director Liability", *The George Washington Law Review*, Vol. 63, p.180.

affairs of a bank. [59]It makes the degree of care to be applied by bank officers and directors more demanding than the standard applied to non-bank officers and directors. The safe keeping of customers' deposits requires to act prudently and diligently according to accepted standards of banking operations, and avoiding the conduct that might result in abnormal risk or loss to a banking institution. For example, upon making payment to customers, a bank has a duty to scrutinize the transactions to ensure that funds are disbursed only according to the approval and signatures required by the deposit agreement.

The duty of customer due diligence dictates that bank officers should identify the person to whom they are giving service to the satisfaction of the law and identification procedure of the directive issued by the NBE. Though the scope of the duty to inquire varies according to the facts of the case and the history of the person with whom they are dealing, in any case, it should not be overlooked that the minimum identification procedure and criteria stipulated by a law are met.

However, the competition that exist between financial institutions to attract new customers and greater market share pushed them to simplify "know your customer" procedure upon opening bank accounts and during payments. This is due to the fear that such customers will shift to another competitive bank if they tighten the requirements to accept new customers and also if they require further evidences to make payment to the customers. The continuation of these practice will create conducive way for fraudsters to plan the ways of committing their fraudulent acts.

Verification may differ depending on whether the depositor is an individual or corporation. In relation to individual depositors, the entire burden of inquiry and verification would be carried by the bank, whereas when a corporation is involved, at least some of the responsibilities for discovering misappropriation by an officer lies with the corporation. Thus, under this chapter the researcher will address the civil liability of banks and bank officers in case money is withdrawn from accounts of customers fraudulently by third parties.

[59] Ibid

3.2. LIABILITY OF BANKS

3.2.1 LIABILITY EMANATING FROM IDENTITY FRAUD

While identity theft is hardly new, law enforcement officials and consumer advocates say the Internet is making identity theft one of the signature crimes of the digital era.[60] Access to the Internet enabled fraudsters to sell all sorts of personal information on websites and, with that information in hand, thieves can acquire credit and make purchases using someone else's identity and credit.[61]

Identity fraud can be committed through sole act of third party or through involvement of bank officer the latter getting unlawful benefit as a return for the assistance in the commission of the act. The question as to whether bank is liable for the misrepresentation of its officer which is made solely for his own benefit and/or for that of a third party and as to whether the bank and/or its officer will be held liable for such acts deserves detailed analysis.

In Nejiha Dewale vs Awash Bank, the applicant filed an application for cassation review of judgments given by lower courts alleging that there is basic error of law.[62] The case started at Federal First Instance court by the then applicant alleging that she sent 45,000 Birr from Dire Dawa to be paid to Ato Sherif Kedir via the respondent Awash Bank. When the beneficiary went to receive the money from the respondent, the respondent admitting that the money was sent, refused to pay to the claiming beneficiary alleging that the money was already paid to another person having the same name after verification of his identity with his ID card and thus, the respondent is not liable to pay the money to the intended beneficiary. The Federal First Instance Court and the Federal High Court rejected the claim of the applicant. Then, the applicant filed an application for review by Cassation Division of Federal Supreme Court. The Cassation Bench decided that the respondent did not return the money he has received in bail as per article

---

[60] *See* O'Brien, *Officials Worried Over a Sharp Rise in Identity Theft*, THE NEW YORK TIMES, April 3, 2000.

[61] Ibid

[62] W/o Nejiha Dewale vs. Awash International Bank, Federal Supreme Court Cassation decisions,[38289]

2792(1) of civil code to the applicant or any person designated by the latter. The respondent should have paid the money to the intended recipient and if payment is made by the respondent to another person that appeared with identity fraud, it is the Bank, not the customer who is defrauded and thus the respondent Awash Bank is liable for the fraudulently withdrawn money.[63]

In another Cassation Bench decision [64] that started at the Federal First Instance Court, the applicant named Sherefedin Abdela brought a suit to claim 145,860 Birr sent from Ato Ahmed Isa for her benefit in 1999 E.C and when the applicant went to the respondent Bank to receive the money, the respondent refused to pay alleging that the money was paid to another person with same name following the regular procedure of banks and thus it is not liable to pay again. The lower courts decided that the bank paid following regular procedure of banks and thus owes no liability. The Cassation Bench affirmed the decision of lower courts after making analysis that banks are liable for fraudulently withdrawn money only where banks failed to follow regular banking procedure and paid without due care or where it is proved that the bank is defrauded. In this case, it is proved by lower courts that the bank followed normal bank procedure. On the contrary, the applicant did not prove that the bank is defrauded. Thus, bank owes no liability.

This decision will also invite questions worth analysis: 1. what is normal banking procedure? Who should implement banking procedures that best prevents or detects frauds? Whose responsibility is it if appropriate fraud prevention or detection banking procedures are not well formulated and implemented? What is the remedy of the customer in such cases as fraudsters, once they withdrew the money, can't be found and their identity is difficult to trace? Is it the customer who bears the burden to prove that the bank is defrauded or it is the burden of the bank to proof the bank is not defrauded? As far as the money is proved to have been withdrawn fraudulently, what kind of further evidence is required to prove that the bank is defrauded? Isn't the case at hand a bank fraud? These are few of the many questions that one may frame from this specific case.

[63] Ibid

[64] Sherifa Abdela vs. Commercial bank of Ethiopia, Federal Supreme Court Cassation Decision, [48269]

Modern legislations assimilate fraud with contract and hold the principal liable for fraud committed in carrying-out of his functions by applying the doctrine of respondeat superior. This doctrine is founded on public policy to attribute liability to the employer connoting that 'Let the master Answer'. It imposes the burden to compensate loss sustained by third parties on the employer. Firstly, an employee is a worker who has limited economic capacity working under someone's direction and authority to fulfill their monetary needs. Thus, if employees are only to be held liable, the person who is injured by their negligent act will not be able to get satisfactory compensation. Secondly, this doctrine will avoid blame game because working for someone in the course of employment without attributing liability on them for the acts of subordinates would allow them to shed and bend their responsibility in choosing responsible and qualitative subordinates.

There are two requirements for the doctrine of responseat superior to be applied. A true employer-employee relationship and the tortious act of an employee must be one within the scope of his employment. 'Scope of employment' implies that the act is done with the express or implied authorization of the employer. Same liability is applied to the situation where the agent acts with the secret purpose to benefit only himself and without the knowledge or consent of the principal.

Like most negligence claims, customers can make a bank liable for money withdrawn fraudulently from their account, if they can prove that: (1) the bank committed some act or some of its officers failed to discharge their obligation of due diligence; (2) that the bank owed a duty to the consumer whose identity was stolen; (3) that the bank breached that duty; and (4) that the breach was the actual and proximate cause for the consumer's injury. [65]

The first obligation imposed on a bank is to exercise customer due diligence in giving banking service. A bank's officer has to make the effort possible to identify to whom payment is being made. Such verification is usually made by asking to present ID cards, driving License or

[65] The fact that the customer opened an account in the bank and deposit money there automatically imposes an obligation upon the bank to safely protect from the act of fraudsters, at least.

Passports which are easy to obtain through forgery or other illegitimate means. It should also be evaluated considering established identification policies and verification of the authenticity of signatures, photographic identification and a comparison of signatures. Thus, upon submission of withdrawal voucher to banks, banks should exercise further inquiry to identify who the person is by asking for additional evidences as and when the need arises.

If we take Customer Account and Transaction Services (CATS) of the Commercial Bank of Ethiopia (CBE), a customer should submit withdrawal voucher together with his/her ID, nd the officer on the counter identifies the customer against the scanned digital photo and authenticates the signature of the customer on the voucher against the scanned signature.[66]

The obligation of customer due diligence will impose additional effort to verify who the customer is. Such obligation is exercised flexibly according to the circumstance of cases and the monetary amount claimed to be withdrawn. For example, one can understand the different caution to be taken to verify the identity of the person when withdrawal of 100 birr and withdrawal of 100,000 birr is asked. The same is true for those suspected to have bad history, criminally and politically exposed persons.

The fact that fraudulent act is committed will show prima facie presumption that there is negligence and that obligations are overlooked by the officer of bank. So, like any presumptions in civil suits, if the existence of fraudulently withdrawn money is proved, there should be the presumption that negligence is there with the concerned bank. The burden of proof should be seen flexibly by the courts depending on additional due diligence that the circumstances require in that particular incident. The discharge of obligations stipulated by the prescribed procedure by itself should not be considered enough in all cases. Because, such procedures are not fit to worn procedures for each fact. Courts should also consider who is in better position to avoid the risk in determining the liability. As far as money is deposited in banks and banks used the deposited money to advance loan and obtain profit from the difference between the lending rate of interest

[66] Customer Account and Transaction Service Procedure, CBE, art. 7.2

and interest paid for deposit; banks should bear the risks associated with the money deposited including but not limited to fraud. As banks are at better position than customers to detect and avoid the risk of fraud, liability allocation should also consider this fact. So, banks and financial institutions operate at their peril when they disregard established security measures designed to prevent identity fraud by exercising customer due diligence.

On the other hand, making banks liable for each and every fraud may put financial institutions at peril and greatly affect the soundness of financial institutions. It may lead even to bank failure which, no doubt, affect the economy of the country as a whole. Thus, appropriate balance should be crafted by the legislature so that both the interest of the customer and that of the financial institution is not put at risk.

In Ethiopia, the Cassation Bench of the Federal Supreme Court has given a ruling that when a claim is brought before a court alleging that a bank yet money withdrawn from my account with forged documents or signature, the case should be settled not by settling the issue of whether there is forgery or not, but instead by settling whether bank made payment without taking appropriate care or without following regular procedure of banks. The court further ruled that if there is no evidence proving that the bank made payment without due care or did not follow regular procedure of a bank, there is indication that the bank committed no fault and thus owes no liability.[67] However, it is possible to argue that it should be banks that should enact and provide a better fraud prevention policies and procedures with the effect that if bank fails to discharge its obligation of updating its fraud prevention procedures and know your customer policies, then the concerned banks should be held liable for the loss. The carrying out of his duties according to established and regular working procedure should be made a defense for the bank officer only, not for a bank.

Law enforcement officials, courts and legislatures view banks as the true victims of the theft and as more victimized customers turn to those institutions for recovery, Courts and possibly the

[67] Commercial Bank of Ethiopia vs Glory PLC (4-persons), Federal Supreme Court Cassation Decisions, [41535].

legislature will be called upon to define the scope of the duties and obligations such institutions owe their customers as well as the public at large.

3.2.2. CHEQUE FRAUD LIABILITY

Each cheque transaction includes a drawer, the payee, and the drawee bank that maintains the funds on which a check is drawn. Unlike other payment frauds, in cheque fraud, the primary liability is assigned to the party that pays, as opposed to the party expecting or initiating the payment.[68] However, customers are not exempted from liability in contrast to "zero liability" policies offered to customers for most types of payment card fraud by banks. [69] Thus, identifying who bears liability depends on circumstance of each case and to whom the fault resulting in payment fraud is attributed.

Banks are liable mostly when they are negligent in verifying the genuineness of the signature on the cheque. Liability may be attributed to the drawee because banks are in a position to verify the drawer's signature by comparing it with the specimen in its possession. It is the bank that is in better position to avoid the fraud and is the last institution to examine the check prior to settlement. Thus, liability should be attributed to the bank in such cases. When the customer's signature on the cheque is forged, the creditor-debtor relationship that exists between a bank and a customer indicates that the bank has no mandate to debit the customer's account due to such forged cheque containing forged signature.

Even when signature on cheque is forged, there are exceptional situations when banks may not be held liable in various jurisdictions. For example under Uniform Commercial Code, if a signature is forged, the customer may be liable for fraud losses under a variety of exceptions, including the following: if the account holder fails to exercise ordinary care; if the customer fails to reconcile statements within a reasonable time; if "comparative fault" is found; or if the counterfeit is virtually identical to the original. [70] However, in case of verifying the genuineness

[68] Ibid (n 4) p 113
[69] Ibid
[70] Ibid

of endorsement on a cheque, it would be different. It will be impossible for banks to verify an endorsement. Banks are not in a position to know the signature of endorsers and that of the person for whom it is endorsed.

Currently in Ethiopia, under National Payment System Proclamation, the establishment of central security depository is incorporated.[71] The central security depository is an entity where securities and other financial instruments are registered and immobilized so that transactions with these instruments are processed through book entry. [72] This necessitates addressing the liability of such depository entity in case there is fraud. Accordingly, for traditional checks, a drawee bank is liable for fraud claims that involve the drawer's signature on the face of a check. However, regarding liability claims for fraud that involves the payee's endorsement on the back of the check, it is the depository bank that is held liable. [73] This is because once the cheque is deposited to the depository entity, it is this entity that should avoid the risk associated with fraud in the endorsement and payments made through them.

The wide use of electronic cheque currently has also the tendency to change the liability regime of both banks and the customers. Some banks have allowed customers to deposit checks with a camera-equipped cell phone for instance. In Ethiopia, too, converting cheques to electronic image was recognized under National Payment System Proclamation of Ethiopia.[74] Thus, it is important to point out that substitute checks are becoming so popular in the society. The digital image of the cheque is scanned or photo of the cheque is taken on a smartphone using a bank-supplied application and electronically transmitting it to the bank. Thus, the electronification of cheque processing changed the issue of assigning liability and made attribution of liability more complex. This complexity is attributed partly to lack of clear updated law that addresses the digital reality of cheque processing. However, in recent years, private agreements among financial institutions have taken on increased importance in ensuring that liability for check fraud is clearly assigned in transactions involving check image exchanges.

[71] National Payment System Proclamation, 2011`,Proclamation no. 414, Neg. Gaz. , Article 4(1)(b).

[72] Ibid, art. 2(4)

[73] Ibid (n 4) p 114.

[74] Ibid (n 71)

Thus, banks must find substitutes for traditional verification processes. But there is no verification processes stipulated by banks in Ethiopia. Thus, there should be minimum requirements regarding verification of the person.

Liability of banks should not be stretched to the extent that they should take extra-ordinary caution during payment of cheques. If we take an example, in electronic cheques the question of whether the paying bank is bound to keep an ultraviolet ray lamp and to scrutinize the cheque under the said lamp will be a question if no infirmity on the face of the said cheque is found. If banks make payment in due course believing in good faith under the circumstances which do not afford a reasonable ground for believing that the holder is not entitled to receive payment of the amount therein, banks should be exempted from liability. If the banker, at the time of verification of serial number and signature on the cheque and the specimen signature of the drawer, found that the cheque has on its face no defects, banks will not be held liable merely because other extra-caution is not taken and that banks should refer to further scrutiny by using advanced technology such as ultraviolet ray lamp to detect that the cheque is forged. However, if material alteration on both the cheques were visible and were not verified by banks, the latter cannot claim protection. In such cases, the bank will be paying the amount on the said cheque at its own risk. This, however, does not protect a banker in case the signature of the customer is forged.

3.2.3. LIABILITY EMANATING FROM FUND TRANSFER LETTER FRAUD

Withdrawal of money through fund transfer letter fraud is becoming one of the most common ways fraudsters employ to fulfil their criminal intent. It is usually perpetrated by employees of organizations by forging the signature of a person usually the manager of the concerned organization. They prepare a letter ordering the payment of indicated amount from the account of the organization to some other account created with a fictitious name. The letter will be printed out on a headed paper of the organization, signed with forged signature in the name of the manager and presented to the bank for execution according to the order. Fraudsters may also claim withdrawal by presenting forged ID prepared in the name of the payee indicated in the letter. In such cases, banks after verifying similarity of specimen signature of the manager and

the signature on the letter, pay or transfer the amount indicated to the person named therein or to the account indicated in the letter. Thus, the legal issue who is responsible for the fraudulent withdrawal and who is going to reimburse the account holder from whose account money is withdrawn is central issue requiring examination of the pertinent provisions of the law, if any.

The latter fraudulent act is perpetrated partly because banking officers in discharge of their duty are negligent in verifying the person to whom they are paying. The CDD obligation dictates that bank officers should identify the party with whom they are dealing according to regular working procedure of a bank. Such customer due diligence requires identifying identity of that person before effecting payment or transfer. The failure of the bank officer to discharge these obligations will drag primary liability to the bank, then to the officer at negligence.

Banks have their own CATS in their daily services. According to CATS of CBE the transfer initiated through payment letter of instruction should only be allowed for the following purpose to the branch by duly authorized person in writing, who receives power of attorney, verifies the signature and confirms the genuineness of the document by communicating with the owners/signatories of the corporate entities; receives delegated person's photo, ID card as well as signature specimen and open mandate file for the future reference; and authenticates the signature of the account holder/authorized signatory. The mandate file shall be maintained electronically as and when the system for the purpose is implemented.

Therefore, payment or transfer should be made after verifying identity of the person and, genuineness of the letter sent to a bank. Such verification includes communicating with the originator of the letter, and comparison of the specimen with the signature on the letter etc. Thus, if bank authorizes payment or transfers fund without discharging these duties, the bank as institution and the officer individually will be held liable.

3.2.4. LIABILITY EMANATING FROM ELECTRONIC PAYMENT FRAUD

The traditional cash-based payment system has been gradually overwhelmed by electronic payment system due to advance in technology in banking industry. An electronic funds transfer refers to all forms of e-payment including ATM, POS, and automated clearing houses. "As banking transactions have moved from physical bank locations to the online world, so have the

criminals who threaten them: by and large, fraud prevention and mitigation are the primary responsibilities of the numerous entities running the various electronic and paper-based payment schemes across the country." [75]

With online banking, banks must provide reasonable security to protect customers' funds and accounts. This reasonable security includes the processes and procedures that banks traditionally use to physically protect funds and methodologies to now protect against new threats. If banks fail to implement reasonable online information security controls, losses to fraudsters will increase and customers will hold banks accountable.

Each bank should establish an assessment of access control mechanisms to authenticate and permit access only to authorized individuals and then implement appropriate controls. The liability of a bank in electronic payment fraud can arise from two situations: first, banks are liable under strict liability situations if they fail to implement control procedures the situation demands; or second, under tort negligence where banks failed to exercise reasonable security standard and duty of care online baking deserves. In today's online technology where criminals commit cyber-crimes and access confidential information of customers, the use of a single factor such as username and password for authentication is becoming insufficient and is beneath what was commercially reasonable for the time.

Many countries established the reasonable duty of care financial institution must follow for an online authentication system that grants access to perform electronic funds transfers. They enacted Guidelines for Authentication in Internet Banking. Banks must implement security measures that warn their customers of suspicious activities that the bank should have noticed. Thus, under tort negligence analysis, failure to implement recommended online authentication procedures will likely result in banks' civil liability for loss sustained by customers.

The trend in many countries shows that banks will defend or at least try to minimize their liability in two ways: through the use of contractual language and by applying exceptions that

[75] Howard S.Koh, '' Liability of Lost or Stolen Funds in case of name and number Discrepancies in Wire Transfer" (1989), Vol.22, Cornell International Law Journal, P.24

exist in law.[76] Banks might also attempt to avoid liability by raising the gist of the action doctrine, contract provisions, and contributory negligence as affirmative defenses.

The defense of Gist of the action doctrine is an affirmative defense raised by banks designed to maintain the conceptual difference between contractual terms and tort claims.[77] This principle precludes plaintiffs from recasting ordinary breach of contract and tort claims. [78] It only applies when the relationship between the parties exists solely due to a contract. However, it does not bar a tort claim where there exists a duty in addition to the contract. However, any attempt by a bank to apply the gist of the action doctrine based purely on the existence of a contract between the parties will fail. This is because customers have multiple grounds based on tort and contractual claims to rely on to claim the recovery of their money. [79] The obligation to follow the required online procedure is not limited to banks only. The customer is also required to follow an agreed upon security procedure between themselves.

Banks will likely attempt to follow the guidelines for authentication in internet banking. They attempt to minimize their obligations by requiring the consumer to use reasonable information security practices and procedures by way of contract. Moreover, they avoid negligence claims by requiring consumers to agree to terms that recognize that the information security measures the banks already employ are "commercially reasonable." This may have the effect of minimizing the implementation of stronger controls.

The defense of contributory negligence is raised by banks asserting that customers negligently contributed to the loss of funds because the fraudsters may have obtained the customers username and password in some fashion such as by trying every possible variant of a password via a specialized script. Perpetrators may also install malware to capture personal information that customers type to authenticate their identity on website.

---

[76] Paul Rice, "Civil Liability Theories for Insufficient Security Authentication in Online Banking ", (2012), Vol. 10 no. 3, De Paul Business and Commercial law Journal, p.455
[77] Ibid
[78] Ibid
[79] Ibid

This means that the practice of authenticating a customer using only a user name and password no longer represents reasonable access controls when customers request access to their online bank account. [80] Instead, banks should move to the use of multiple factors to authenticate users. For example, in America Federal Reserve system Regulations established Interagency Guidelines Establishing Information Security Standards that requires three basic factors': something the user *knows* (e.g., password, PIN**);** something the user *has* (e.g., ATM card, smart card); and something the user *is* (e.g., biometric characteristic, such as a fingerprint) ". to identify the customer accessing online their bank account. [81]

Proper implementation of this Guidance requires the use of at least two or more of these categories. The use of two factors from a single category will not prove sufficient. For example, a bank that implements a two factor authentication system might require customers to provide their username, password, and a six-digit number from a previously issued physical token. The six-digit number expires either ten-minutes after the bank issued it or after the customer uses it, whichever occurs first. Thus, a thief would have to obtain all three pieces of information in order to compromise the account. Implementation of these multi-factor authentication program should be appropriate to the level of risk in that application. What constitutes legally appropriate authentication may also change over time as new threats arise and better technology is developed to address them.[82]

For example, Google, Google Mail, Google Documents, and Google Reader now offers two-factor authentication for its online applications. Google uses two step verification scheme using two factors: something the user knows such as username and password, and also provide the verification code that Google sent to the users' in a text message. Therefore, if Google offers his advanced feature capable of receiving text messages set to protect e-mail and other online applications, banking customers will increasingly question why their banks do not offer similar protection.[83] As the fraudsters develop more and more technology to overcome the security

[80] Ibid

[81] Ibid p. 447

[82] Ibid

[83] Ibid

measures of banks, the definition of reasonable and legally appropriate authentication will also grow to encompass ever more complex processes that may include previously unheard of technology.

3.2.5. LIABILITY EMANATING FROM PAYMENT CARDS (ATM)

In 1994, experienced criminals would have required 1900 years to find out a PIN. Three years later, they would only have needed 96 days, shortly after only 19 days, since 1999 no more than 24 hours.[84] With the advent of e-banking, the use of ATM has increased dramatically from time to time. It played a great role in easing the time spent in finding where banks are and waiting for working days and hours of the bank to make payments, withdrawals or deposits. It is one of an attempt to create cash-less society thereby shifting paper-based payment systems to electronic payment systems.

With regard to liability related with ATM fraud, banks deny their liability raising the defense that the card holder is the only person who knows the PIN and it is entirely the fault of the card holder if such PIN is disclosed to third party. In other words, it is assumed that the card holder has complete control over the card and thus it can be concluded that either the card holder must have withdrawn the respective amount, or they permitted a third person so to do, or they were so negligent as to permit unauthorized third person to obtain possession of the card and PIN. Where a third person obtains the PIN, it is assumed that the card holder has been engaged in careless behavior, despite the ease by which a PIN can be obtained by a third person. Once the card holder lost the control of the card and PIN, the fraudsters may withdraw as much money as they can except the daily limit of withdrawal. The card holder knows the existence of such fraudulent withdrawal only after unknown debit posting on his account.

In order to reduce the possibility of fraud by fraudsters, the card holder is expected to separate two components for security reasons. 'Saving the EC components separately' means keeping them in different boxes, pieces of furniture and locked drawers, or in different pockets of items

[84] The detailed report of 19 January 1999 is available at: http://www.heise.de/tp/deutsch/inhalte/te/ 1771/1.html.

of clothing.[85] Such duty emanates either from the law or contractual terms the card holder and the card issuer agree. As PIN is the most important identifier of the card holder at ATMs and POS terminals, card holders are contractually bound to keep the PIN safe and secret and are not entitled to inform anybody of the PIN.

However, the duty to keep PIN secret and determining whether the card holder acted negligently differs depending on each circumstances of the case. For example, making permanent record of the PIN for the purposes of an aid to memory is not considered as negligent act. However, the PIN must not be written down on the card or otherwise stored together, to avoid a thief obtaining the PIN if the card is stolen. If a card and PIN are used promptly at an ATM, the prima facie evidence argues for the fact that the card holder has noted the PIN on the card or stored it with the card.

Card holders are also obliged to hide their PIN number when they use ATM or POS machines for cash withdrawal or to make payment. But it is worth-mentioning to differentiate active and passive observation of the PIN. Passive observation is the most common method through which third parties see PIN of another persons' for example by looking over someone's shoulder at ATMs in busy places or at POS terminals in supermarkets. However, whatever happens, the law of evidence and how the pleading are drawn up will be of great importance in establishing which party is put to proof to prove their case.[86]

When we look at decision of courts in ATM withdrawal, the prevailing judicial stand is that the prima facie evidence is granted in favor of the bank. Such prima facie stand is taken based on the assertion that it is impossible to decode PIN at short notice, mutable experience of life and technological progress. The customer is required to report the incident as soon as he became cognizant of the withdrawal. The failure to report same will demonstrate that the customer is not diligent enough to safeguard his interest.

---

[85] D.Gerwin Hayback, " Civil law Liability for unauthorized Withdrawals at ATM in Germany", Digital Evidence and Electronic Signature Law Review, Vol.6 (2009) P.59.

[86] Ibid

In one case brought before the Federal First Instance Court [87] the plaintiff instituted a file on the defendant claiming that money is withdrawn from his account at different times using ATM without his authorization or knowledge. Thus, after clarifying who withdrew money from the ATM's camera, the plaintiff claimed the decision to be given ordering the defendant to reimburse the money. After hearing both parties, the court gave decision that since the ATM card is in the hand of the plaintiff and the plaintiff brought no evidence as to whether the ATM card is lost or stolen, and there is no evidence produced proving that the plaintiff notified the bank so that the account is blocked not to use ATM services, it is presumed that the withdrawals are made either by the plaintiff or by those who obtained the ATM and its PIN number with the consent of the plaintiff or with his authorization. Rejecting the claim made by the plaintiff, the court made an analysis that the plaintiff did not prove that the money is withdrawn due to the defendant's fault.

However, courts should consider limits of prima facie presumption that it is not possible for a customer to challenge a bank effectively until the safety standard of the electronic payment system is no longer granted to be authentic or genuine. If for example the customer notifies the bank that he has lost his ATM and the bank failed to deactivate the use of ATM by that account, if money is withdrawn after the notification the banks are held liable to reimburse the amount withdrawn after notification. In one case decided by Federal Supreme Court Cassation Bench [88] the court decided that once the customer notified the bank in writing that the ATM card is lost, it is the obligation of the bank to disable the use of the account by ATM. Additionally the court in its ruling held that unless the bank proves that it followed regular procedure, took due care and committed no fault the bank will not be relieved from liability by alleging that the customer did not ask his account to be closed.

3.3 LIABILITY OF BANK OFFICERS

Banks perform their activities through their employees. Thus, all liabilities that banks face we discussed above come from the negligent acts of their officers. Banks are held liable because

[87] Dagima Bushura vs. Awash International Bank, Federal First Instance Court, [80218]
[88] Abebayehu Girma vs. Dashen bank, Federal Supreme Court Cassation Decision, [96309]

they are vicariously liable as employers. An employer shall be liable under the law where one of its employees incurs a liability in the discharge of his duties. [89] Thus, acts of their employees result in liability of banks. The liability is deemed incurred in the discharge of duties where the wrongful act or abstention was committed for the purpose of carrying-out duties. Damage is deemed to be caused in discharge of duty where it is caused by a paid worker at the place where or during the time when he is normally employed. [90] If banks are vicariously held liable for faults committed by their employees, the question of what the liability of their officers requires analysis in light of pertinent legislations.

Bank officers have the duty to act in good faith and with ordinary care and diligence as ordinarily prudent men would exercise in one's affairs with reference to the conduct such financial institution requires. The different type of fraud banking industries have been facing throughout the country due to negligence on the part of bank officers necessitate analysis of what the liability of banking officers should be so that they carry out their functions diligently in order to avoid liability. The law imposes an affirmative duty upon bank officers. It is this duty and the resulting civil liability for the neglect of same that entails their liability.

There is no special law regulating liability that bank officers have in Ethiopian banking industry. Nor is there indication of what their liability is. In such situations, one can logically argue that the provisions of contract and extra-contractual liability can be applied. Accordingly, liability of bank officers to banks may emanate from contractual relationship between banks and their officers. A bank officer, when employed by a bank, owes the duty of due diligence to the bank. Thus, if bank pays compensation to a customer who sustained loss due to the negligence of an officer, it implies that the concerned officer breached the duty of diligence he owes towards the bank, which subjects him to liability of reimbursing the amount paid by the bank to the customer due to breach of contractual obligation of acting with due care and diligence.

[89] Civil Code of the Empire of Ethiopia of 1960, Proc . No. 166 /1960, Arts.2130.

[90] Ibid article 2132.

On the other hand, the failure of an officer to discharge his professional duty prudently is a fault under Ethiopian the extra-contractual law. A bank officer is a professional person employed by a bank to give his professional service to the bank's customers or to the bank. If such professional fails to discharge his duties according to accepted rules of the practice of his profession, then he will be guilty of imprudence or of negligence constituting definite ignorance of his duties under the Ethiopian tort law.[91]

Thus, what constitutes fault in the course of employee's carrying-out of their duty will be seen in light of obligations imposed on them. No field of the law can be approached as an exact science, and that part of the law dealing with officers' liability is no exception. Thus, it is necessary to make general survey of obligations that are imposed upon these officers in their day-to-day activities and the failure to discharge of which brings civil liability upon them.

When a customer deposits money in a bank, thus divesting himself of the immediate control of his property, he expects, and has the right to expect, that the banks will exercise ordinary care and prudence. The degree of care required of bank officers in their handling of banking affairs, has been generally stated as, that care which men of ordinary prudence would exercise under similar circumstances depending on circumstance of each case. But, it is impossible to definitely define what is expected as a general rule, but a few broad principles of liability have been developed and are applied by the courts to these particular types of cases, which principles are reflected in various decisions.

In payment frauds perpetrated through identity cheating, bank officers are liable when they failed to follow regular procedures stipulated by the bank. Their liability arises when they failed to identify the identity of the person to whom they are making payment following regular and stipulated working procedure of the concerned bank. By assuming the position, they impliedly undertake to use as much diligence and care as the proper performance of the duties of their office requires, and to give the enterprise the benefit of their best care and judgment. Hence, bank officers are also expected to exercise enhanced due diligence and ask for additional

[91] Ibid

identification documents when suspicious circumstances happen. It is the duty of these officers to know the degree of due care they are supposed to exhibit, and they are presumed to know and that they have the means of knowing. Thus, prevention of payment fraud requires additional efforts to identify the person requiring service depending on circumstance of each case.

In cheque fraud, banks officers are held liable mostly when they are negligent in verifying the genuineness of the signature on the cheque. They should compare and verify the signature on the cheque and the specimen signature the drawer gave to the bank. In electronic cheque, liability of banks and their officers should not be stretched to the extent that they should take extra-ordinary caution during payment of cheques as far as there is no apparent infirmity on the cheque. If banks make payment in due course believing in good faith under circumstances which do not afford a reasonable ground for believing that he is not entitled to receive payment of the amount therein, banks and bank officers should be exempted from liability. If the banker, during verification of serial number and signature on the cheque and the specimen signature of the customer, found that the cheque visually has no defects, the bank officers will not be held liable merely because other extra-caution such as ultraviolet ray lamp is not taken.

In case of withdrawal of money through fund transfer order, if the bank officer failed to discharge his obligation of KYC due diligence and it is found that there is negligence on the part of the bank officer to verify identity of the customer, the bank officer will be held liable.

In case of electronic payment fraud, the possibility of being liable is rare except where there is disregard of already established security measures by bank or there is personal involvement of the officer in the perpetration of the act.

With regard to liability related with ATM fraud, the possibility of bank officer to be held liable for ATM fraud is not apparent save to exceptional situations where the circumstance warrant the officer disclosed the PIN of the customer upon issuance of card or where the latter failed to deactivate the ATM card after the loss of ATM is reported to him personally or committing of any express procedure of bank is proved.

To whom such officers are liable in case they are held liable is also another point that requires analysis once they are held liable. Accordingly, customers whose money is fraudulently withdrawn has no contractual relationship with the bank officer directly rather their contractual

relationship exists with the bank. Thus, the lack of privity or contractual relation between the customer and the bank officers bars the customer to bring the action directly to the officer. The duty to exercise due diligence by the officer is primarily owed to the bank not to the customers whose injuries are incidental. Thus, as rule customers will claim the damage from the bank with whom they have contractual relationship and that is vicariously liable for the acts of its employees and then the latter may claim damage from the employee who directly involved in the negligent act.

However, if we make bank officer liable for each and every act arising from his duty, it would be highly detrimental to the public interest. Because, banking institutions cannot generally be operated save through its officers, and if officers were held liable at law to the customers in damages for every act and negligence, responsible men could not be found who would take upon themselves the perils and dangers of the position. Almost all persons may lack will to work as banking officer in order to avoid liability arising therefrom. However, as an exception, where there is 'gross negligence'(not negligence), incompetency, reckless disregard of their duty to care and protect money in their hand or where such officers unlawfully benefitted personally from perpetration of the act, it will be justifiable if such bank officers are also held liable directly to the customers.

CHAPTER FOUR

CONCLUSION, FINDINGS AND RECOMMENDATION

4.1 CONCLUSION

Payment fraud is one of the main challenges of todays' bank industry. It resulted in loss of billions of dollar and sometimes bank failures. Ethiopia has also faced payment frauds at different times sustaining loss of significant amount of money. It generally takes place in a financial system when safeguards and procedural checks are inadequate or when they are not scrupulously adhered to. Fraud reduces profitability of banks thereby affects the soundness of financial institutions as a whole.

Banks are under fiduciary obligation to protect money deposited in customer accounts. The contractual relationship between the banker and customer upon opening an account impose an obligation of KYC in order to identify for whom the former is giving service by using reliable, independent source documents, data or information. Thus, bank directors and its officers are required to carry-out their functions in safe and sound banking practice with all its fiduciary duty of care imposed by law. They are expected to discharge their duty in good faith with ordinary care and diligence as ordinarily prudent men would exercise in his own affairs.

There is no clear law that address liability of bank officer in payment frauds in Ethiopia. The fact that such liability has salient feature different from other liabilities incorporated in Ethiopian civil code necessitates enacting of special law striking the balance of many competing interests apparent in banking sector.

In payment fraud perpetrated through identity fraud, bank officers are liable when they failed to follow regular procedures stipulated by bank. Their liability arises when they failed to identify the identity of the person for whom they are making payment by asking their reliable documents capable of identifying their identity following regular and stipulated working procedure of banks.

Bank officers are also expected to exercise enhanced due diligence and additional identification documents when suspicious circumstances happen.

In cheque fraud, banks officers are held liable mostly when they are negligent in verifying the genuineness of the signature on the cheque. They should compare and verify the signature on the cheque and the specimen signature the drawer given to the bank. In electronic cheque, liability of banks and its officers should not be stretched to the extent that they should take extra-ordinary caution during payment of cheque using technologies that detect the cheque is forged as far as there is no apparent infirmity on the cheque. If banks make payment in due course believing in good faith under circumstances which do not afford a reasonable ground for believing that he is not entitled to receive payment of the amount therein, banks and bank officers should be exempted from liability.

Fund transfer letter fraud is one of the most common ways the fraudsters employ to achieve their criminal intent. This fraudulent act is perpetrated partly because the banking officers in discharge of their duty is negligent in verifying the person for whom they are paying. Practically, such fund transfer order fraud is associated with opening of fictitious account to which the transfer will be made by the fraudster before ordering such payment. Thus, if it is found that there is negligence on the part of the bank officer to verify identity of the customer upon opening the account to which the money is transferred or upon making payment, the bank officer will be held liable.

The liability of the bank in electronic payment fraud arises under strict liability if they fail to implement control procedures the situation demand or second under tort negligence where banks failed to exercise reasonable security standard and duty of care online baking deserves. Thus, in electronic payment fraud bank officers' liability is minimal except where there is disregard of already established security measures by bank or there is personal involvement of the officer in the perpetration of the act.

With regard to liability related with ATM fraud, the card holder is the only person who knows the PIN and it is entirely the fault of the card holder if such PIN is disclosed to third party. The card-holder is assumed to have complete control over the card and thus the card holder must have withdrawn the respective amount, or they permitted a third person so to do. Banks are held

liable in ATM fraud when it failed to deactivate the ATM after report of its loss is made. However, the possibility of bank officer to be held liable for ATM fraud is very rare save to exceptional situations where the circumstance warrant the officer disclosed the PIN of the customer upon issuance of card or where the latter failed to deactivate the ATM card after the loss of ATM is reported to him personally.

As far as special law addressing liability in bank industries are not enacted, the liability regime of banks and bank officers can be decided by using contractual and extra-contractual provisions. Bank officers are professionals and if they are negligent to follow working rules and procedures of banks thereby failed to discharge their professional duty, banks officers can be held liable.

Moreover, Bank officers are not fully aware of their obligations and liability when payment fraud occurs. Lack of clear law addressing the issue and failure of banks in giving consistent training on updated fraud prevention and detection techniques are the prominent lacunas to mention in Ethiopian banking industry. This has also increased the fraud risk in Ethiopian banking sector.

The practice in courts with regard to liability of banks in payment fraud is not consistent. Decisions given by same courts in similar cases are different. The binding decisions given in recent times by Cassation division of Federal Supreme Court indicates that banks are held liable when they pay money to the fraudsters without following regular working procedure stipulated by banks. However, this issue raises a lot of questions that worth detail analysis.

4.2. PROBLEMS FOUND (FINDINGS)

1. The researcher found that the main challenge with regard to liability of bank officer in payment fraud is lack of clear law addressing the subject-matter. There is no clear law in Ethiopia addressing what liability of bank officers is when payment fraud is committed through identity fraud, cheque fraud, Fund transfer Letter fraud, ATM fraud and E-payment fraud. Lack of clear law addressing this issue is one of the main reasons why decisions of courts are not becoming uniform or predictable. Moreover, limiting liability of banks to circumstances when banks failed to follow regular working procedure is not logical considering who is at better

position to avoid fraud and who is required to implement working procedures that best eliminates fraud.

2. Payment systems change faster than laws and regulations. Thus, there is lack of clearly stipulated obligation upon bank and bank officer that keeps pace with the change in technology and growth of using electronic payment systems. As the fraudsters develop more and more technology to overcome the security measures of banks, banks and its customers will be vulnerable to loss of their money. When banks develop one security measure, fraudsters develop counter technology or use its weakness to defraud banks.

3. Customers deposit money with trust that banks through its officers act prudently in managing and carrying out of affairs of the bank. The failure of the bank officer to discharge his obligation entails liability on the bank officer. On the other hand, making the officer liable for every negligence in exercise of his duty will tend the officers to escape this position. Bank officers also function their duty within limit of infrastructures supplied by the bank. Therefore, some of the payment fraud may be beyond the capacity of the bank officer to detect with available facilities at hand. On the other hand, making banks liable for each and every fraud may put the financial institutions at peril and greatly affect soundness of financial institutions. The use by fraudsters of latest technology to thwart the existing financial system of banks necessitates updating its fraud prevention and detection strategies with latest technology. If banks failed to install and supply technology, liability should be borne by banks which will otherwise make banks not to update their fraud prevention strategy. So, how to balance all these interests are challenging so that the interest of the customer, bank officer and that of the financial institution is not at stake.

4. The obligation of know your customer requires full awareness of what to do and what to require when giving service to customer. But the researcher found through an interview that not all employees have full awareness of such requirements and thus discharge their obligation accordingly in all dealings with their customer.

5. As sensitive personal information of customers are being hacked by fraudsters, the sufficiency of practice of authenticating a customer using only a user name and password is questionable when customers request access to their online bank account.

4.3. RECOMMENDATION.

1. Banking law has its own peculiar features. It must be governed by special law enacted considering all circumstances of the banking sector and the services it renders. Thus, clear law should be enacted indicating liability of bank officers when payment fraud is committed due to their failure to discharge their obligation of due diligence in verification of customers withdrawing money. With faster change in advance of technology, tailored laws that keep pace with fast changes in payment systems that require to protect the right of customers should be enacted.

2. Making banks and their officers liable for all payment fraudsters will bring great loss to the banking sector. On the other hand, customers who deposited their money in banks should get appropriate compensation for the loss of their deposit fraudulently. Thus, laws assigning liability on both banks and their officers that considers all these factors should be enacted.

3. Obligation and requirements of know your customer principle varies depending on the nature of fraud committed. Such requirements change from day to day with the change of technology to facilitate forging of documents and committing online frauds. Therefore, Guidelines Establishing Information Security Standards that set minimum standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information should be established. To this end, NBE in charge of regulation should issue directive necessitating the implementation of such guidelines in Ethiopian banks.

4. The degree of KYC required from bank officers differs in all type of fraud. Thus, the law should clearly specify what the liability of banks and/or their officers is in each type of fraud. Clear and updated KYC requirements should be implemented by banks on time. NBE should stipulate directive requiring approval of withdrawing money above a certain amount of money

before payment. Similarly, liability of bank officer in case transfer fund letter fraud is committed should consider whether the officer has cross-checked the signature on the letter and the specimen that exists, whether that fraud can be detected by checking the name of the organization, its logo, letterhead, stamp and other necessary details visible if due care is employed by the officer. In E-payment fraud, liability is mostly borne by bank, in contrast to the officer, due to the failure of the bank to introduce security measures of online users.

5. The issue of who should prove existence of liability and whether banks paid following regular working procedures stipulated by bank requires some sort of presumptions in favor of the customer. Thus, once the perpetration of payment fraud is proved, presumption should be taken as to negligence and banks alleging they committed no negligence should proof the contrary.

6. Authentication of online users by using user name and password is not enough in todays' world. The use of passwords should move to the use of multiple factors to authenticate users such as biometric measurement of the fingerprint or other biometric measurements, such as user authorization with an iris scan. The costs may be high – but safety, particularly in the electronic age, is worth its price. Moreover, banks should establish One time Password (OTP) that expires after few minutes in online payments. It should also introduce other verification methods such as sending password by text messages to phone number registered upon opening an account.

7. Banks should make further improvements to the security architecture of ATMs and POS terminals by providing an effective shielding of the number pads, video control, increased program code and internet safety. They should also replace traditional magnet strips by highly effective computer chips.

8. Prevention of frauds starts with identification of weakness in current systems of the organization. Thus, banks officers should be given quality training so that they get sound knowledge and understanding of banking practices and principles thereby prevent fraud. Banks should also arrange the means of upgrading the awareness of its customers regarding payment frauds and how they should protect themselves from such acts.

BIBLIOGRAPHY

Books

1. Bergman B, "E-fraud -state of art and counter measures" (2005)
2. Donald R. Cressey, Other people's money, (2013),
3. Shewangu Dzomira, Risk Governance and Control: Financial Market and Institutions,(2014) available at https:/www.researchgate.net
4. *Faisal Santiago, (2012) Pengantar Hukum Bisnis, Jakarta; Mitra Wacana Media, hal,*
5. *Kern A., Corporate Governance & Banking Regulation, (University of Cambridge 2004)*
6. Sandeap Dhameja, Kat Jacob, and Richard D.Porter, Clarifying Liability for Twenty First Century Payment Fraud, (Federal Reserve Bank of Chicago 2013),

Journals

1. Admasu Bezabeh & Asayehegn Desta, 'Banking Sector Reform in Ethiopia',International Journal of Business & Commerce, vol 3
2. Ashu Khanna and Bindu Arrora, International Journal of Business Science and Applied Management, Vol.4 (2009)
3. Bambore PL "Customer satisfaction and electronic banking service on some selected Banks in Ethiopia, International Journal of Research in Computer Application, (2013)
4. Bank director Liability, *The George Washington Law Review*, Vol **63:**
5. Cornell International Law Journal Volume 22
6. DePaul Business and Commercial Law Journal Volume 10, 2012
7. Digital Evidence and Electronic Signature Law Review, Vol 6
8. Gebrehiwot Ageba and Derk Bienen, (2008), Ethiopia's Accession to the WTO and the Financial Service Sector, Ethiopian Business Law Series, Faculty of Law, A.A., Vol.2

9. Gerwin Heyback, "Civil Law Liability for Unauthorized Withdrawal at ATM in Germany", Digital Evidence and Electronic Signature law Review, Vol. 6 (2009)
10. Joseph T. Wells, "Why Employee Commit Fraud", Journal of Accountancy, (2001)
11. Kanniainen, "Alternative for Banks to offer Secure Mobile Payments", International Journal of Bank Marketing, Vol. 28 no. 5 (2010),
12. Lina Fernandes, ''Fraud in E-Payment transactions; threats and Counter-measures" Asia Pacific Journal of Marketing and Management Review, Vol.2 (2013)
13. Owolabi.S.A."Fraud and Fraudulent Practices in Nigerian Banking Industry", An International Multi-Disciplinary Journal. Ethiopia, Vol.4 (2010), p.241
14. Rajev Saxena,"Cyber Laundering the Next Step for Money Launderers?", St. Thomas Law Review, Vol.10, (1998)
15. Sullivan, R.J, "The changing nature of U.S. card payment fraud: industry and public policy options", Economic Review, Vol. 95 No. 2, (2010)

Cases

1. Abebayehu Girma vs Dashen bank
2. Commercial Bank of Ethiopia vs Glory PLC (4-persons) Volume 12, file no. 41535
3. Dagima Bushura vs Awash International Bank
4. W/o Nejiha Dewale vs. Awash International Bank

Laws

1. CATS of CBE
2. Criminal code of FDRE,2004`,proclamation no. 414, Neg. Gaz.
3. Customer Due Diligence bank Directive, directive no. SBB/46/2010, National Bank of Ethiopia,
4. Ethiopian Civil Code
5. Global Bank Limited, Know Your Customer Policy, (Dec. 2006),
6. Licensing and supervision of banking Business Fraud Monitoring Directive, directive no. SSB/59/2014,National Bank of Ethiopia, art. 2.5
7. National payment system proclamation no. 718/2011

Reports

1. Australian Federal Police report of 2011

2. USA department of justice report

Interviews

1. Interview with undisclosed name, customer service officer at Awash Bank, April 5, 2021
2. Interview conducted with name undisclosed, service officer at commercial bank of Ethiopia, April 1, 2021
3. Interview with name undisclosed, customer service officer at Debub Global Bank, April 7, 2021