

This book analyzes the limits of e-banking regulations in Ethiopia. It addresses the key issues revolving around the limits of the e-banking regulation that are not responsive to the adoption and advancement of the e-banking products and services in the country: It explores and examines the policy, legal and institutional frameworks of the e-banking business in Ethiopia. Ethiopia does not have a comprehensive primary legislation that regulates the e-banking business, but many issues of the e-banking business are regulated by the National Payment System Proclamation and its implementing directives. But the current regulations provided by the National Payment System proclamation and its implementing directives are not full-fledged. Over that, the formulation of the national retail payment strategy which is used as a basis for both the legal and regulatory framework has not yet finished. The author recommends that it is through the primary legislation that the rights and obligation of citizens defined; therefore, instead of regulating by issuing directives, it is better to regulate the basic issues of the e-banking by a primary legislation.



Equbamariam Kidane is a lecturer at Assosa University, one of the public universities in Ethiopia. Before he joined to Assosa University, he was working as a Legal Contract Adviser in Ethiotelcom. He studied law (LLB) from Mekelle University School of Law. He specializes in Business and Corporate Law from Bahirdar University School of Law.



978-613-8-44582-1

**EUE** ÉDITIONS  
UNIVERSITAIRES  
EUROPÉENNES



Equbamariam Kidane Asegu

# The Limits of Electronic Banking Regulation in Ethiopia

**Equbamariam Kidane Asegu**

**The Limits of Electronic Banking Regulation in Ethiopia**



**Equbamariam Kidane Asegu**

**The Limits of Electronic Banking  
Regulation in Ethiopia**

**Éditions universitaires européennes**

**Imprint**

Any brand names and product names mentioned in this book are subject to trademark, brand or patent protection and are trademarks or registered trademarks of their respective holders. The use of brand names, product names, common names, trade names, product descriptions etc. even without a particular marking in this work is in no way to be construed to mean that such names may be regarded as unrestricted in respect of trademark and brand protection legislation and could thus be used by anyone.

Cover image: [www.ingimage.com](http://www.ingimage.com)

Publisher:

Éditions universitaires européennes

is a trademark of

International Book Market Service Ltd., member of OmniScriptum Publishing Group

17 Meldrum Street, Beau Bassin 71504, Mauritius

Printed at: see last page

**ISBN: 978-613-8-44582-1**

Copyright © Equbamariam Kidane Asegu

Copyright © 2018 International Book Market Service Ltd., member of  
OmniScriptum Publishing Group

**THE LIMITS OF E-BANKING REGULATION IN  
ETHIOPIA**

**EQUBAMARIAM KIDANE**

**December, 2018**

## **Acknowledgment**

All praise and thanks go to Almighty GOD, the source of all good knowledge and wisdom, strength and help without HIM it is impossible to breathe, let alone accomplish this work. GOD helps me by letting good people pass my way and support me throughout this work. Those people includes; my beloved father Kidane Asegu, my beloved mother Biriha Asgodom, my beloved wife Bire Kiros and my beloved daughter Selemawit Equbamariam. [My Family I love you all!]

Second, I want to acknowledge My Advisor Dr. Solomon Abay Yimer and those informants who were willing to participate in my interview and gave me important documents as well as information, specifically, Ato Ephirem Baraki, Ato Abenezet, Ato Solomon Damitew, Ato Kebede Demissie, Ato Temesgen Zeleke, Ato Fikiremarkos Abebe from NBE, Ato Damitew Weldekidan, Ato Mesfin Getachw, Ato Mintesinot Siyum, Ato Berihun Gebru, Ato Endalle Tessema, Ato Bahire Birhane, Ato Anteneh Gebriye and Ato Birhane G/cherkos from Commercial Bank of Ethiopia, Ato Elias Mitiku from Premier Switch Solution(PSS) and Ato Cherinet Kebede from Awash International Bank S.C. Finally, my dear friends Ghidey Belay also gave me constructive comment on draft proposal of this work.

## Table of Contents

CHAPTER ONE .....	1
INTRODUCTION .....	1
1.1 Background of the Study.....	1
1.2 Problem Statement.....	5
1.3 The objective of the study.....	5
1.3.1 General Objective .....	5
1.3.2 Specific objective.....	5
1.4 Research Questions .....	5
1.4.1 General Research question.....	5
1.4.2 Specific Research question .....	6
1.5 Significant of the Study.....	6
1.6 Literature Review.....	6
1.7 Research Methodology .....	9
1.7.1 Research Design: Population and Sample size .....	10
1.7.2 Data Types and Collection Tools for Empirical Part of the Study.....	10
1.7.3 Data Types and Collection Tools for Doctrinal Research Method .....	11
1.7.4 Data Analysis.....	11
1.8 The scope of the study .....	11
CHAPTER TWO .....	12
THE PRACTICE AND PROBLEMS OF E-BANKING IN ETHIOPIA .....	12
2.1 Introduction.....	12
2.2 The Practice of E-banking in Ethiopia.....	12
<b>2.2.1 The Current State of Non-Consumer E-banking</b> .....	13
<b>2.2.2 The Current State of Consumer E-banking</b> .....	14
<b>2.2.2.1 Automatic Teller Machine (ATM)</b> .....	15
<b>2.2.2.2 Point of Sale (POS) Terminal</b> .....	17
<b>2.2.2.3 Mobile Banking</b> .....	19
<b>2.2.2.4 Internet Banking</b> .....	21
<b>2.2.2.5 Mobile Wallet</b> .....	22
<b>2.2.2.6 Electronic Billing Presentment and Payment Business</b> .....	23
<b>2.2.2.7 Electronic Payment Instruments</b> .....	24
<b>2.2.2.8 Cheque Truncation</b> .....	26
2.3 Problems with Electronic Banking in Ethiopia.....	27
<b>2.3.1 Problems Related to Authentication Customer’s Authorization</b> .....	27
<b>2.3.2 Problems Related to Admissibility of E-banking Records</b> .....	28
<b>2.3.3 Problems Related to Confidentiality of Customer’s Financial Information</b> .....	29

2.3.4	Problems Related to Failure to Electronic Fund Transfer.....	30
2.3.5	Problems Related to Loss of Right to Countermand Payment .....	32
2.3.6	Security and Unauthorized Access to Customers' Account.....	33
2.3.7	Problems Related to allocation of Losses.....	34
2.3.8	Problems Related to Cross-Border E-Banking Transactions .....	35
2.3.9	Problems Related to Dispute Resolution.....	36
2.3.10	Problems Related to Non-financial Infrastructure .....	38
CHAPTER THREE .....		39
THE LIMITS OF REGULATION AND NEED FOR REFORM .....		39
3.1	Introduction.....	39
3.2	Constitutional Framework.....	39
3.3	Policy Framework: National Retail Payments Strategy.....	41
3.4	The Legal Framework of E-Banking Regulation in Ethiopia .....	44
3.4.1	Definition .....	46
3.4.2	Entry Regulation .....	48
3.4.2.1	Business Plan .....	49
3.4.2.2	Operational Policy and Procedure Manual .....	51
3.4.2.3	Risk Management Policy and Procedure.....	53
3.4.2.4	Information Security Policy .....	54
3.4.2.5	Consumer Protection Policy.....	56
3.4.2.6	Minute of the Board of Directors.....	56
3.4.2.7	Pilot Period Test .....	57
3.4.3	Operational Regulation .....	59
3.4.3.1	Terms and Conditions of the E-banking Service Agreements .....	59
3.4.3.2	Preauthorized Electronic Fund Transfer Services.....	65
3.4.3.3	Cheque or Other Paper Based Payment Instrument Truncation.....	66
3.4.3.4	Interoperability of E-Banking Products and Services.....	69
3.4.3.5	Privacy and Confidentiality of Customers' Accounts Information.....	72
3.4.3.6	Authentication of Electronic Banking Signatures.....	75
3.4.3.7	Admissibility of Electronic Banking Records.....	78
3.4.3.8	Irrevocability of Electronic Fund Transfer .....	80
3.4.3.9	Cross-Border E-banking Transactions .....	82
3.4.3.10	Fraud, Error and Improper Handling of Payment Instruments Related Liabilities 83	
3.4.3.11	Documentation and Periodic Statements of E-Banking Transactions .....	88
3.4.3.12	E-Banking Transaction Limits .....	89
3.4.3.13	Price Regulation .....	91
3.4.3.14	Competition Regulation.....	93

<b>3.4.3.15 Dispute Settlement System</b> .....	94
3.4.4 Exit Regulation .....	99
3.5 Regulatory Issues of E-Banking .....	100
3.5.1 National Bank of Ethiopia.....	100
3.5.2 National Payment System Council .....	104
CHAPTER FOUR.....	105
CONCLUSION AND RECOMMENDATION .....	105
5.1 Conclusion .....	105
5.2 Findings.....	109
5.2 Recommendation .....	112
Bibliography .....	116

## Acronyms

ACH	Automated Clearing House
ATM	Automated teller machine
BCBS	Basel Committee on Banking Supervision
BIS	Bank for International Settlements
CBE	Commercial Bank of Ethiopia
Draft Directive	Draft Electronic Funds Transfer Service Directive
EATS	Ethiopian Automated Transfer System
E-banking	Electronic banking
ECC	Ethiopian Chamber of Commerce
ECX	Ethiopian Commodity Exchange
EEPCo	Ethiopian Electric Power Corporation
EFT	Electronic Fund Transfer
EFTPOS	Electronic fund transfer at point of sale
ERCA	Ethiopian Revenue and Customs Authority
FDRE	Federal Democratic Republic Ethiopia
FIC	Financial Intelligence Center
HAC	Honor all cards
HPR	House Peoples' Representatives
I-banking	Internet banking
IMF	International Monetary Fund
INSA	Information Security Agency
ITU	International Telecommunication Union
KYC	Know Your Customer
M-banking	Mobile banking
MOFED	Ministry of Finance and Economic Development
NBE	National Bank of Ethiopia
NFIC	National Financial Inclusive Council
NFIS	National Financial Inclusive Strategy
NPSC	National Payment System Council
NPSP	National Payment System Proclamation
NRPSS	National Retail Payment System Strategy
PIN	Personal identification number

POS	Point of Sale Terminal
RTGS	Real Time Gross Settlement
TCCPA	Trade Competition and Consumer Protection Authority
WTO	World Trade Organization

## **Abstract**

*Generally, the Ethiopian e-banking is regulated by numerous legal documents such as the Constitution, Commercial Code, Civil Code, proclamations, regulations, directives, and circular letters. However, the main legislation which regulates the e-banking products and services is National Payment System Proclamation and its implementing directives.*

*This research analyzes the limits of e-banking regulations in Ethiopia. It addresses the key issues revolving around the limits of the e-banking regulation that are not responsive to the adoption and advancement of the e-banking products and services in the country: The research explores and examines the policy, legal and institutional frameworks of the e-banking business in Ethiopia. In doing this research, mainly empirical research has employed through qualitative research methodology.*

*The main finding of the research is that Ethiopia does not have a comprehensive primary legislation that regulates the e-banking business, but many issues of the e-banking business are regulated by the National Payment System Proclamation and its implementing directives. But the current regulations provided by the National Payment System proclamation and its implementing directives are not full-fledged, to this effect, one, this time, there is no regulation that regulates the allocation of losses that happened due to fraudulent and erroneous e-banking transactions. Two, the NBE has not adjudicative power emanated from a law, but in practice, the NBE is investigating and adjudicating e-banking cases upon the complaint of the customers. Third, the national payment system law mandates the government to organize a National Payment Council that advice the NBE, though the government has not yet established such council. Finally, the formulation of the national retail payment strategy which is used as a basis for both the legal and regulatory framework has not yet finished.*

*Based on the above finding the researcher recommends that first, it is through the primary legislation that the rights and obligation of citizens defined; therefore, instead of regulating by issuing directives, it is better to regulate the basic issues of the e-banking by a primary legislation and delegate to the regulator to issue directives for its detail regulation. The wide-ranging primary legislation must not only able to set the reciprocal rights and obligations of the customers and the banks, but also able to regulate the regulatory organ discretionary power. Second, the NBE needs also to formulate national retail payment strategy that is used as a basis for both the legal and regulatory frameworks. Finally, the government of Ethiopia should organize the National Payment System Council that advice the NBE on issues related to the national payment system.*

# CHAPTER ONE

## INTRODUCTION

### 1.1 Background of the Study

Banking has traditionally been established on the branch-banking model; they were giving services only using their branches and a person who has an account in one branch was not able to access banking services even within a different branch of the same bank. The unprecedented technological development in general and the birth of the internet, in particular, has changed the way banking services has been delivered for years. Nowadays, the success of a bank is measured against its innovation to deliver innovative products and services to their customers. Thus, banks are forced to introduce technologies in performing their day to day activities, and e-banking is one of the innovative services which enable the banks to provide banking products and services through electronic channels. It very hard to provide a clear-cut definition for e-banking because of the dynamic developments related with it, but the Basel Committee on Electronic Banking defines e-banking as the provision of retail and small value banking products and services using electronic channels.<sup>1</sup> Such products and services include deposit-taking, lending, account management, financial advice, electronic bill payment, and the provision of other electronic payment products and services such as electronic money.<sup>2</sup> Scholars also tried to define what constitutes e-banking and one of among the scholars Kilonzo defined e-banking or electronic fund transfer as the third and the advanced form of payment, the first being payment using fiat money (notes and coins) and the second paper-based payment instruments (commercial instruments).<sup>3</sup> E-banking is a subset of e-finance in which the traditional banking services are provided to customers using the electronic channels such as ATM, POS, internet, mobile phones, telephones, without presenting before the premises of the banks. A similar definition is given by the National Payment System Proclamation which includes e-banking with schemes of “fund transfer”. It thus defines “fund transfer” schemes;

... means any transfer of funds, either representing an order of payment or a transfer of money, which is initiated by a person by way of instruction, authorization or order to financial institution to debit or credit an account maintained with that financial institution and *includes point of sale*

---

<sup>1</sup> Risk Management Principles for Electronic Banking, Basel Committee at <[https://www.fsa.go.jp/inter/bis/bj\\_20010510a.pdf](https://www.fsa.go.jp/inter/bis/bj_20010510a.pdf)>4.

<sup>2</sup> Ibid.

<sup>3</sup> Zakayo Ndobir Lukumay, ‘An Analysis of the Legal Basis for Electronic Banking in Tanzania’ (Phd Dissertation, University of Dar es Salaam, 2011) 79.

*transfers, automated teller machine transactions, direct deposits or withdrawal of funds, transfers initiated by telephone, internet, card or other devices;*<sup>4</sup> [Emphasis mine].

As per the Proclamation, fund transfer service is the transfer, withdrawal or deposit of funds either using the traditional banking services or using the e-banking products and services. The italicized phrase mentioned in the indented paragraph indicates that banking products and services such as the deposit, withdrawal or fund transfer are possible using the electronic channels such as ATM, POS, internet, telephone, cards or any other electronic devices. The Proclamation equates e-banking with the transfer of funds using electronic channels and even by the actual definition given to ‘fund transfers’ in the Proclamation it includes both the deposit and withdrawal of funds using the electronic channels. But, the definition only allows the provision of deposit, withdrawal, and transfer of funds using the electronic channels the fourth service namely the lending service is not included in the definition.

Based on the methods of banking services delivery there are two broad forms of e-banking. The first is the provision of both traditional and modern banking services (e-banking products and services) at once: this type of banks is a traditional brick and mortar banks which also provides e-banking, brick and click banking services. All commercial banks of Ethiopia are traditional brick and mortar banks which combine the electronic delivery channels such as ATM, POS, mobile phones and the internet. The second way of delivery is ‘virtual bank’ which delivers banking products and services using electronic channels only and this type of bank is with no traditional brick and mortar services but only with brick and click banking services. In virtual banks all the banking services are only provided using the electronic channels even account opening is also made using the said channels; it is a bank with no branches made of premises at all. No virtual bank has not yet established in Ethiopia. Again, based upon the type of users e-banking is divided into two; consumer activated and non-consumer activated e-banking.<sup>5</sup> In non-consumers e-banking, it is the bank that activates the system whereas in consumer activated e-banking it is the consumers who activate the system and access the banking services using the electronic channels. Instead of categorizing as a consumer and non-consumer activated e-banking, the National Payment System Proclamation categorized the e-banking into two; ‘large value funds transfer system’ and ‘retail funds transfer system’.<sup>6</sup> As per the Proclamation, ‘large value fund transfer system’ is electronic fund transfer in which the amount/value of the transfer is considered as a large value by a

---

<sup>4</sup> National Payment System Proclamation No. 718/2011, Federal Negarit Gazzeta, 17<sup>th</sup> year No. 84, Art 2(13). [Herein after National Payment System Proclamation].

<sup>5</sup> Lukumay (n3) 80&306.

<sup>6</sup> National Payment System Proclamation, Art 2(14) & (22).

directive to be issued by the NBE and it consists of inter-bank funds transfer system, high priority and time-critical government fund transfers, clearing and settlement of securities of the government and any other fund transfer system prescribed by the NBE as a large value.<sup>7</sup> But, 'retail funds transfer system' is defined as a cheque clearing system administered by the NBE or by a person authorized by the NBE.<sup>8</sup> From the definition given by the Proclamation, 'large value fund transfer' equates to non-consumer-activated e-banking product and service whereas 'retail value fund transfer' equates to consumer-activated e-banking product and services. This Thesis is focused on consumer-activated e-banking products and services as opposed to non-consumer-activated e-banking products and services.

The introduction of technology is not an option to the traditional banks rather it is even an obligation that is imposed by the central banks of many countries including the National Bank of Ethiopia.<sup>9</sup> However, electronic banking is not without risks; it is disclosed to many risks including strategic, operational, legal and reputational risks.<sup>10</sup> Consequently, such risks associated with the electronic banking causes the loss of billions of dollars yearly.<sup>11</sup> To counter these problems the global community has been trying to deal with those risks by establishing international<sup>12</sup>, regional<sup>13</sup> and national legal and institutional framework that aims to ensure among other things secured, prudent and predictable e-banking services to the users. Not all countries are members or adhere the international standards, sound management principles, guidelines or model laws of e-banking regulation. For this reason, the regulation of the e-banking service is highly determined by national regulations; the national regulation determines the policy, legislative and regulatory framework of the e-banking regulation in general, and the entry requirement, prudential regulation, competition regulation, and consumer protection issues in particular.

---

<sup>7</sup> National Payment System Proclamation, Art 2(14).

<sup>8</sup> National Payment System Proclamation, Art 2(22).

<sup>9</sup> 'CBE's Core banking project to become operational' Capital (Addis Ababa, 18 March 2018) < <http://capitalethiopia.com/2012/01/09/cbes-core-banking-project-to-become-operational/#.Wq4dZZdRXWV> > accessed 18 March 2018

<sup>10</sup> See the Basel Committee on Banking Supervision identifies three main risks associated with the e-banking of 2003.

<sup>11</sup> Online fraud costs global economy many times more than \$100bn at <<https://www.theguardian.com/technology/2013/oct/30/online-fraud-costs-more-than-100-billion-dollars>> accessed 18 March 2018

<sup>12</sup> The Basel Committee on Banking Supervision adopted Fourteen Principles of Risk Management of Electronic Banking. Similarly, the OECD adopted in 2002 Guideline on the Security of Information Systems and Networks, IMF, UNCITRAL incorporates a model law for e-commerce law and e-signature, WTO.

<sup>13</sup> The Council of Europe Convention on Cyber Crimes Budapest Convention 23.11.2001.

In this regard, the drawback of the Ethiopian e-banking regulation has been a subject of an ongoing debate among policy makers, academicians, international organizations such as World Bank.<sup>14</sup> Despite the existence of abundant studies on the factors, challenges, opportunities of e-banking from another discipline such as economics and accounting, researches on the legal framework of e-banking and its limitations are scant. Generally, in Ethiopia, an array of public laws such as the Constitution, proclamations, regulations, directives, circular letters and some private laws are among legal frameworks that regulate the e-banking. Likewise, maintaining financial stability, economic growth and financial inclusiveness are the legally and boldly stated principal objectives of the national payment system law.<sup>15</sup> This objective of the national payment system is adhered by providing secured, safe and efficient financial infrastructure.<sup>16</sup> One may wonder whether Ethiopian policy, legislative and regulatory framework is working towards creating safe and efficient e-banking products and services. The National Payment Proclamation delegates the National Bank of Ethiopia to issue directives on various issues of the e-banking regulation including on the basic terms and conditions of the bank-customer agreement<sup>17</sup>, investigation and complaint handling procedure<sup>18</sup>, imaging of paper-based instruments and their processing<sup>19</sup>, the amount of ‘large value funds transfer system’<sup>20</sup>, designate payment instruments and determine the conditions, rules procedures and standards for the governance, operation and management of a system<sup>21</sup>, finality of payment systems<sup>22</sup>, criteria’s for appointment and tenure of external auditors<sup>23</sup>, dispute settlement system.<sup>24</sup> But, the NBE has not yet issued a directive for any of the mentioned matters with the exception of the directive issued for the regulation of mobile and agent banking. Therefore, what is the limits of the e-banking regulation in Ethiopia is an important concern of this study.

---

<sup>14</sup> The world Bank by assessment studies advises the Ethiopian government to issue adequate regulatory framework to achieve the financial inclusiveness strategy.

<sup>15</sup> See the preamble of the National Payment System Proclamation.

<sup>16</sup> Ibid.

<sup>17</sup> National Payment System Proclamation, Art. 19(3).

<sup>18</sup> National Payment System Proclamation, Art. 20(2).

<sup>19</sup> National Payment System Proclamation, Art. 24(5).

<sup>20</sup> National Payment System Proclamation, Art. 2(14).

<sup>21</sup> National Payment System Proclamation, Art. 4(2)(b)&(c)

<sup>22</sup> National Payment System Proclamation, Art. 14(3).

<sup>23</sup> National Payment System Proclamation, Art. 29(3).

<sup>24</sup> National Payment System Proclamation, Art. 31(4).

## **1.2 Problem Statement**

The provision of e-banking products and services has been escorted by a number of problems which are increasingly causing significant financial losses to the e-banking consumers. A few of the frequent problems are fraud, theft, and robbery of payment instruments which results in the unauthorized access of customer's account, failure to access and effect the transfer of funds due to technical imperfections, and erroneous electronic fund transfers. Over that, the Ethiopian e-banking business is accompanied by problems related to: authorization and authentication of customer's instruction, admissibility of e-banking records (e-evidence), absence of countermand for erroneous electronic fund transfers, confidentiality and privacy of critical financial information, and lack of adequate dispute resolution mechanism that protects the consumers of the e-banking.

Therefore, the need to explore the adequacy of the current e-banking regulation in regulating the aforementioned problems initiates me to conduct the study. Accordingly, this research analyzes the limits of the e-banking regulation in Ethiopia and thereby suggests appropriate policy and legal measures that could be taken by the government.

## **1.3 The objective of the study**

### **1.3.1 General Objective**

The main purpose of this research is to explore and analyze the limits of the current policies, laws, and practices of e-banking regulation in Ethiopia and suggest appropriate policy, legal and regulatory frameworks.

### **1.3.2 Specific objective**

1. To examine and analyze the practice and problems of e-banking business in Ethiopia.
2. To examine and analyze the limits of the current policies, laws, and practices in regulating e-banking business.
3. To initiate the possible policy, legal and regulatory remedies that the government should take to address the limits.

## **1.4 Research Questions**

### **1.4.1 General Research question**

What are the limits of e-banking regulation in Ethiopia?

### 1.4.2 Specific Research question

1. What are the practical problems of e-banking in Ethiopia?
2. What are the limits of the current policies, laws, and practices in regulating e-banking?
3. What should be done to address the limits of e-banking regulation in the country?

### 1.5 Significant of the Study

Commercial banks, government (regulatory authority) and customers of the commercial banks could be the direct beneficiaries of the research. Thus, the research is expected to benefit the government in evaluating the current policies, laws, and practices or implementing it in relation to e-banking regulation. Besides, the government will get an opportunity to identify the limits of the e-banking regulation that necessitates regulation. Secondly, the commercial banks are the beneficiary of this research as the limits of the current practices is identified and appropriate measures are initiated. Thirdly, consumers of e-banking so as to know the level of protection provided by the current legislative and regulatory framework and take precautionary remedies to the risks and liabilities associated with e-banking. The last but not the least is it will be as a source of knowledge for academicians and also used as a source of research to the coming researchers that want to make research with issues which are related with e-banking.

### 1.6 Literature Review

E-banking service is a new development in the banking business of the country. For this reason, so far there is no any research, article or book which studies the limits of the e-banking regulation in Ethiopia. But, this does not mean that there are no researches related to the e-banking service at all. There are significant researches made by non-lawyers; some of the researches and articles wrote by researchers and authors are stated here below.

The author Ato Kefeni Gurimu in his book ‘የባንክ ስራና ሕጎች’<sup>25</sup> explored and analyze the Ethiopian banking business and its laws. The author mainly analyzes the regulation of the traditional banking business but say a few about the limits of the e-banking products and services; he analyzed the drawback of the current regulation in relation to data protection of the consumers of e-banking and initiated a legislative response.<sup>26</sup> Outside of the data

---

<sup>25</sup> It is Amharic word and its translated meaning is ‘banking business and its laws’.

<sup>26</sup> Kefeni Gurmu, ‘የባንክ ስራና ሕጎች’ (Aster Nega Printing Press, September 2010) 11-18.

protection issues of the e-banking, he didn't say anything about e-banking regulation and its limits.

The second author who raised the issues of the e-banking regulation is Ato Gezu Ayele Mengistu: the author indicates that the recent terms and conditions of the e-banking agreements do not adequately protect the interest of the customers rather it gives a cumbersome to the customers, and as per the author this is happened due to the failure of the NBE to inspect the standard terms and conditions of the commercial banks of the e-banking service agreements.<sup>27</sup> Another issue that Ato Gezu raise is the inadequacy of the current legal framework in regulating erroneous electronic fund transfers, denial of e-banking transactions, the share of liability between banks and customers in cases of unauthorized withdrawals, and regulatory problems related to cross-border electronic fund transfer.<sup>28</sup> The book of Ato Gezu is not full-fledged; as it only raises few limits of e-banking regulation without making detail analysis and examination of the Ethiopian policies and laws and the international recommendations of e-banking that Ethiopia could take a lesson and over that he doesn't initiate appropriate legislative and regulatory frameworks for the limits he has already identified.

The researchers Kinfé Micheal Yilma and Halefom Hailu Abraha<sup>29</sup> studied the internet and regulatory response in Ethiopia. They review the current legal framework of internet regulation and initiate appropriate measures to fill the gap. The researchers examined the legal framework of the e-commerce, e-signature, cybercrime and the general outlook of the National Payment System Proclamation. But, the researchers don't say anything about the regulation of e-banking in the country.

Senait wondafrash Mulugeta<sup>30</sup> in her thesis studied the regulatory framework of the e-commerce and the lessons that could be taken from the ECX. But, she doesn't raise the regulation of e-banking services totally and even she does not say anything over the limits of e-banking regulation in Ethiopia.

---

<sup>27</sup>Ato Gezu Ayele Mengistu, 'የኢ.ጉ.ዩ.ጵ.ዩ የባንክ እና የሚ.ተ.ላለፉ የንግድ ሰነዶች', (Far East Trading PLC Press, 2009) 50.

<sup>28</sup>Gezu Ayele(n31)48-49.

<sup>29</sup> Kinfé Micheal Yilma *e tal*, 'The Internet and Regulatory Responses in Ethiopia: Telecoms, Cybercrimes, Privacy, E-commerce, and the New Media', Mizan Law Review, 2015, Vol. 9, No. 1.

<sup>30</sup> Senait Wondafrash Mulugeta, 'Regulating E-commerce in Ethiopia: Lessons from the Rules of Ethiopian Commodity Exchange' (LLM thesis, Addis Ababa University, School of Law, 2015). [Unpublished available at Addis Ababa University online research repository].

There are significant researches that are made by economists and accountants but neither of them tried to examine the legal issues of e-banking in Ethiopia. From among the researchers who make a study on e-commerce are Dr. Arun Korath and Dr. Sangheethan S.<sup>31</sup>, and in the article that they wrote together they tried to elaborate the reason why the consumers are not adoptive to the e-banking technologies. They studied the reasons behind the customers' failure to accept the e-banking products and services. Gardachew Werku<sup>32</sup> also studied the practice, opportunities, and challenges of e-banking service in Ethiopia. Similarly, Ayana Gemechu Bultum<sup>33</sup> identifies the factors that affect the adoption of the electronic banking system in Ethiopia. Wondwossen Tadesse and Tsegay G.Kidan studied the challenges and opportunities of the e-payment system; the researchers showed that there was no legal framework for both e-commerce and e-payment at the time where they made their study. And as per the information collected from the Justice and Legal Research Studies Institute by the said researchers, the reason for not adopting comprehensive legal framework is the inexistence of large pool of e-commerce activities (the research is undertaken in 2005); but six years later, in 2011, the country enacted a national payment system law that not only regulates the payment system but also includes significant provisions that regulate the e-banking business.

As it is mentioned in the above paragraphs, the examination and analysis of the above-named accountants and economists is based upon the factors, challenges, and opportunities of e-banking business, customer satisfaction issues of e-banking in terms the behavior of the customers and its effect to the operation of e-banking, not in terms of its legal and regulatory frameworks. Whatever the case, the researcher have assessed some thesis and articles which have included e-banking or e-payment in their title but their analysis and area of discussion is totally different and even not easy to understand it as they use economic models to make analysis and define the challenges and opportunities of e-banking, attitude of customers towards the e-banking service.

---

<sup>31</sup> Dr. Arun Korath and Dr. Sangheethan. S, 'A study on the Consumer Adoption Electronic Banking Technology with Reference to Ethiopian Banking sector' (April 2016) *International Journal of Science Technology and Engineering*, vol. 2, Issue 10.

<sup>32</sup> Gardachew Werku, *Electronic-Banking in Ethiopia- Practices, Opportunities and Challenges*, *Journal of Internet Banking and Commerce*, Vol. 15 No. 2 August 2010.

<sup>33</sup> Ayana Gemechu Bultum, 'Factors Affecting Adoption of Electronic Banking System in Ethiopian Banking Industry', *Journal of Management Information System and E-commerce*, Vol. 1, No. 1, 2014.

As aforementioned, so far there are no books, researches, and articles on the limits of e-banking regulation in Ethiopia. Even though I am not a hundred percent sure, I am the beginner in studying the limits of the Ethiopian e-banking regulation.

## 1.7 Research Methodology

The theme of the research is to explore the limits of e-banking regulation and initiate an appropriate policy, laws, and practices that addressed such limits. In order to achieve this purpose, it is important that an appropriate choice of methodology is made. The choice of the research strategy depends upon the purpose of the study. If the purpose of the study is to test variables and/or to generalize about a particular population quantitative research method is appropriate but where the purpose of the study is to make an in-depth explanation qualitative research method is employed. As it is mentioned in the above, the research is not to test a hypothesis based upon isolating variables rather the research is to make an in-depth study on the limits of e-banking regulation in Ethiopia, for this reason, qualitative research methodology is employed in conducting the research.

Once the researcher identified the research method, the next question is to choose an appropriate research type. There are three types of legal researches, namely doctrinal legal research, empirical legal research, and international and comparative legal research.<sup>34</sup> The doctrinal research, commonly called ‘black-letter’, aims to systematize, rectify and clarify the law on a particular topic by distinctive mode of analysis to authoritative texts that mainly consists of primary and secondary sources.<sup>35</sup> One of its leading assumptions is that “the character of the legal scholarship is derived from the law itself.”<sup>36</sup> Contrary to the doctrinal legal research, the empirical legal research studies the gap between the ‘law in books’ and ‘law in action’, and the operation of the law in society.<sup>37</sup> Unlike the two which are employed in studying domestic issues only, international and comparative legal research aims to facilitate the understanding of the operation of international public and private laws and legal systems and its impact in the formulation of domestic public policy and law in an era of global interdependence.<sup>38</sup> As it is mentioned in the above, the purpose of this research is to explore in-depth the limits of e-banking regulation in Ethiopia and recommend an appropriate

---

<sup>34</sup> Mike McConville and Wing Hong Chui, ‘Introduction and Overview’, in Mike McConville and Wing Hong Chui (ed(s)), *Research Methods for Law* (Edinburgh University Press Ltd, 2007)3.

<sup>35</sup> Mike McConville and Hong Chui (n38)3.

<sup>36</sup> Mike McConville and Hong Chui (n38)3.

<sup>37</sup> Mike McConville and Hong Chui (n38)3.

<sup>38</sup> Mike McConville and Hong Chui (n38)3.

policy, laws, and practices to address such limits. Thus, the research mainly employed empirical research method in examining the limits of the current policies, practices, and laws.

### **1.7.1 Research Design: Population and Sample size**

Since the purpose of the study is to explore the limits of e-banking regulation and initiate a remedy for it, the researcher employed a non-random purposive sampling technique in selecting key informants, laws, policy documents and literature for the purpose of data collection. For this reason, the researcher selected key informants from the National Bank of Ethiopia, officers of the operators of the payment infrastructure, consumers, merchants who use POS terminal to accept payment and officers of commercial banks according to their connection with the matter under investigation and purpose of the study. In addition to the non-purposive sampling method, the researcher also employed a snowball empirical data collection method to locate some of the key informants who have a knowledge on the topic being studied. In qualitative study, it is usually difficult, if not impossible, to determine the sample size in advance because the search goes on until the data is saturated or the point of redundancy. To the extent possible, the researcher tried to saturate empirically collected data.

### **1.7.2 Data Types and Collection Tools for Empirical Part of the Study**

The Researcher collected primary empirical data using semi-structured interview and focus group discussion. A semi-structured interview is preferred over structured because it is flexible and helps to explore things in detail. Again, a semi-structured interview is preferred from the unstructured interview because the former is less time consuming and more pre-planned than the latter. Thus, the researcher employed semi-structured interview because it is pre-planned and flexible which is adaptable to collect data used for empirical analysis. A semi-structured interview is employed with the careful and purposeful selection of the key-officers, legal practitioners, consumers and merchants who have the disclosure to know and appreciate the subject matter of the study. Focus group discussion is preferred to collect data's that individual interviewees cannot give; focus group discussion is employed with a careful and purposeful selection of the key-officers of the Commercial Bank of Ethiopia in light of the research objectives. The research also uses the researcher's experience as a user of ATM banking, M-banking and M-money services. And finally, document analysis through finding tools are employed for secondary data of the empirical study.

### **1.7.3 Data Types and Collection Tools for Doctrinal Research Method**

In doing the doctrinal research method, both primary and secondary data collected, consulted and analyzed. With regards to primary data, the research employed the World Bank National Retail Payments Strategy Consultative Report, Basel Risk Management Principles on Electronic Banking, UNCITRAL Legal Guide on Electronic Fund Transfer, UNCITRAL Model Electronic Commerce Law in 1996, UNCITRAL Model Electronic Signature Law in 2001, US Electronic Fund Transfer Act, Bangladesh Electronic Fund Transfer Act, and the policies, laws and regulations of the country. The study examined and analyzed the fairness of the standard terms and conditions of the e-banking service agreements and internal complaint handling procedures of all commercial banks of Ethiopia. Moreover, the study used secondary data's including brochures of the commercial banks, court decisions, books, official government reports, articles and senior thesis available in domestic and foreign literature in relation to e-banking regulation.

### **1.7.4 Data Analysis**

In the end, the researcher used a qualitative data analysis method for both primary and secondary data of the empirical part of the study, and it employed pure legal and documentary analysis to the 'black-letters' of the law (primary sources) and the secondary data of the doctrinal part of the study.

## **1.8 The scope of the study**

The study is concerned with the limits of e-banking regulation in Ethiopia; the policies, laws, and practices which regulates e-banking are explored and analyzed. The regulation of operators, non-financial institutions which are engaged in the provision of technological services to banks, and agent bankers (ordinary business persons which provides m-money services on behalf of the banks) are not included in the study.

# CHAPTER TWO

## THE PRACTICE AND PROBLEMS OF E-BANKING IN ETHIOPIA

### 2.1 Introduction

This chapter discusses the practice and problems of e-banking in Ethiopia. It is divided into two major parts, each contains sections and sub-sections: while part one deals with the practice of e-banking and part two examine the current problems of e-banking products and services in Ethiopia. Accordingly, it examines the various forms of e-banking products and services with their respective payment instruments and then it analyzes the practical problems of e-banking products and services in Ethiopia.

### 2.2 The Practice of E-banking in Ethiopia

With the development of new technologies, the way the banking products and services delivered is fundamentally changed, Ethiopia's banking sector has, therefore, had to deploy ICT and introduce a branch banking commonly called e-banking in order to meet the challenges of the day. Not only with the willingness to introduce the technology but also the National Bank by a directive mandates every commercial bank to introduce core banking technologies.<sup>39</sup> By now, all private and government-owned banks introduced different forms of e-banking products and services.<sup>40</sup> The entire operational bank branches in the country are inter-connected through core-banking systems and the inter-bank payment system, Ethiopian Automated Transfer System (ETATS).<sup>41</sup> Through the ETATS, by now, both consumer and non-consumer e-banking products and services are delivered by the commercial banks of the country. The next sub-sections discuss the practice of both consumer and non-consumer e-banking products and services.

---

<sup>39</sup> 2M editor, National Bank of Ethiopia Inaugurated New Core Banking System, 2Merkato.Com, at <<http://www.2merkato.com/news/alerts/2708-national-bank-of-ethiopia-inaugurated-new-core-banking-system>> accessed May 12, 2018.

<sup>40</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>41</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

## 2.2.1 The Current State of Non-Consumer E-banking

The National Bank of Ethiopia has made a number of initiatives towards modernization of payments and settlements systems.<sup>42</sup> As part of the modernization of the payment system, the National Bank of Ethiopia introduces a national payment and settlement system called ‘Ethiopian Automated Transfer System’ (ETATS) on June 07, 2011.<sup>43</sup> This payment and settlement system consists of Real Time Gross Settlement System (RTGS) and Automated Clearing House (ACH). RTGS is the electronic payment and settlement system for inter-bank transfers operated and owned by the National Bank of Ethiopia.<sup>44</sup> RTGS is an online real-time gross settlement system that processes high value and time-sensitive payment instructions among banks, government institutions and any other institution to be prescribed by the NBE.<sup>45</sup> Currently, this payment system is used mainly for interbank fund transfer as well as for government large value fund transfers. All banks of the country including the NBE have ‘payment and settlement account’ within the RTGS, and it is through this account that the large value interbank transfer is settled.<sup>46</sup>

With regard to electronic clearing system, the NBE has implemented the Automated Clearing House (ACH) system for the cheques clearing system as part of the RTGS.<sup>47</sup> ACH facilitates interbank electronic debit clearing processing by receiving electronic journals and generating settlement entries, netting, and other clearing reports.<sup>48</sup> The system further sends the settlement file through the VISA and MasterCard systems infrastructure to the RTGS for a final settlement in the members’ financial account.<sup>49</sup> ACH facilitates electronic credit clearing of high volume low-value interbank payments such as salaries and utility expenses.<sup>50</sup>

---

<sup>42</sup> See the minute of National Payment System Proclamation.

<sup>43</sup> Interview with Ato Solomon Damitew, Principal Manager Payment Systems Oversight and Development, National Bank of Ethiopia (Addis Ababa, 04 May 2018).

<sup>44</sup> Interview with Ato Solomon Damitew, Principal Manager Payment Systems Oversight and Development, National Bank of Ethiopia (Addis Ababa, 04 May 2018).

<sup>45</sup> National Payment System Proclamation, Art 2(14).

<sup>46</sup> Interview with Ato Solomon Damitew, Principal Manager Payment Systems Oversight and Development, National Bank of Ethiopia (Addis Ababa, 04 May 2018).

<sup>47</sup> National Payment System Proclamation, Art 2(22).

<sup>48</sup> Interview with Ato Solomon Damitew, Principal Manager Payment Systems Oversight and Development, National Bank of Ethiopia (Addis Ababa, 04 May 2018).

<sup>49</sup> Interview with Ato Solomon Damitew, Principal Manager Payment Systems Oversight and Development, National Bank of Ethiopia (Addis Ababa, 04 May 2018).

<sup>50</sup> Interview with Ato Solomon Damitew, Principal Manager Payment Systems Oversight and Development, National Bank of Ethiopia (Addis Ababa, 04 May 2018).

This payment system is processed at the Automated Clearing House electronically and settled through the bank's 'payment and settlement account' held at the NBE.<sup>51</sup>

On clearance of card-based transactions, there are currently two prominent inter-bank retail payment card switches. These are the visa-based member domestic transaction switch known as EthSwitch and the Premier Switch Solutions.<sup>52</sup> EthSwitch is a company formed by the contribution of all Ethiopian banks, and it has also the backing of the Ethiopian Bankers' association and the NBE.<sup>53</sup> EthSwitch makes the Ethiopian e-banking products and service to be interoperable, and the interoperability of the payment systems enables the customers to access financial services via all ATM and POS terminals that are found in the country regardless of their home bank.<sup>54</sup> The system of the EthSwitch is linked to the Ethiopian Automated Transfer System which comprises the Real Time Gross Settlement and Automated Clearing House to facilitate efficient clearing and settlement of all transactions.<sup>55</sup> But, the Premier Switch Solution (PSS) is owned by a consortium of six banks; United Bank, Awash International Bank, Nib International, Berhan International Bank, Addis International Bank and Cooperative Bank of Oromia.<sup>56</sup> While EthSwitch facilitates the clearing of interbank card transactions of all Ethiopian banks, but PSS facilitates the clearing of the interbank card transactions of the six-member banks.<sup>57</sup> The National Bank of Ethiopia provides final settlement service to members of these switches through 'Payment and settlement account' held at the National Bank.<sup>58</sup>

## 2.2.2 The Current State of Consumer E-banking

By now, the Ethiopian banks provide four forms of electronic banking: ATM banking, mobile banking, POS banking, and Internet banking. Over that, the banks are providing

---

<sup>51</sup> Interview with Ato Solomon Damitew, Principal Manager Payment Systems Over Sight and Development, National Bank of Ethiopia (Addis Ababa, 04 May 2018).

<sup>52</sup> Interview with Ato Solomon Damitew, Principal Manager Payment Systems Over Sight and Development, National Bank of Ethiopia (Addis Ababa, 04 May 2018).

<sup>53</sup> 'EthSwitch, BPC Partner to Create National Switch Infrastructure for Ethiopia', <<https://www.atmmarketplace.com/news/ethswitch-bpc-partner-to-create-national-switch-infrastructure-for-ethiopia/>>, accessed 12 May 2018.

<sup>54</sup> Interview with Ato Elias Mitiku, Unit Head of Clearing and Settlement, Premier Switch Solution (Addis Ababa, 12 August 2018).

<sup>55</sup> Interview with Ato Elias Mitiku, Unit Head of Clearing and Settlement, Premier Switch Solution (Addis Ababa, 12 August 2018).

<sup>56</sup> See the official website of Premier Switch Solutions. < <http://www.psethiopia.com/> >. [Last accessed May 12, 2018].

<sup>57</sup> Interview with Ato Elias Mitiku, Unit Head of Clearing and Settlement, Premier Switch Solution (Addis Ababa, 12 August 2018).

<sup>58</sup> Interview with Elias Mitiku, Unit Head of Clearing and Settlement, Premier Switch Solution (Addis Ababa, 12 August 2018).

electronic bill presentment and payment services to their customers. Besides, the banks provide e-banking products and service to their customers through agent banking arrangement. The practices of the consumer-based e-bankings are discussed in the next sub-sections.

### **2.2.2.1 Automatic Teller Machine (ATM)**

By now, all government and privately owned commercial banks have ATMs which enables their customers to withdraw cash, check balances, and/or transfer funds between accounts.<sup>59</sup> As of March 31, 2018, the total number of ATM deployed in the country is 3,111.<sup>60</sup> Out of these ATMs, 54% belongs to the Commercial Bank of Ethiopia, Dashen Bank, Awash Bank and Wegagen Bank shares 9%, 9% and 6% of the total ATMs respectively.<sup>61</sup> The number of ATMs of Debut Global Bank, Enat Bank, and Abay Bank is very low and insignificant.<sup>62</sup> ATM banking services are unevenly distributed among regions. Most of the ATMs are located in Addis Ababa and other major cities of the country: out of the total ATMs 41.1% are concentrated in Addis Ababa and followed by Oromia and Amhara regions which have a share of 21% and 12% respectively.<sup>63</sup> ATMs distribution in Gambella, Benshangul Gumuz and Harari is insignificant.<sup>64</sup>

ATM banking requires the use of a magnetically encoded plastic card and a validation code, or personal identification number (PIN). The customer inserts the card into the computer terminal(ATM), punches in the PIN sequence, and then instructs the computer (ATM) to complete the desired banking transaction; the customer's account is immediately debited for cash withdrawal, or for fund transfer and is credited with any deposit. The customer has access to the bank services twenty-four hours a day and seven days a week through the ATM terminal.

As far as the sharing of payment systems is concerned the banking industry in Ethiopia has shown its maturity by effectively cooperating in implementing shared ATMs and POS terminals. In May 2016, a consortium of 17 local commercial banks formally signed off to implement a shared switch infrastructure for clearing of their card transactions known as EthSwith.S.C. Since that time, all debit cardholders of Ethiopian banks are able to reap the

---

<sup>59</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>60</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>61</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>62</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>63</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>64</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

advantages of the interoperability of the e-banking products by having convenient services while using any ATM of the members of the consortium. This was made possible by the cooperation of the commercial banks in Ethiopia, having informed of the need to optimize customers outreach and creating convenient banking services.

As far as the cross-border issues of ATM banking are concerned, the ‘Dollar Account’ holders of Ethiopian banks can access banking services using the foreign bank’s ATM terminals outside of the Ethiopian territory.<sup>65</sup> The persons allowed to have a ‘Dollar Account’ are very limited and includes exporters, government top officials, Ethiopian diaspora and diplomatic communities.<sup>66</sup> Those dollar account holders have debit cards which can enable them to access banking transactions outside of Ethiopia. They can withdraw or transfer funds up to \$400 per day.<sup>67</sup> The withdrawal or fund transfer made by the dollar account holders outside of Ethiopia is settled from the collateral account of the Ethiopian banks opened usually in the European and American banks.<sup>68</sup> But this does not mean that the Ethiopian banks cannot access dollars outside of Europe and America, they can access any foreign currency so far as the banks have a collateral account and the arrangement to enable the dollar account holders to access foreign currency in their ATM terminals.<sup>69</sup> The Ethiopian banks have a collateral account in many countries including European and American banks, this collateral account is usually called ‘Vostro maestro account’.

Similarly, the VISA and Master cardholders of any foreign country can; withdraw cash, make bill payments, forex, fund transfer, and balance inquiry through the ATMs terminals owned by the Ethiopian banks within Ethiopian territory.<sup>70</sup> The e-banking transaction which is made using the VISA and Master card is very complex and it passes many steps for settlement. The banking transaction done using the VISA and Master cards is real electronic transaction and the account of the cardholder is debited automatically when he/she orders any e-banking

---

<sup>65</sup> Interview with Ato Berihu Gebru, Business support Officer, Commercial Bank of Ethiopia (Addis Ababa, 12 May 2018).

<sup>66</sup> Interview with Ato Berihu Gebru, Business support Officer, Commercial Bank of Ethiopia (Addis Ababa, 12 May 2018).

<sup>67</sup> Interview with Ato Berihu Gebru, Business support Officer, Commercial Bank of Ethiopia (Addis Ababa, 12 May 2018).

<sup>68</sup> Interview with Ato Berihu Gebru, Business support Officer, Commercial Bank of Ethiopia (Addis Ababa, 12 May 2018).

<sup>69</sup> Interview with Ato Berihu Gebru, Business support Officer, Commercial Bank of Ethiopia (Addis Ababa, 12 May 2018).

<sup>70</sup> Focus group discussion with Ato Birhane Gebrecherkos, Ato Berihu Gebru, Ato Endalle Tessema, Ato Bahire Birhane and Ato Anteneh Gebriye, Commercial Bank of Ethiopia (Addis Ababa, 12 May 2018).

transaction using the ATM terminals.<sup>71</sup> Once the VISA or Master cardholder makes e-banking transaction using the ATM terminals owned by the Ethiopian banks, the e-banking transactions of the cardholder are collected from the merchants and then transferred to VISA and Master cards for settlement.<sup>72</sup> And the VISA and Master cards settled by hard currency for any amount of money withdrawn by their customers within Ethiopian banks.<sup>73</sup> Similar to the above-mentioned for dollar accountholders, the foreign banks credited the collateral account of the Ethiopian banks for the amount of money withdrawn by their customers within Ethiopia.<sup>74</sup>

### **2.2.2.2 Point of Sale (POS) Terminal**

As it is mentioned in the introduction part of this Thesis, the point of sale terminal is an electronic device where buyers usually use as a means of fund transfer in exchange of the goods and services delivered or provide by the merchants. But sometimes where the ATM terminal fails, the banks allow their customers to withdraw cash by first printing a cash-withdrawal slip using the POS terminal. Similar to the ATM terminal which is mentioned in the above, POS terminal require the use of a magnetically encoded plastic card and a validation code, or personal identification number (PIN). The consumer inserts the card into the computer terminal, punches in the PIN sequence, and then instructs the computer to complete the fund transfer. The consumer's account is immediately debited for the amount of the fund transfer he/she made and the merchant's account is credited with the same amount. The consumer has access to the POS terminal so far as the business premises of the merchants are opened.

Coming to the Ethiopian case, all the debt or prepaid cardholders of Ethiopian banks can use the POS terminals to buy any product or services using their card so far as the merchant has POS terminal in his/her business premises.<sup>75</sup> Similar to what has been already stated in ATM

---

<sup>71</sup> Focus group discussion with Ato Birhane Gebrecherkos, Ato Berihu Gebru, Ato Endalle Tessema, Ato Bahire Birhane and Ato Anteneh Gebriye, Commercial Bank of Ethiopia (Addis Ababa, 12 May 2018).

<sup>72</sup> Focus group discussion with Ato Birhane Gebrecherkos, Ato Berihu Gebru, Ato Endalle Tessema, Ato Bahire Birhane and Ato Anteneh Gebriye, Commercial Bank of Ethiopia (Addis Ababa, 12 May 2018).

<sup>73</sup> Focus group discussion with Ato Birhane Gebrecherkos, Ato Berihu Gebru, Ato Endalle Tessema, Ato Bahire Birhane and Ato Anteneh Gebriye, Commercial Bank of Ethiopia (Addis Ababa, 12 May 2018).

<sup>74</sup> Focus group discussion with Ato Birhane Gebrecherkos, Ato Berihu Gebru, Ato Endalle Tessema, Ato Bahire Birhane and Ato Anteneh Gebriye, Commercial Bank of Ethiopia (Addis Ababa, 12 May 2018).

<sup>75</sup> Interview with Ato Elias Mitiku, Unit Head of Clearing and Settlement, Premier Switch Solution (Addis Ababa, 12 August 2018).

banking, the POS terminals of every Ethiopian bank are interoperable.<sup>76</sup> The interoperability of the ATM and POS terminals is operated by the same company, EthSwitch S.C.<sup>77</sup>

As of March 2018, 9,502 POS terminals are deployed by Ethiopian banks.<sup>78</sup> Not all banks deployed POS terminals; only ten banks deployed POS terminals, and these are Commercial Bank of Ethiopia, Dashen Bank, Awash International Bank, Wogagen Bank, Bank of Abyssinia, United Bank, Nib International Bank, Lion International Bank, Berhan Bank, and Abay Bank.<sup>79</sup> Similar to the ATM terminals, the POS terminals are concentrated in Addis Ababa and major cities of the country.<sup>80</sup> But despite its variation in volume, POS terminals are deployed in all regions.<sup>81</sup> Out of the deployed POS terminals, 70% are located in Addis Ababa, and Oromia and Amhara Regions followed Addis Ababa by 10.7% and 8.5% shares respectively.<sup>82</sup> A very limited number of POS terminals located in Somalia, Harari, Afar, and Benshangul Gumuz which are deployed by the Commercial Bank of Ethiopia. In relation to this, out of the above-mentioned POS terminals 7,449 are located at merchant sites; the left 2,053 are used by the banks themselves.<sup>83</sup> Out of the total number of merchants, 76% belongs to CBE, whereas, 12% belongs to Dashen Bank, and the other eight banks share 12% of the merchants together.<sup>84</sup> With regard to the concentration of the merchants, 78% of the merchants who have POS terminal in their business premises are located in Addis Ababa and the left 22% are outside of Addis Ababa.<sup>85</sup>

With regard to cross-border issues of POS terminals, the ‘Dollar Account’ holders of Ethiopian banks can access POS terminals owned by foreign banks outside of the Ethiopian territory.<sup>86</sup> They can transfer funds through the POS terminals up to 400 dollars per day.<sup>87</sup> But, this is possible only when there is an agreement in relation to the access of the POS terminals owned by the foreign banks, currently, the Ethiopian banks have an agreement with

---

<sup>76</sup> Interview with Ato Elias Mitiku, Unit Head of Clearing and Settlement, Premier Switch Solution (Addis Ababa, 12 August 2018).

<sup>77</sup> Interview with Ato Elias Mitiku, Unit Head of Clearing and Settlement, Premier Switch Solution (Addis Ababa, 12 August 2018).

<sup>78</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>79</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>80</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>81</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>82</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>83</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>84</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>85</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>86</sup> Interview with Ato Berihu Gebru, Business support Officer, Commercial Bank of Ethiopia (Addis Ababa, 12 May 2018).

<sup>87</sup> Interview with Ato Berihu Gebru, Business support Officer, Commercial Bank of Ethiopia (Addis Ababa, 12 May 2018).

VISA and Master Card companies.<sup>88</sup> Similar to what is stated in the ATM banking, the fund transfer made by the dollar account holders outside of Ethiopia is settled from the collateral account of the Ethiopian banks opened in the foreign banks; usually in the European and American banks.<sup>89</sup> Similarly, the VISA and Master cardholders of any foreign country can transfer funds through POS terminals owned by the Ethiopian banks within Ethiopian territory. The fund transfer order made through the POS terminal using VISA and Master Card as a payment instrument is a real electronic transaction and the account of the cardholder is debited automatically. Once the VISA or Master cardholder transfer fund to the merchants through the POS terminal, the merchant sent the batch to the banks, and the banks by collecting the batch credited the account of merchant by the said amount and the banks send the batch electronically to VISA and Master cards for settlement and finally VISA and Master Cards credited the Ethiopian bank's collateral account by the same amount.

One more thing in relation to POS terminal is the existence of offline transaction, the VISA or Master cardholder call to Ethiopian merchants being outside of Ethiopia and orders the merchant to make a payment to a third party or hold a bed for him/her or to a third party.<sup>90</sup> In doing so, the cardholder informs the details of the card; the issuer of the card, the card number, expiry date, and others.

### **2.2.2.3 Mobile Banking**

Mobile banking is one form of e-banking which is provided by a bank or other financial institution that allows its customers to conduct financial transactions remotely using mobile devices such as mobile phones, smartphones, and tablets with a SIM.<sup>91</sup> 'Mobile banking' is the provision of banking products and services using mobile devices but 'mobile money' is money which is stored in the mobile phone and which can be used to make payments to third parties.<sup>92</sup> Mobile money (mobile payment) is a payment service operated under the financial regulatory framework and performed from or via a mobile device.<sup>93</sup> In mobile banking, there

---

<sup>88</sup> Interview with Ato Berihu Gebru, Business support Officer, Commercial Bank of Ethiopia (Addis Ababa, 12 May 2018).

<sup>89</sup> Interview with Ato Berihu Gebru, Business support Officer, Commercial Bank of Ethiopia (Addis Ababa, 12 May 2018).

<sup>90</sup> Interview with Ato Berihu Gebru, Business support Officer, Commercial Bank of Ethiopia (Addis Ababa, 12 May 2018).

<sup>91</sup> 'Mobile Banking', Wikipedia, at < [https://en.wikipedia.org/wiki/Mobile\\_banking](https://en.wikipedia.org/wiki/Mobile_banking) > accessed 20 March 2018].

<sup>92</sup> Ibid.

<sup>93</sup> 'Mobile Payment', Wikipedia, at < [https://en.wikipedia.org/wiki/Mobile\\_payment](https://en.wikipedia.org/wiki/Mobile_payment) > accessed 20 March 2018.

is the opening and maintenance of ‘mobile account’ at financial institution whereas in mobile money it is a stored-value prepaid payment mechanism.

Banks and microfinance institutions in Ethiopia has begun providing mobile banking services since 2015.<sup>94</sup> Compared to other African nations, Ethiopian financial institutions were very late to introduce the mobile banking services.<sup>95</sup> In bank-led mobile banking, banks and microfinance make use of mobile phones to reach many customers as an extension of their services and products. With mobile banking, a customer can access banking services from any corner of the country at any time using his/her mobile phone. The available mobile banking services include balance inquiry, transaction details, payment of utility bills, bank statement, intra-account transfers, inter-account transfers and alerts for withdrawal on a customer account.<sup>96</sup> The government-owned giant bank, CBE, launched mobile banking service on December 11, 2017, after it has passed the pilot period provided in the Regulation of Mobile and Agent Banking Service Directive.<sup>97</sup> Using the mobile banking service of the CBE, a customer can deposit, withdraw, transfer money, make payments, buy mobile airtime and pay the bill in a very simple and convenient way.<sup>98</sup>

Currently, ten banks are offering mobile banking services. Similar to other delivery channels, CBE dominates the mobile banking services.<sup>99</sup> However, the number of mobile banking subscribers of the other banks is also increasing.<sup>100</sup> As of March 2018, there were 2,745,716 mobile banking subscribers.<sup>101</sup> Despite the variation in the number of subscribers, mobile banking is delivered in all regions of the country. Addis Ababa, Oromia, Amhara, and SNNP share the largest number of mobile banking subscribers.<sup>102</sup> Unlike the other delivery channels, the distribution of mobile banking users is fair among regions.<sup>103</sup>

---

<sup>94</sup> Alemayehu Bacha, ‘Ethiopia Commence Mobile Banking Service’, 05 February 2015, at <<http://www.2merkato.com/news/alerts/3563-ethiopia-commence-mobile-banking-service>> accessed 19 March 2018.

<sup>95</sup> Alemayehu Balcha(n98).

<sup>96</sup> See the official website of the CBE and other privately-owned commercial banks.

<sup>97</sup> Biniam, ‘CBE Launches Mobile Money Platform’, 2018. <<http://www.combanketh.et/More/CBENews.aspx?p=articles&news=86&title=CBE%20launches%20mobile%20money%20platform>> accessed 19 March 2018.

<sup>98</sup> Biniam(n101).

<sup>99</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>100</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>101</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>102</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>103</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

### 2.2.2.4 Internet Banking

In Ethiopia, e-banking has been around for quite some time in the form of ATMs and mobile phones. In more recent times, it has added a new delivery channel called internet banking which has facilitated banking transactions for both customers and banks. This new delivery channel, internet banking, is at an infant stage with a very small number of customers compared to the other forms of e-banking.<sup>104</sup> For the customers, internet banking offers fast and more convenient banking products and services which is available around the clock irrespective of the customer's locations.<sup>105</sup> And for banks, it is much more efficient and cost-saving channel.<sup>106</sup>

As it is stated in the above, internet banking is in its infant stage and by March 2018, only 98,187 customers subscribe to use Internet banking.<sup>107</sup> Due to its dependency on the non-financial infrastructure particularly internet connection, Internet banking is not a widely used payment channel.<sup>108</sup> The internet banking users show many ups and downs, in the second quarter of 2017/2018, the number of Internet banking users decreased due to the removal of the inactive internet banking users of the CBE.<sup>109</sup> However, the number of Internet banking users increased by March 2018 by 10,592.<sup>110</sup> Commercial Bank of Ethiopia launched internet banking in June 2012.<sup>111</sup> Through the Internet banking, CBE offers the fastest and more convenient banking services including: viewing account balances and transactions; making fund transfers between a customer's own current and saving accounts; effecting payments to third parties, including bill payments to predefined CBE customers within Ethiopia; viewing and downloading current and saving account statements; requesting for stop payment on cheques; and applying for letter of credit.<sup>112</sup> A few other banks that provide internet banking include Dashen Bank, Awash International Bank, Wegagen Bank, and Zemen Bank.<sup>113</sup>

---

<sup>104</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>105</sup> Rupa Rege Nitsure, 'E-Banking: Challenges and Opportunities', *Economic and Political weekly*, 2003, Vol. 38, No. 51/52, PP. 5377-5381, p. 5377. < <http://www.jstor.org/stable/4414436> > accessed 19-04/2018.

<sup>106</sup> Nitsure(n109)5377.

<sup>107</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>108</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>109</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>110</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>111</sup> Meron Teklebirhan, 'Commercial Bank of Ethiopia Launches E-banking', online, 2Merkato.com. <<http://www.2merkato.com/news/banking-and-finance/1345-commercial-bank-of-ethiopia-launches-e-banking>>

<sup>112</sup> 'Internet Banking', <<http://www.combanketh.et/EPayment/InternetBanking.aspx> > [official website of CBE].

<sup>113</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

### 2.2.2.5 Mobile Wallet

The mobile wallet is a new mobile money that customers access banking services mainly deposits, withdrawal, and payments. Despite problems in relation to the provision of the services, the mobile wallet services are increasing from time to time. Currently, out of the seventeen banks, only nine banks are providing mobile wallet services to their customers.<sup>114</sup> In Ethiopia, there are two operators which provide an operating system to the mobile wallet services provided by the financial institutions; Netherland-based BelCash, and the Ireland-based MOSS ICT.<sup>115</sup> The mobile wallet service provided by BelCash is branded as ‘HelloCash’ whereas the mobile wallet service provided by MOSS ICT is branded as ‘M-Birr’.<sup>116</sup> It is through the agent bankers that the mobile wallet account is opened.<sup>117</sup> Again, the deposit, withdrawal, and transfer of funds of the mobile wallet are done by the agent bankers.<sup>118</sup>

The mobile wallet is different from mobile banking, mobile banking is the provision of banking services through mobile phones, whereas, a mobile wallet is a form of mobile money in which the money is stored in the mobile phone of the person. In mobile banking, the balance is kept in the financial account of the person held in the financial institutions, whereas, the balance of the mobile wallet is kept in the SIM of the mobile phone, no financial account in mobile wallets.<sup>119</sup> Like the balances of mobile airtime, the balances of the mobile wallet are within the SIM. Mobile banking can be provided only by financial institutions, whereas, the mobile wallet can be provided including by non-financial institutions. The mobile wallet is the digitalization of the user’s physical wallet onto a mobile device.<sup>120</sup> In the mobile wallet, the operator of the mobile payment platform could be deemed to be receiving

---

<sup>114</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>115</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>116</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>117</sup> Interview with Ato Berihu Gebru, Business support Officer, Commercial Bank of Ethiopia (Addis Ababa, 12 May 2018).

<sup>118</sup> Interview with Ato Berihu Gebru, Business support Officer, Commercial Bank of Ethiopia (Addis Ababa, 12 May 2018).

<sup>119</sup> Interview with Ato Berihu Gebru, Business support Officer, Commercial Bank of Ethiopia (Addis Ababa, 12 May 2018).

<sup>120</sup> Niels Vandezane, Mobile Wallets and Virtual Alternative Currenmcies under the EU Legal Framework on Electronic Payments, Interdisciplinary Center for Law and ICT, KU Leuven, ICRI Working Paper 16/2013. At <<https://www.law.kuleuven.be/icri/>>[Last accessed April 11, 2018].

money in the form of payment information from the buyer for the sole purpose of delivering it to the merchant seller.<sup>121</sup>

The other mobile money which can be transferred from the holder to the third party using the mobile phone is the mobile airtime issued by Ethio telecom, a giant and monopole government-owned telecom company engaged in the provision of telecom services in Ethiopia. Ethio telecom issued five stored-value cards valued Birr 5, 10, 15, 50 and 100. The customers of the company buy these stored value cards mainly for mobile airtime but once customers credited their mobile phones, they can also transfer the mobile airtime to their friends (either for free or for payment) or buy professional advice, make donation to the Renaissance Dam, make donation to ‘Macedonia’, or participate in any games of chance using the mobile money. The minimum and maximum mobile airtime value that can be transferred by the customers of Ethio telecom is Birr 5 and 1000 respectively.<sup>122</sup> Unlike, the mobile wallet in which the balances of the customer are kept in the data centers of the financial institutions, the balances of mobile money are in the operating system of the telecom company, Ethio telecom. The Thesis revolves on the limits of the e-banking regulation; thus, the mobile money is beyond the scope of this study.

#### **2.2.2.6 Electronic Billing Presentment and Payment Business**

Electronic billing presentment is the process through which bills are delivered electronically to the consumers, who can then pay the bill using different electronic channels including using e-banking products and services. Each time, usually each month, the customer reviews the bill and makes a payment to it. There are three steps in electronic bill presentment: service initiation-enrollment into the service, presenting the bill or invoice, and making the payment.<sup>123</sup>

The electronic bill presentment and payment may be done using banks and non-bank payment service providers. In Ethiopia, both banks and non-banks participate in the electronic bill presentment and payments. A good example of non-bank electronic bill presentment and payment service is provided by Kifiya Lehulu. Kifiya, in association with

---

<sup>121</sup> Kevin V. Tu, ‘Regulating the New Cashless World’, University of New Mexico School of Law, thesis, February 18, 2013.

<sup>122</sup> See the application developed by Ethio telecom, named ‘ethio Self-Care’, (Click the application, select the ‘Information’, select ‘credit transfer’ and finally click ‘Service Description’.)

<sup>123</sup> Paul A. Murphy, ‘Current Issues: Electronic Bill Presentment and Payment: An Efficient opportunity for Utilities and Consumers’, American Water Works Association, Vol. 95, No. 8, August 2003, PP. 28-33. P. 28. <<http://www.jstor.org/stable/41311539>>. [Accessed 19-04-2018]

the Ministry of Communication and Information Technology, launched electronic bill presentment and payment system in February 2013.<sup>124</sup> It provides bill payment services to three utilities; namely, water, electricity, and telephone at 34 centers.<sup>125</sup> The regulation of non-bank bill payment service provides is outside of the study. In addition to the services provided by Kifiya Financial Technologies, currently, the Ethiopian commercial banks are engaged in the provision of electronic bill payment services. In dead, the electronic bill payment service is in its infant stage but a significant number of customers use banks to pay their bill.<sup>126</sup> This service is comprising of utility (water, electricity, and telecoms), transport (Ethiopian Airline and some bus transportations including Selam Bus, Walia Bus), and others. The regulation of non-bank bill payment service provides is outside of the study.

### **2.2.2.7 Electronic Payment Instruments**

As it has been already addressed in the above, the ATM and POS terminals can be accessed only using electronic payment instruments namely debit card, credit card, and stored value cards. Thus, the issuance of these electronic payment instruments is indispensable: there are no ATM and POS banking services unless the customers of the banks are equipped with such electronic payment instruments. By now, the Ethiopian banks are allowed only to issue debit and prepaid cards, but not credit cards.<sup>127</sup> A debt card is a plastic payment card that can be used instead of cash when making purchases; the money comes directly from the customer's financial account when performing any transaction.<sup>128</sup> A debt card is different from a credit card, while debit card requires the existence of a balance in the financial account of the user but in credit card the user can also transact (withdraw or transfer fund) even in the absence of sufficient balance in his/her financial account. A stored-value card is a prepaid card that has a monetary value that is recorded as data on the card itself and thus can be used without online access to an associated financial account.<sup>129</sup> The stored-value card could be one-time or multi-time use. The multi-time stored-value card is different from the one-time stored-value card as the balances of the former could be increased by crediting money in the

---

<sup>124</sup> Bethelhem Lemma, 'Ethiopia: Kifiya Financial Technology Receives Zambezi Award', *2Markato.com*, July 20, 2015.

<sup>125</sup> Bethelhem Lemma(n128).

<sup>126</sup> Interview with Ato Berihu Gebru, Business support Officer, Commercial Bank of Ethiopia (Addis Ababa, 12 May 2018).

<sup>127</sup> Interview with Ato Solomon Damitew, Principal Manager Payment Systems Over Sight and Development, National Bank of Ethiopia (Addis Ababa, 04 May 2018).

<sup>128</sup> *Wikipedia*, "Debit Card". < [https://en.wikipedia.org/wiki/Debit\\_card](https://en.wikipedia.org/wiki/Debit_card) > accessed 12 May 2018.

<sup>129</sup> *Wikipedia*, "Prepaid Card". < [https://en.wikipedia.org/wiki/Prepaid\\_card](https://en.wikipedia.org/wiki/Prepaid_card) > accessed 12 May 2018.

financial institution. The National Payment System Proclamation recognizes the stored-value card which its value can be increased or decreased.<sup>130</sup>

As part of the ATM and POS banking, Ethiopian banks issued debit and prepaid cards that enable their customers to access banking activities using the ATM and POS terminals. The plastic debit cards issued by the Ethiopian banks have different brand names, for example, the brand name for Lion bank is ‘Lion Card’, Wegagen Bank brand is ‘Agar Card’ and Hibiret Bank brand is ‘Hibir Card’. The debit card issued by the Ethiopian banks can be used to cash withdrawals, bill payments, forex, fund transfer, and balance inquiry through the ATMs terminals, or to buy goods or services from merchants who have a point of sale terminal in their premises. One thing that should be clear at this level is the Ethiopian banks issue the debit card themselves, the NBE has only a regulatory role.<sup>131</sup>

A debit card is the most widely used electronic payment instrument used in the country. This debit card is chip-based and all the debit cards issued so far are VISA branded; but nowadays, some banks are introducing new debit card branded Ethio-Pay which is issued by EthSwich.<sup>132</sup> By now, the number of Ethio-Pay cards is insignificant.<sup>133</sup> As per the report of the National Bank, more than 95% of the active debit cards are used only for cash withdrawals. As of March 2018, 6,623,887 active debit cards are in use by the customers of the Ethiopian banks.<sup>134</sup> Out of the total active debit cards in use, more than 65% of the are issued by the CBE and Dashen Bank and Abay Bank share 10% and 6.3% respectively out of the mentioned number of the debit card.<sup>135</sup> Wegagen Bank, Bank of Abyssinia and United Bank also issued a significant number of debit cards.<sup>136</sup> But, Debeb Global Bank, Enat Bank, Addis International Bank, Zemen Bank, and Lion International Bank together issued less than one percent out of the total number of debit cards.<sup>137</sup> Similar to the other electronic channels, more than half of the debit card is concentrated in the country’s capital, Addis Ababa, followed by Oromia and Amhara.<sup>138</sup>

---

<sup>130</sup> National Payment System Proclamation, Art 2(27).

<sup>131</sup> National Payment System proclamation, Art 2(27).

<sup>132</sup> Interview with Ato Solomon Damitew, Principal Manager Payment Systems Over Sight and Development, National Bank of Ethiopia (Addis Ababa, 04 May 2018).

<sup>133</sup> Interview with Ato Solomon Damitew, Principal Manager Payment Systems Over Sight and Development, National Bank of Ethiopia (Addis Ababa, 04 May 2018).

<sup>134</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>135</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>136</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>137</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>138</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

Prepaid is the second and least used electronic payment instrument in the country.<sup>139</sup> So far out of the seventeen banks, only six banks issued prepaid cards; Wegagen Bank, Commercial Bank of Ethiopia, Bank of Abyssinia, Zemen Bank, United Bank, and Abay Bank. As of March 2018, 43,199 prepaid cards are issued by the said banks.<sup>140</sup> Out of the total number of prepaid cards, 21,561 cards are issued by Wegagen Bank, 20,252 cards are issued by CBE and the left insignificant prepaid cards are issued by the four banks; Bank of Abyssinia, Zemen Bank, United Bank, and Abay Bank.<sup>141</sup>

### 2.2.2.8 Cheque Truncation

Cheque truncation is the conversion of paper-based cheque into a substitute electronic form for transmission to the paying bank.<sup>142</sup> By simple words, cheque truncation is the process of converting paper cheques into an electronic format that are then used during the transaction cycle.<sup>143</sup> Cheque truncation reduces or totally eliminates if properly done the physical movement of paper-based cheques and it reduces the time and cost of processing the cheque clearance system.<sup>144</sup> It also reduces the settlement periods.<sup>145</sup> Similar to other countries payment systems, the Ethiopian national payment system recognizes the conversion of physical cheques into electronic form to submit for payment; according to the National Payment System Proclamation, physical cheque or any other payment instrument can be converted into electronic data by exchange and storage of its image and the corresponding information which shall represent the original instrument.<sup>146</sup> Such an image of the paper-based instrument is equivalent of the paper it represents.<sup>147</sup> Once the image of the paper-based payment instrument is converted into electronic form and submitted to the payer bank for payment, the payer bank has the obligation to pay to the said amount of money. Once payment is done, the paper-based cheque which is changed into electronic form cannot be negotiated and it shall be destroyed.<sup>148</sup>

---

<sup>139</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>140</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>141</sup> National Bank of Ethiopia, Draft Annual Report 2017/18.

<sup>142</sup> *Wikipedia*, "Cheque Truncation". < [https://en.wikipedia.org/wiki/Cheque\\_truncation](https://en.wikipedia.org/wiki/Cheque_truncation) > accessed 12 May 201.

<sup>143</sup> 'Cheque Truncation: Advantages & Disadvantages', at < <https://www.sybrin.com/blog-cheque-truncation-advantages-and-disadvantages> > accessed 26 April 2018.

<sup>144</sup> *Ibid.*

<sup>145</sup> *Ibid.*

<sup>146</sup> National Payment System Proclamation, Art 24(1).

<sup>147</sup> National Payment System Proclamation, Art 24(2).

<sup>148</sup> National Payment System Proclamation, Art 24(3).

Since last year, the NBE introduces standard physical cheque, and all banks are currently using the standard cheque in issuing cheques to their customers.<sup>149</sup> As an extension of the standard cheque the Ethiopian Bankers Association is working the ‘Cheque Truncation Project’ with the purpose of introducing the cheque truncation service in the near future.<sup>150</sup> By now, the project is in its final stage and it is planned to begin cheque truncation services to the customers of the banks in the next year.<sup>151</sup>

## **2.3 Problems with Electronic Banking in Ethiopia**

Although e-banking is convenient and cost-effective, the birth of the new e-banking products and services creates numerous and complex problems. Some of the most and troubling problems are: liability for unauthorized electronic fund transactions; authentication of customer’s authorization; admissibility of e-banking records; allocation of losses for unauthorized access of customer’s account; problems related with the liability of failure to effect electronic fund transfer due to system malfunction; human error; issue related with outsourcing of operating system; issues related with cross-border electronic fund transfer; issues related with customer’s liability; loss of various rights including the right to countermand the electronic fund transfer, privacy and confidentiality of customer’s financial information. The next sub-sections is devoted to discusses the practical problems associated with e-banking products and services in Ethiopia.

### **2.3.1 Problems Related to Authentication Customer’s Authorization**

Contract law conventionally requires the parties to attach their signatures to a written document; like any other contract, the deposit or fund transfer services require the signatures of the parties. In the traditional banking business, the authorization of the customer to the deposit or fund transfer service was authenticated by the physical photo and handwritten signature attached with the deposit book. The change in the service delivery method requires the change in the authenticity of the customer’s authorization. Thus, by now, the customer’s authorization is authenticate using the electronic authorization means. Like any other country’s banks, the Ethiopian banks are authenticating the customer’s authorization using

---

<sup>149</sup> Interview with Ato Solomon Damitew, Principal Manager Payment Systems Over Sight and Development, National Bank of Ethiopia (Addis Ababa, 04 May 2018).

<sup>150</sup> Interview with Ato Solomon Damitew, Principal Manager Payment Systems Over Sight and Development, National Bank of Ethiopia (Addis Ababa, 04 May 2018).

<sup>151</sup> Interview with Ato Solomon Damitew, Principal Manager Payment Systems Over Sight and Development, National Bank of Ethiopia (Addis Ababa, 04 May 2018).

the electronic-based authentication means. The core-banking system enables the Ethiopian banks to provide banking services to their customers at any of their online branches, and for deposit book based bank transaction services, the banks use two-factor authentication method—photo and the digital image of the handwritten signatures.<sup>152</sup> But, for any electronic fund transaction made through electronic devices, the Ethiopian banks use different authentication methods: For ATM and POS banking, the banks use the PAN (card) and the PIN to authenticate the customer’s authorization, and in addition to the PAN and PIN method when a cash is withdrawn or fund is transferred the ATM terminals automatically captured the photograph of the person who initiates the instruction.<sup>153</sup> For mobile banking, the banks use SIM and the PIN. And for internet banking, the banks use the two-factor authentication method using the token method.<sup>154</sup> By now, there are two problems in relation to the authentication of the customer’s authorization: one, the PIN/password of the electronic devices is four digit, which is very short and easy for theft during initiating e-banking transaction using the electronic devices; two, the erroneous keying of the PIN/password is tolerable up to three times in some banks of the country, and this creates a conducive condition for fraudulent transaction.<sup>155</sup>

### **2.3.2 Problems Related to Admissibility of E-banking Records**

The e-banking record is in the form of transaction receipts produced by electronic channels like ATMs, POS, mobile phones, the Internet and or any other electronic device or output generated internally within a bank or third party’s computer systems, or records comprising a mix of human input and calculations generated and stored by a computer. It is important to underline that electronic evidence is subject to the same rules of evidence as paper documents, however, the unique nature of e-evidence, as well as the ease with which it can be manipulated or falsified, creates the problems of admissibility not raised with the paper-based evidence.<sup>156</sup> Thus, unlike the paper-based evidence, the admissibility of the e-banking records

---

<sup>152</sup> Interview with Ato Mintesinot Seyum, Manager of Mobile and Internet Banking, Commercial Bank of Ethiopia (Addis Ababa, 03 May 2018).

<sup>153</sup> Interview with Ato Mintesinot Seyum, Manager of Mobile and Internet Banking, Commercial Bank of Ethiopia (Addis Ababa, 03 May 2018).

<sup>154</sup> Interview with Ato Mintesinot Seyum, Manager of Mobile and Internet Banking, Commercial Bank of Ethiopia (Addis Ababa, 03 May 2018).

<sup>155</sup> Interview with Ato Ephirem Baraki, Senior Legal Expert, National Bank of Ethiopia (Addis Ababa, 09 August 2018).

<sup>156</sup> Hon. Alan Pendleton, ‘Admissibility of Electronic Evidence: A new Evidentiary Frontier’, Bench & Bar of Minnesota, 2013. At < <http://mnbenchbar.com/2013/10/admissibility-of-electronic-evidence/> > accessed 21 March 2018.

raises the following four questions: First, who is the author of the e-signature or record?<sup>157</sup> The unauthorized access of the customer's account is raised here, again, how much the electronic entry is accurate as the employees of the bank may enter data's what is not initiated by the customers. Second, is the computer program that created the record reliable?<sup>158</sup> This raises the question of what if the computer were not functioning properly at the material time, and how much such computer-generated evidence is accurate as a computer does not always function properly. Third, were the records altered, manipulated, or damaged after they were created?<sup>159</sup> The e-evidence can be easily altered, manipulated, or damaged and how the court can be confident that such brought e-evidence is the original one. Fourth, is the electronic record a complete record of the electronic communication?<sup>160</sup> In any circumstances the e-communication is not full-fledged; it only shows part of the e-communications and in this time how it can be considered as a conclusive evidence is also one of the controversial issues.<sup>161</sup>

### **2.3.3 Problems Related to Confidentiality of Customer's Financial Information**

Confidentiality is central to the trust between the customer and the financial institutions. The duty of confidentiality of financial institutions is not only limited to the e-banking products and services, but it also applies to traditional banking services. Confidentiality is the assurance that key information is not disclosed to third parties without proper authorization and is made available only to those who have a legitimate need or right to access it.<sup>162</sup> In the banking view, confidentiality is the assurance that key information remains private and is not disclosed or used by those unauthorized to do so; and the unauthorized disclosure or misuse of the customer's data exposes the bank to both reputational and legal risks.<sup>163</sup>

The customers of the Ethiopian commercial banks access their financial accounts through the use of their identity card, passwords(PIN), or other authentication procedures provided to them by the banks. The use of those methods deters the unauthorized access of the customer's

---

<sup>157</sup> Lucy L. Thomson, 'Mobile Devices New Challenges for admissibility of Electronic Evidence', *SciTech Lawyer*, Vol. 9, No. 3, 2013, p. 3-4.

<sup>158</sup> Lucy L. Thomson (n162) 3-4.

<sup>159</sup> Lucy L. Thomson (n162) 3-4.

<sup>160</sup> Lucy L. Thomson (n162) 3-4.

<sup>161</sup> Lucy L. Thomson (n162) 3-4.

<sup>162</sup> Jayaram Kondabagil, *Risk Management in Electronic Banking: Concepts and Best Practices*, John Wiley & Sons (Asia) Pte Ltd, 2007, p. 70.

<sup>163</sup> Jayaram Kondabagil(n167)70-71.

financial account by third parties. In relation to the use of identity cards, there is no any possibility for unauthorized access by a third party because of the existence of cross-checking of the photograph in the system and the person who initiates withdrawal in the branches of the commercial banks. But, in the second case, accessing the financial account using a PIN, it is highly disclosed to unauthorized access of the customer's personal information. The personal financial information of the customer may be disclosed to third parties due to one or more of the following four circumstance. First, if the customer him/herself divulged his/her PIN voluntarily friends and members of the family. Second, when the customer failed to properly cover the keyboard of the ATM machine, and use the passwords of the M-banking or the Internet banking being observed by others. Third, when the customer writes in a paper or saves in a computer or mobile phone and if such paper, computer or phone is accessed by a third party either voluntary lending or because it is lost or stolen. Fourth, hackers can also hack the accounts of a customer using malware as it has been addressed in the Introduction section of this Thesis.<sup>164</sup> In Ethiopia, the first three reasons are the usual for the unauthorized access of the customer's financial information. The fourth one is not as such frequent but once the Russian Security Officers warns the Ethiopian banks to take care of the repetitive trial of hackers sourced from North Korea.<sup>165</sup> To avoid the possibility of unauthorized access of customer's account, the Ethiopian commercial banks incorporate Secure Socket Layer (SSL) and other technologies.<sup>166</sup>

### **2.3.4 Problems Related to Failure to Electronic Fund Transfer**

Financial institutions are under a duty to repay customer's funds. This duty includes to make payment to third parties as per the order of the customer; such duty emanates from the banker-customer relationship. Like in the traditional banking, the bank may fail to make an electronic fund transfer as per the order of its customer. Banks failure to make e-banking transaction takes the form of either a complete failure to make an electronic fund transfer or a failure to make an electronic fund transfer properly.<sup>167</sup> A good example of this could be the failure of e-banking transaction is the bank's unjustifiable denial of cash withdrawal from an

---

<sup>164</sup> Hackers can hack banks Using Malwares in a Distant at <<http://www.ibtimes.co.uk/global-banks-alert-hackers-launch-covert-atm-heists-via-malware-1641030>> accessed May 01, 2018.

<sup>165</sup> Dawit Endeshaw, 'North Korea-linked hackers target Ethiopian banks', The Reporter English,(8 April 2017), at<<http://www.thereporterethiopia.com/content/north-korea-linked-hackers-target-ethiopian-banks>>accessed 27 April 2018.

<sup>166</sup> Interview with Ato Elias Mitiku, Unit Head of Clearing and Settlement, Premier Switch Solution (12 May 2018).

<sup>167</sup> Fayad Algudah, The liability of Banks in Electronic Fund Transfer Transactions: A study in British and the United State Law, Ph.D Thesis, The University of Edinburgh, 1992, [Unpublished available online] 64.

ATM.<sup>168</sup> A failure to make an e-banking transaction properly means a performance of the transaction but without compliance with the terms and conditions of the customer's instructions.<sup>169</sup> The failure of the e-banking transaction may be happened due to: first, human error, error from the instruction feed by the customer to the ATM or any other electronic device, second, malfunction and errors from the system.<sup>170</sup>

#### **2.3.4.1 Human Error**

Human error may happen either by a customer or by the bank in the course of processing the e-banking transaction. Internet banking screens for online payments commonly require the name and account number of the intended recipient's account to be keyed in. In practice, an electronic fund transfer is processed on the basis of both the account number and the name of the account holder. This has the effect that, if the payer keys in the wrong account number the payer has the chance to discover the error as the name of the erroneous account holder is different from the name of the intended recipient, but where the name of the wrongly keyed account number and the name of the intended recipient is the same, the payer will not have the chance to discover the error and due to this he will authorize the transaction; this time the error may only come to light when the intended recipient tells the payer that the payment has not been received. When the payer tries to find out where the payment has actually gone, he may be told that the recipient's name and location cannot be released for reasons of confidentiality. The bank may respond that it has acted on the basis of the instructions it was given, that is, the account number. Again, if the fund transfer is made to a customer with a different bank, the recipient's bank may claim that it has no liability because it acted on the instructions it received from the payer's bank. Error in the electronic payment systems may be caused by a number of factors:<sup>171</sup> First, there may be a failure of the transaction to be completed (e.g., fund transfer at an ATM is not credited to the consumer's account or a third party is not made).<sup>172</sup> Second, an e-banking transaction may be executed for an incorrect amount.<sup>173</sup> Third, payments may be made to a wrong party or at a wrong time.<sup>174</sup> In any such

---

<sup>168</sup> Fayad Algudah (n172) 64.

<sup>169</sup> Fayad Algudah (n172) 64.

<sup>170</sup> Fayad Algudah (n172) 64.

<sup>171</sup> Focus group discussion with Ato Birhane Gebrecherkos, Ato Berihu Gebru, Ato Endalle Tessema, Ato Bahire Birhane and Ato Anteneh Gebriye, Commercial Bank of Ethiopia (Addis Ababa, 12 May 2018).

<sup>172</sup> Focus group discussion with Ato Birhane Gebrecherkos, Ato Berihu Gebru, Ato Endalle Tessema, Ato Bahire Birhane and Ato Anteneh Gebriye, Commercial Bank of Ethiopia (Addis Ababa, 12 May 2018).

<sup>173</sup> Focus group discussion with Ato Birhane Gebrecherkos, Ato Berihu Gebru, Ato Endalle Tessema, Ato Bahire Birhane and Ato Anteneh Gebriye, Commercial Bank of Ethiopia (Addis Ababa, 12 May 2018).

<sup>174</sup> Focus group discussion with Ato Birhane Gebrecherkos, Ato Berihu Gebru, Ato Endalle Tessema, Ato Bahire Birhane and Ato Anteneh Gebriye, Commercial Bank of Ethiopia (Addis Ababa, 12 May 2018).

event, the above errors and malfunctions may cause considerable damage and losses to the consumers of e-banking.<sup>175</sup>

#### **2.3.4.2 Malfunction and Errors in the System**

As data communication networks are used to accomplish financial transactions, the potential for system error, malfunction, and resulting losses will increase correspondingly.<sup>176</sup> This potential for error and malfunction in computer transmission results in enormous loss of funds and consequential damage.<sup>177</sup> The Ethiopian banks may claim that the malfunction and errors are not due to negligence on their part, but due to the operation of the system, in which case it is arguable that the banks should be liable for losses incurred by the customer.<sup>178</sup> The Ethiopian commercial banks use the standard terms and conditions to disclaim liability for failure to carry out a transaction on the event of mechanical failure of the electronic device or transmission problem, or unavailability of services or circumstances beyond the bank's control prevent the transaction from being effected.<sup>179</sup>

#### **2.3.5 Problems Related to Loss of Right to Countermand Payment**

Once the existence error is discovered, it is expected that such error is corrected by the bank upon the request of the customer. In the traditional banking services, since the fund transfer orders were paper-based, stop payment were easy and possible in view of the fact that the clearing cycle is relatively longer- usually it takes three to four days before payment is completed, which is usually when the payee is notified of the payment by the payee bank.<sup>180</sup> But the e-banking transactions does not have such a long time to effect payment to the recipient of the payment; the account of the payee debited and credited to the recipient account automatically; once the fund is transferred using the electronic channels, such transfer is final and irrevocable. Generally, countermand is not possible after the customer's

---

<sup>175</sup> Focus group discussion with Ato Birhane Gebrecherkos, Ato Berihu Gebru, Ato Endalle Tessema, Ato Bahire Birhane and Ato Anteneh Gebriye, Commercial Bank of Ethiopia (Addis Ababa, 12 May 2018).

<sup>176</sup> Owen and Komarow, *The Emerging Law of Data Communications Networks: Some Thoughts on the Right and Responsibilities of Service Users and Providers*, 2 Computer Law Reporter, p. 276, as quoted by, Scott R. Porter, Scott R. Porter, 'On Line Financial services: Liability for errors or Malfunction in Stock Transactions over Personal Computers', *Computer & High-Technology Law Journal*, Vol.1, p.327.

<sup>177</sup> Ibid.

<sup>178</sup> Interview with Ato Elias Mitiku, Unit Head of Clearing and Settlement, Premier Switch Solution (Addis Ababa, 12 May 2018).

<sup>179</sup> Interview with Ato Elias Mitiku, Unit Head of Clearing and Settlement, Premier Switch Solution (Addis Ababa, 12 May 2018).

<sup>180</sup> Lukumay (n3)128-130.

instructions are entered into the electronic devices.<sup>181</sup> The Ethiopian banks under the standard terms and conditions of the e-banking insert a provision that defines the irrevocability of the electronic fund transfer once instruction to do so is inserted into the system.<sup>182</sup> Thus, the irrevocability of the electronic fund transfer is one of the problems in e-banking in Ethiopia that denies the customers to get back their money by reversing the e-banking entry.<sup>183</sup> The fund transfer made through the POS terminal will not be reversed even upon the return of the defective goods to the merchant; in practice, the merchants refund the money in cash to the customer.<sup>184</sup> A similar condition is applied for any fund transfer made using the M-banking services.<sup>185</sup>

### 2.3.6 Security and Unauthorized Access to Customers' Account

According to Aychiluhim Desisa and Tibebe Beshah, all Ethiopian banks engaged in the provision of Internet banking services are motivated to facilitate some security landscapes focusing only on bank site security only and the banks believe that customer site security is up to the customer to secure or not.<sup>186</sup> The researchers also identified that the major security problem is social engineering and its loophole is customer site security.<sup>187</sup> A research undertaken by Kaspersky Lab, a Russian multinational cybersecurity and anti-virus provider, listed Ethiopian banks among those banks that are under cyber-attack by North Korean-linked hackers group a.k.a Lazarus hackers.<sup>188</sup> The company corporate manager Mr. Olga Bezpyatkina states that there have been several victim Ethiopian banks with a large set of Lazarus malware tools and those malware infections were quite serious that indicates a preparation for a major theft of money from the targeted banks using the malware tools.<sup>189</sup> As per the research, those group of hackers' targets 18 countries around the world and Ethiopia, Kenya, Gabon, and Nigeria are the only African countries targeted by the said

---

<sup>181</sup> Lukumay (n3)128-130.

<sup>182</sup> Interview with Ato Ephirem Baraki, Senior Legal Expert, National Bank of Ethiopia (Addis Ababa, 09 August 2018).

<sup>183</sup> Interview with Ato Ephirem Baraki, Senior Legal Expert, National Bank of Ethiopia (Addis Ababa, 09 August 2018).

<sup>184</sup> Interview with Aster Cheru, Tiegist Zeleke, Elsabet Alemayoh, Meseret Fikadu, the POS terminal runners of Oil-Libya Finfine Branch, Glorious PVT.LTD Beherawi Branch, Ethiopian Electronics PLC and Ethiopia Hotel respectively.

<sup>185</sup> Ibid.

<sup>186</sup> Aychiluhim Desisa & Tibebe Beshah, 'Internet Banking Security Framework: The Case of Ethiopian Banking Industry', *HiLCoE Journal of Computer Science and Technology*, Vol. 2No. 2, pp. 7-13, at P. 11.

<sup>187</sup> Ibid.

<sup>188</sup> Dawit Endeshaw, 'North Korea-linked hackers target Ethiopian banks', *The Reporter English*, (8 April 2017), at <<http://www.thereporterethiopia.com/content/north-korea-linked-hackers-target-ethiopian-banks>> accessed April 27, 2018.

<sup>189</sup> Dawit Endeshaw(n193).

hackers.<sup>190</sup> Besides, the e-banking may be subject to unauthorized withdrawal and theft by its own employees; some employees of a bank has attempted to withdraw cash from ATM terminal by preparing forged payment instrument, though the PSS officer does not volunteer to disclose the name of the bank.<sup>191</sup>

Another fraudulent e-banking transaction comes to view; when the cardholder falsely denies that an ATM cash withdrawal shown on his account was not made by him, or when a third-party find, manufacture, steal, and obtain the PIN and then withdraw a cash from the true cardholder's account.<sup>192</sup> The cardholder could voluntarily disclose his PIN to someone else who later obtains easy access to the card or any other electronic device (mobile phone or PC), or the cardholder could simply be careless about the way in which he records his PIN in close proximity to his card or any other electronic device, thus making it easy for someone else to steal, or borrow the card or the electronic device and use it without the cardholder knowledge or consent.<sup>193</sup> Similarly, the voluntarily lending of the account holder's mobile phone, and the voluntary disclosure of the password of his mobile banking or the careless use of the password when the account holder is being overlooked by someone else may disclose the account holder to fraudulent m-banking transaction.<sup>194</sup> Again, the careless use of the I-banking password or hacking technologies discloses the account holder's account to fraudulent transaction. In relation to hacking technologies, though the NBE officer is not volunteer to disclose the name of the bank and the name and University of the hackers, some university students has withdrawn cash by using the hacking technology.<sup>195</sup> The criminal case of the university students is pending.<sup>196</sup>

### **2.3.7 Problems Related to allocation of Losses**

The fundamental issue to be considered in relation to the above-mentioned problems of e-banking is the loss or liability allocation between the financial institution and the consumer on whose behalf the e-banking transaction is purported to be initiated. Loss, theft or robbery

---

<sup>190</sup> Dawit Endeshaw(n193).

<sup>191</sup> Interview with Ato Elias Mitiku, Unit Head of Clearing and Settlement, Premier Switch Solution (Addis Ababa, 12 May 2018).

<sup>192</sup> EFT and EDI – Legal Consequence of Fraud, Malfunctions and Mistakes in Payment Card Transactions, Andrew Laidlaw, International Yearbook of Computers and Technology, Volume Six, 1992. P. 89-90.

<sup>193</sup> Id., p.90.

<sup>194</sup> Ibid.

<sup>195</sup> Interview with Ato Ephrem Baraki, Senior Legal Expert, National Bank of Ethiopia (Addis Ababa, 09 August 2018).

<sup>196</sup> Interview with Ato Ephrem Baraki, Senior Legal Expert, National Bank of Ethiopia (Addis Ababa, 09 August 2018).

of the debt or credit card may cause the customer to suffer financial losses, if the third party who possess such card withdraws the customer's money from the electronic terminals. In such situations the question of whether the bank or the consumer should be liable for the loss sustained due to malfunction, error, or fraudulent withdrawal of money from the consumers account kept in the banks come to view. By now, the Ethiopian commercial banks are shifting the liabilities to their customers using the adhesive e-banking service agreement.<sup>197</sup> Thus, the consumers of the e-banking products and services are carrying all the liabilities arising out system malfunction and errors, and unauthorized fraudulent withdrawal of money from financial accounts kept in the banks.

### **2.3.8 Problems Related to Cross-Border E-Banking Transactions**

Cross-border e-banking is the provision of transactional online banking products or services by a bank in one country to the residents of another country.<sup>198</sup> The dependence on technology for providing the services with necessary security, and the cross-border of nature of the transactions, involves additional risks for banks and new challenges for regulators.<sup>199</sup> Using the internet, banks can source deposits from jurisdictions where they are not licensed or supervised or have access to payment systems.<sup>200</sup> Due to the technological advancement, customers can deposit funds outside of their home country. The key issues for banking supervisors in e-banking are how to ensure effective regulation of operations both in their own markets (as host regulator) when services are provided from abroad, and in foreign markets when the bank is licensed in the home jurisdiction.<sup>201</sup> Thus, the particular concerns to consumers in cross-border e-banking revolve around jurisdictional and choice of law issues.<sup>202</sup>

In practice, the Ethiopian merchants are witnessing financial losses due to fraudulent e-banking transactions: In one international hotel a customer uses the Visa card to make payments in exchange of the service he has accessed within the hotel, and until the time the

---

<sup>197</sup> The close reading of terms and conditions of the e-banking service agreements shows that the banks shift all the liabilities arising out of system error and malfunction to their customers.

<sup>198</sup> Basel Committee on Banking Supervision: 'Management and Supervision of Cross-Border E-banking Activities' at <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwjO8szPpNLaAhXsB5oKHbayDecQFggpMAE&url=http%3A%2F%2Fwww.bis.org%2Fpubl%2Fbcbs93.pdf&usg=AOvVaw36XoR8W9IRyzDtrDhKXUMa> > [Last accessed April 24, 2018].

<sup>199</sup> Andre Schaechter, 'Issues in Electronic Banking: An Overview', IMF Policy Discussion Paper, March 2002, p.1.

<sup>200</sup> Lukumay (n3)142.

<sup>201</sup> Basel Risk Management Principles for Electronic Banking 2-3.

<sup>202</sup> Basel Risk Management Principles for Electronic Banking 2-3.

persons leaves Ethiopia there was no fraud report at all. At the end of the month, the hotel submits the batch for settlement before its bank (acquirer bank), and the acquirer bank again before it reimburses the money to its customer (merchant) submits the batches to its intermediary banks and one of the receipts are denied by its intermediary banks by saying the real owner of the payment instrument was not in Ethiopia in the said time and all the transactions made by the unauthorized transactions made by fraudulent third party would not be reimbursed. And following the response of the intermediary bank, the Ethiopian bank denied reimbursement for such fraudulent cross-border e-banking transaction. The hotel and its acquiring bank didn't know how the fraudulent online transaction was held, but according to the technology expert, such fraudulent transaction is possible only using forged payment instrument.<sup>203</sup>

The online fraudulent transaction is very rare and even very abstract to identify it early, but worse than the online transaction the offline transaction is highly disclosed to fraud.<sup>204</sup> Though there are truthful customers who come to Ethiopia as per their words and pay the said money to the merchants for the offline cross-border e-banking transaction, through offline transaction a significant number of foreigners cheats the Ethiopian merchants, and the merchants are facing substantial losses in relation to this fraud. Many merchants claim to the CBE in relation to misleading reserve and payment to the third party based upon the offline transactions.<sup>205</sup>

### **2.3.9 Problems Related to Dispute Resolution**

As it has been already mentioned in the above sections, the e-banking products and services are disclosed to numerous problems, due to the existence of these problems, the dispute is indispensable. But, it is important to keep in mind that most of the of e-banking transactions take place without facing one or more of the above-mentioned problems; it is rare for a system to be perfect and it will be the case that things will sometimes wrong. Unauthorized access of customer's account, malfunction, erroneous transaction and the absence of the right to countermand are the usual problems that the Ethiopian consumers face in their day to day

---

<sup>203</sup> Interview with Ato Elias Mitiku, Unit Head of Clearing and Settlement, Premier Switch Solution (Addis Ababa, 12 May 2018).

<sup>204</sup> Interview with Ato Elias Mitiku, Unit Head of Clearing and Settlement, Premier Switch Solution (Addis Ababa, 12 May 2018).

<sup>205</sup> Focus group discussion with Ato Birhane Gebrecherkos, Ato Berihu Gebru, Ato Endalle Tessema, Ato Bahire Birhane and Ato Anteneh Gebriye, Commercial Bank of Ethiopia (Addis Ababa, 12 May 2018).

e-banking transactions.<sup>206</sup> Over that, the financial institutions are intently shifting all the liabilities arise out of the risks associated with the e-banking. Generally, the problems of e-banking which are mentioned in the above may cause huge financial losses to consumers transacting banking products and services using the electronic channels. This raises the issue of dispute settlement; how a customer can claim his/her money back or obtain compensation for their loss? By now, the consumers of the e-banking are required to appear before the nearest branch of their home-bank to notify the bank about the existence of a problem, and the online branch address the problem where it can be easily fixed, if not, it advises the consumers on how to submit their formal complaint and within how many days the complaint will be solved. But the usual problems in relation to the internal complaint handling system is that the online branch orders the complainer to submit its complaint before the branch bank which issues the financial account. Again, if the consumer's card is held by the ATM terminal owned outside of his home-bank or if the consumer gets financial losses due to the use of ATM terminal outside of his home-bank, though the consumers appear before the nearest branch and complain the existence of such problems, in practice the banks order to complain before the bank who owns the ATM terminal.<sup>207</sup> But, with all its problems, many of the complaints of the consumers mainly those minor complaints related with the holding of cards and malfunction are addressed using the internal complaint handling system.<sup>208</sup>

After exhausting the internal complaint handling system, in practice, some consumers of the e-banking products and services are submitting their cases before the NBE, and the NBE accept the complaints from the customers of the banks and gives a recommendation for the banks to address such complaints; the NBE only provides public remedy, not private remedy, but the customer can use such recommendations to claim his rights before the regular courts.<sup>209</sup> By now, the NBE is complaining to the TCCPA to adjudicate e-banking disputes as for any other consumer complaints, but the TCCPA denies that its establishment proclamation does not empower it to settle disputes in relation to the e-banking products and services.<sup>210</sup> Thus, currently, the TCCPA is empowered to settle disputes in relation to the

---

<sup>206</sup> Interview with Ato Ephirem Baraki, Senior Legal Expert, National Bank of Ethiopia (Addis Ababa, 09 August 2018).

<sup>207</sup> Interview with Tebeje Hailu and Yonas Mokenen, consumers of e-banking Bahir Dar, 19 June 2018).

<sup>208</sup> Interview with Ato Ephirem Baraki, Senior Legal Expert, National Bank of Ethiopia (Addis Ababa, 09 August 2018).

<sup>209</sup> Interview with Ato Ephirem Baraki, Senior Legal Expert, National Bank of Ethiopia (Addis Ababa, 09 August 2018).

<sup>210</sup> Interview with Ato Ephirem Baraki, Senior Legal Expert, National Bank of Ethiopia (Addis Ababa, 09 August 2018).

consumers of any goods or services including the consumers of the e-banking products and services, though in practice it denies the complaining consumers by saying that it does not have a material jurisdiction to entertain e-banking disputes.<sup>211</sup>

The litigation dispute settlement system provided by the ongoing laws of the country are not cost-effective dispute settlement systems. The cost of initiating proceedings and enforcing the judgment may outweigh the amount in dispute. The absence of cost-effective dispute settlement raises the issue of the protection of consumers of the e-banking; consumers may disregard their rights because of the cost of the dispute settlement system. Over that, the awareness of the consumers on the available dispute settlement system is also one of the problems in Ethiopian case; as the researcher has interviewed some customers of the banks, the customers do not have even any clue as to how they can enforce their rights when they lost their money due to unauthorized withdrawal or due to the malfunction of the system.<sup>212</sup>

### **2.3.10 Problems Related to Non-financial Infrastructure**

The provision of e-banking products and services not only requires a financial infrastructure but also the non-financial infrastructure; power and connection. The power outage in the middle of processing the e-banking transaction causes stops the ATM terminal and holds the payment instrument.<sup>213</sup> Similarly, the power outage stops the process of the fund transfer made by the POS terminal without even showing whether fund transfer is effective or not.<sup>214</sup> Similar to the power outage, the frequent downtime of connectivity is one cause for the malfunction and erroneous e-banking transactions.<sup>215</sup> Thus, by now, the Ethiopian e-banking consumers are witnessing substantial financial losses due to power outage and downtime of connection during processing of the e-banking transactions. Over that, the continuous breakdown of power and/or connection for long hours and sometimes for weeks are denying the consumers of the e-banking products and services from accessing banking services at any time that they like to access the services.

---

<sup>211</sup> Interview with Ato Ephirem Baraki, Senior Legal Expert, National Bank of Ethiopia (Addis Ababa, 09 August 2018).

<sup>212</sup> Interview with Ato Natan Lemma, Meseret Fikadu, Tebeje Hailu, G/hiwot Guesh, Yonas Berhe and Yonas Mokenen (June and May 2018).

<sup>213</sup> Interview with Ato Natan Lemma, Meseret Fikadu, Tebeje Hailu, G/hiwot Guesh, Yonas Berhe and Yonas Mokenen (June and May 2018).

<sup>214</sup> Interview with Aster Cheru, Tiegist Zeleke, Elsabet Alemayoh, Meseret Fikadu, the POS terminal runners of Oil-Libya Finfine Branch, Glorious PVT.LTD Beherawi Branch, Ethiopian Electronics PLC and Ethiopia Hotel respectively (June 2018).

<sup>215</sup> Interview with Aster Cheru, Tiegist Zeleke, Elsabet Alemayoh, Meseret Fikadu, the POS terminal runners of Oil-Libya Finfine Branch, Glorious PVT.LTD Beherawi Branch, Ethiopian Electronics PLC and Ethiopia Hotel respectively (June 2018).

## CHAPTER THREE

### THE LIMITS OF REGULATION AND NEED FOR REFORM

#### 3.1 Introduction

As the central body of the Thesis, this chapter is devoted to discussing the policy, legislative and regulatory foundations of e-banking business in Ethiopia in order to ascertain the extent to which it addresses issues raised by the adoption of e-banking products and services, particularly those issues affecting the consumers of the e-banking products and services. This chapter is divided into four major parts, each contains sections and sub-sections; part-one deals with the constitutional framework, part-two deals with the policy framework, part-three deals with legislative framework, and the last part covers the regulatory framework of the e-banking regulation. Accordingly, it examines and analyzes the Constitution, policies, legislation (proclamations, directives and circular letters of the NBE), and practices of e-banking regulation in Ethiopia and by doing so, it investigates the limits of the policies, laws and regulatory frameworks of the e-banking regulation.

#### 3.2 Constitutional Framework

With the coming of the 1995 FDRE Constitution, Ethiopia has introduced federal state structure in which power of the state is constitutionally divided between the federal and regional governments.<sup>216</sup> The Constitution mandated the Federal Government with the power to “...*administer the National Bank, print and borrow money, mint coins, regulate foreign exchange and money in circulation.*”<sup>217</sup> Thus, according to the Ethiopian Constitution, regulation of matters relates to payment and settlement systems including e-banking products and services falls under the exclusive ambit of Federal Government power. It should be noted that this is not peculiar to Ethiopia, in almost all countries that follow a federal system of government, the legislative power to banks and banking is given to the federal governments. To give one illustrative example, under the Nigerian Constitution, organ of the Federal government, i.e. the National Assembly, the Parliament comprises of the Senate and House of Representatives, is vested with exclusive power to legislate laws on the regulation of banks

---

<sup>216</sup> FDRE Constitution, Art 50(1).

<sup>217</sup> FDRE Constitution, Art 51(7).

and banking businesses.<sup>218</sup> Moreover, under Article 72 of the Nigerian Constitution, Regions have the obligation to act in accordance with the laws legislated by the Federal Government.

The FDRE Constitution entrusts the House of People Representative with power and duty to approve general policies and strategies of economic, social and development, and fiscal and monetary policy of the country.<sup>219</sup> Thus, the involvement of the HOPR with regard to policies and strategies is only limited to approval; the preparation of the policies and strategies lies with the executive wing of the government; Council of Ministries. Though it raises constitutionality issue, in some primary legislation the HOPR delegated to a specific executive organ to issue policies without requiring approval from the HOPR; for example, the HOPR delegates the NBE to formulate and implement the exchange rate policy.<sup>220</sup> Thus, the NBE is delegated both to formulate and implement the foreign exchange policy without seeking approval from the HOPR.

The power of the HOPR is not limited to the formulation of policies but it is also entrusted to enact laws on matters relating to the local currency, the administration of the National Bank, and foreign exchange.<sup>221</sup> The administration of National Bank includes the regulation of banks and banking business which in turn includes e-banking products and services. Thus, according to the FDRE Constitution, the power to enact policies and laws on matters relating to e-banking lies with the Federal Government; not with states or concurrent power. Again, from among the Federal Government organs, it is the HOPR who has the power to issue the policies and laws relating to e-banking regulations.<sup>222</sup> Moreover, both the Council of Ministries and the National Bank have a delegated legislative power to enact regulations and directives that regulate the e-banking products and services respectively.<sup>223</sup> With regard to the enforcement institutions, Article 77(4) of the Constitution, as well as proclamation No.591/2008, empowers the Council of Ministers and National Bank of Ethiopia to enforce the laws issued by the legislative organ of the government. Thus, the FDRE Constitution clearly sets the layer and institutions of government that have power and authorities over e-banking regulation.

---

<sup>218</sup> The Constitution of the Nigeria, Art 72(1).

<sup>219</sup> FDRE Constitution, Art 55(10).

<sup>220</sup> National Bank of Ethiopia Establishment (as Amended) Proclamation, Art 5(5).

<sup>221</sup> FDRE Constitution, Art 55(10).

<sup>222</sup> FDRE Constitution, Art 55(10).

<sup>223</sup> National Payment System Proclamation, Art 37(1)&(2).

### 3.3 Policy Framework: National Retail Payments Strategy

According to the Amended National Bank Establishment Proclamation, the NBE is obliged to take the necessary steps to establish, modernize, conduct, monitor, regulate and supervise payments, clearing and settlement systems.<sup>224</sup> Again, as per the National Payment System Proclamation, the NBE acts as a forum for the consideration of the policy framework of the national payment system.<sup>225</sup> Again, according to the same Proclamation, the national payment system of the country comprises of large value fund transfer system and retail fund transfer system.<sup>226</sup> Large value fund transfer system is electronic fund transfer which are typical of relatively high-value and which includes but not limited to interbank fund transfer, government fund transfer, clearing and settlement of securities of the government, and any other fund transfer system prescribed by the NBE as large value;<sup>227</sup> but, the NBE has not yet issued a directive that defines large value transfer. Contrary to large value fund transfer system, retail funds transfer system is a fund transfer system consists of the cheque clearing system which is operated and administered by the NBE or any retail fund transfer system operated by a licensed operator.<sup>228</sup> The definition given by the Proclamation to retail fund transfer is not clear, therefore, it will be better to refer to the definition given by the WB. As per the WB definition, retail payment system is defined as a payment that meets at least one of the following characteristics: the payment is not directly related to a financial market transaction; the settlement is not time critical; the payer, payee or both are individuals or non-financial institutions; either the payer, payee or both are not the direct participants of the payment system.<sup>229</sup> As per the WB, retail payment includes person-to-person, person-to-business, business-to-person, business-to-business, person-to-government, business-to-government, government-to-person, and government-to-business payments.<sup>230</sup> Again, as per the WB, there are four forms of retail payment instruments: *First*, paper-based instruments which include cash, cheque, money orders, and traveler cheque.<sup>231</sup> *Second*, electronic-based products which include the credit transfer using ATM, mobile phones, computer, internet, and any other electronic device, or the debit transfer made through electronic conversion of

---

<sup>224</sup> National Bank of Ethiopia Establishment (as Amended) Proclamation, Art 5(15).

<sup>225</sup> National Payment System Proclamation, Art 4(2)(k).

<sup>226</sup> National Payment System Proclamation, Art 2(14) & (22).

<sup>227</sup> National Payment System Proclamation, Art 2(14).

<sup>228</sup> National Payment System Proclamation, Art 2(22).

<sup>229</sup> 'Developing a Comprehensive National Retail Payments Strategy' (World Bank Financial Infrastructure Series, October 2012)6. < <http://documents.worldbank.org/curated/en/839121469729131991/Developing-a-comprehensive-national-retail-payments-strategy> > accessed 18May 2018.

<sup>230</sup> *Ibid.*

<sup>231</sup> *Ibid.*, 18.

cheques.<sup>232</sup> *Third*, card-based payment instruments which include the use of credit, debit, prepaid and any other smart-cards to transfer fund from the payer to the beneficiary.<sup>233</sup> The *fourth* is innovative payment products which mainly comprises e-many.<sup>234</sup> Thus, the small value electronic fund transfers made through electronic channels, card-based fund transfers, and e-money are part of the retail payment instruments in which their policy framework is defined under the national retail payment strategy of a country.

As it is mentioned in the above, the NBE is entrusted to issue the national payment system policies and strategies. Retail payment strategy is part and parcel of the national payment system; therefore, the power to formulate the retail payment strategy of the country lies with the NBE. By now, the NBE is coordination with the WB is drafting the retail payment strategy of the country.<sup>235</sup> The draft is in its infant stage, and the officers of the NBE are not volunteered to disclose the documents of the draft to the researcher.<sup>236</sup> The country has not yet issued a separate and comprehensive retail payment strategy, but many aspects of the retail payment strategy are included under the National Financial Inclusion Strategy (NFIS). Therefore, in the absence of separate and comprehensive retail payment strategy, the NFIS could be used as a gap filling strategy to know the stand of the Ethiopian government towards the e-banking business.

The National Council for Financial Inclusive is founded by the government to formulate a national financial inclusive strategy.<sup>237</sup> The Council is responsible to the Office of the Prime Minister and there is no any law which defines the establishment of this Council. The Council is recognized and established within the National Financial Inclusive Strategy issued by the Council itself. The members of the Council are; Minister of MOFED (chairperson), minister of Ministry of Agriculture and Natural Resources, with the Rank of Minister-Chief of Macroeconomic Planning, Effectiveness, Follow-up and Support, Commissioner of National Plan Commission, Director of Ethiopian Development Research Institute and Governor of the National Bank of Ethiopia.<sup>238</sup> The Vice-Governor of the NB serves as a Secretary of the

---

<sup>232</sup> Developing a Comprehensive National Retail Payments Strategy' (World Bank Financial Infrastructure Series, October 2012)18. < <http://documents.worldbank.org/curated/en/839121469729131991/Developing-a-comprehensive-national-retail-payments-strategy> > accessed 18May 2018.

<sup>233</sup> Ibid.

<sup>234</sup> Ibid,19.

<sup>235</sup> Interview with Ato Solomon Damitew, Principal Manager Payment Systems Over Sight and Development, National Bank of Ethiopia (Addis Ababa, 04 May 2018).

<sup>236</sup> Interview with Ato Solomon Damitew, Principal Manager Payment Systems Over Sight and Development, National Bank of Ethiopia (Addis Ababa, 04 May 2018).

<sup>237</sup> See, the 'Summary' section of the National Financial Inclusive Strategy.

<sup>238</sup> National Financial Inclusion Strategy (National Council for Financial Inclusion, April 2017)42.

Council.<sup>239</sup> In order to carry out its obligations the Council founded a National Steering Committee for Financial Inclusion (Financial Inclusive Secretariat), and the Secretariat is entrusted to formulate financial inclusive strategy as well as to monitor and evaluate the implementation of the strategy.<sup>240</sup> By the virtue of the power entrusted to it, the Financial Inclusive Secretariat in coordination with the WB has formulated the National Financial Inclusive Strategy.<sup>241</sup>

The National Financial Inclusion Strategy mandates the NBE among another thing to maintain safe, sound and stable financial sector; issue directives on operators of payment instruments and reassess the role, regulation and oversight of the technology service providers; strengthens regulatory and oversight capacity at NBE on electronic retail payments; review legal requirements on paper-based record keeping to remove obstacles for electronic transactions; conduct a comprehensive assessment of the legal, regulatory and institutional framework for secured transactions; review the directives on agent banking; issue directive on electronic banking, conduct a diagnostic to consider options for an effective dispute resolution mechanism (e.g financial sector ombudsperson) for the financial sector, covering regulated and unregulated financial technology service providers; promote shared payment systems and interoperability of the e-banking services; leverages providers to deploy ATM and POS terminals in rural communities; and conduct a detailed diagnostic of the legal, regulatory, supervisory and overall institutional framework for financial consumer protection.<sup>242</sup> The financial inclusion strategy includes significant issues of the e-banking business, but it has many limitations. In general, the current policy framework of the country has the following limits:

*First*, as it is stated in the above the country has not yet issued a comprehensive national retail payment strategy. The NBE is working with the World Bank to draft the retail payment strategy of the country, though it is in the infant stage.

*Second*, though the policy issues of the e-banking business are mainly addressed in the national retail payment strategies, in the absence of comprehensive retail payment strategy, the financial inclusive strategies are also a reference to know the policy framework of the country. But the policy objectives of the retail payment strategy and the financial inclusive strategy is different; the policy objective of the National Financial Inclusive Strategy is to

---

<sup>239</sup> National Financial Inclusion Strategy 42.

<sup>240</sup> National Financial Inclusive Strategy 42.

<sup>241</sup> National Financial Inclusion Strategy 42.

<sup>242</sup> National Financial Inclusion Strategy, 69-74.

achieve a universal access of the financial products and services by all adults, but the policy objective of the national payments strategy is to create a stable, sound and efficient e-banking products and services. The divergence of the policy objectives creates divergent policy intervention strategies. Thus, the use of the National Financial Inclusive Strategy with a different policy objective may lead to the implementation of erroneous strategies in the e-banking business of the country, which may, in the end, goes against the sound and efficient management of the e-banking products and services.

*Third*, the National Financial Inclusive Strategy dictates that the National Council for Financial Inclusive is set up by the government, but there is neither a proclamation nor a regulation that defines the establishment of such Council. As the National Financial Inclusive Council is not founded by law, the strategy formulated by the Council raises validity issue; thus, the use of the National Financial Inclusive Strategy to know the policy framework of the e-banking raises legality issue as well.

### **3.4 The Legal Framework of E-Banking Regulation in Ethiopia**

The electronic provision of banking products and services is regulated by numerous legal documents. The major legal documents that regulate e-banking are the Constitution, primary legislation(proclamation), secondary legislation (regulations and directives). The constitutional framework is discussed in the above<sup>243</sup> as it determines both the policy and legal framework of the e-banking regulations. Following the constitution, the main primary legislation that regulates e-banking is the National Payment System Proclamation 718/2011. In addition to this, some legal provisions of the primary legislation of Banking Business Proclamation, Micro-finance Business Proclamation, Computer Crime Proclamation No.958/2016, Anti-Money Laundering, and Terrorism Financing Proclamation, Commercial Code, Civil Code<sup>244</sup>, Amended National Bank Establishment Proclamation and Criminal code<sup>245</sup> have relevancy in regulating e-banking business. Within the category of secondary legislation, various directives and circular letters of the NBE mainly the Regulation of Mobile and Agent Banking Services Directive No. FIS/01/2012, Fraud Monitoring Directive No.

---

<sup>243</sup> See section 3.2, p.39.

<sup>244</sup>Civil Code Proclamation No. 165/1960, *Negarit Gazeta*, 19<sup>th</sup> year, Extraordinary Issue No.1, Article 1749 & 1750. [Herein after the Civil Code]

<sup>245</sup> The Criminal Code of The Federal Democratic Republic of Ethiopia Proclamation No. 414/2004, *Federal Negarit Gazetta*, Article 346, 348, 778 & 785. [Herein after The Criminal Code]

SBB/59/2014, Circular No. BSD/06/2013, Circular No. FIS/01/2014, and Circular No. FIS/02/2014 regulates the e-banking business in Ethiopia.

As it has already mentioned in the introduction part of this Thesis,<sup>246</sup> the Ethiopian commercial banks provide both traditional and modern banking services to their customers. The current legal framework does not allow the establishment of virtual banks, and due to this, no virtual bank is yet established in the country. The financial institutions, namely, banks and microfinance, which are already established to provide traditional banking services are the institutions which are allowed to provide e-banking products and services to their customers: no any other institution allowed to provide e-banking products and services. As the financial institutions are engaged in the provision of both traditional and e-banking services, the provision of these services is regulated by both the traditional and e-banking legal frameworks. The traditional banking services are mainly regulated by the Commercial Code and the Banking Business Proclamation No. 591/2008, but the e-banking regulation is mainly regulated by the National Payment System Proclamation No 718/2011 and its implementing directives. As a result of this, in discussing the regulations of the e-banking products and services where it is found necessary the regulation of traditional banking business is discussed.

As it mentioned in the above, the National Payment System Proclamation, which comprises six parts<sup>247</sup> and 39 provisions, is primarily intended to regulate the national payment system. As part of the national payment system, it also regulates e-banking products and services as well as sets the powers and functions of the enforcement organs. However, as we will see in the next sub-sections, the National Payment System Proclamation delegates most aspects of e-banking to be regulated by directives that was expected to be issued by the NBE, but, most of the supposedly implementing directives that were expected to be issued by the NBE has not yet issued with the exception of Mobile and Agent Banking Directive and some circular letters which clarifies the said Directive. But, by now, the NBE prepared a Draft Electronic Transfer Service Directive (Draft Directive), and this directive is distributed to the commercial banks, operators and Ethiopian Banker's Association for comment.<sup>248</sup> The

---

<sup>246</sup> See section 1.1, p.2.

<sup>247</sup> The six parts of the proclamation are: Part one General Part; Part two: Powers and Duties of the National Bank, and Issuance of Authorization; Part three: Settlement, Netting and Finality; Part four: Electronic Fund Transfer; Part five: Regulation and Oversight and Part Six: Miscellaneous Provisions.

<sup>248</sup> Interview with Ato Solomon Damitew, Principal Manager Payment Systems Over Sight and Development, National Bank of Ethiopia (Addis Ababa, 04 May 2018).

regulations provided by the Draft Directive are also included in the below discussions. But, before indulging to the detail regulatory framework, defining the terms used by the law is necessary to understand the real intention of the law. Due to this, the next section deals with the clarification of the ambiguous use of terms by the said laws.

### 3.4.1 Definition

As it is mentioned in the introduction part of this Thesis<sup>249</sup>, according to the National Payment System Proclamation, the term ‘fund transfer’ includes both traditional fund transfer and electronic fund transfer.<sup>250</sup> And the definition is given to the ‘electronic fund transfer’ equates to ‘e-banking’. Again, the Regulation of Mobile and Agent Banking Services Directive No. FIS/01/2012 equates ‘mobile banking’ with ‘e-banking’. According to the Directive, the term ‘mobile banking’ is defined as, “...*performing banking activities which primarily consists of opening and maintaining **mobile/regular accounts** and accepting deposits; furthermore, it includes performing fund transfer or cash in and cash out services using **mobile devices**.*”<sup>251</sup> [Emphasis mine]. By the definition, all the banking services; cash in, fund transfer and cash out services can be delivered using the ‘mobile banking services’. Again, the Directive defines ‘**mobile account**’ as “... *an account maintained by a customer in a financial institution in which debits and credits are effected by virtue of electronic fund transfer and which is used to conduct mobile banking activities as outlined in these directives.*”<sup>252</sup> By the literal meaning of the definition given to ‘mobile account’, ‘mobile account’ is a regular account in the financial institutions in which the cash in and cash out services are effected by virtue of the electronic fund transfer(e-banking). The last and most important definition in the said Directive is the definition given to ‘**mobile devices**’. The Directive defined ‘**mobile devices**’ to include mobile phones, smart phones, table personal computers, the point of sale terminals or any other similar devices.<sup>253</sup> Thus, the definition given to ‘mobile device’ is not limited to mobile phones only but it includes POS terminals, table personal computers, ATMs and any other similar electronic devices. Therefore, the Directive is named as ‘Regulation of Mobile and Agent Banking Services Directive’ which looks like as it only regulates mobile banking which is provided only through mobile phones, but by the definition given to ‘mobile banking’, ‘mobile account’, and ‘mobile devices’, it

---

<sup>249</sup> See section 1.1, p.1.

<sup>250</sup> See section 1.1, p.1&2.

<sup>251</sup> Regulation of Mobile and Agent Banking Services Directive No. FIS/01/2012, Art 2.11. [Herein after Regulation of Mobile and Agent Banking Service Directive).

<sup>252</sup> Regulation of Mobile and Agent Banking Service Directive, Art 2.10.

<sup>253</sup> Regulation of Mobile and Agent Banking Service Directive, Art 2.12.

indicates that such legal framework applies to all e-banking products and services delivered using any electronic devices including POS, ATM, mobile phones, smart phones, table personal computers and any other electronic devices. Moreover, Circular No. BSD/06/2013 states; “*It has to be recalled that the NBE has authorized some banks to engage in information-based mobile and/or internet banking services [up] until the relevant regulatory framework is put in place.*”<sup>254</sup> [Emphasis mine]. The circular states that the NBE has authorized the provision of mobile and/or internet banking services (e-banking) without providing adequate regulatory framework and due to this in the second paragraph of the same Circular it states, “*This is, therefore, to require all banks, already authorized to provide the aforementioned low-risk services, to apply for authorization from the NBE in line with provisions of Regulation of Mobile and Agent Banking Services Directive No. FIS/01/2012.*”<sup>255</sup> [Emphasis mine]. The cumulative meaning of the two paragraphs of the Circular indicates that the ‘Regulation of Mobile and Agent Banking Services Directive’ is intended to regulate the mobile and/or internet banking (e-banking) services rendered by the financial institutions. This indicates that the Directive equates ‘mobile banking’ with ‘e-banking’.

To alleviate the above-mentioned ambiguity, the Draft Electronic Fund Transfer Service Directive (hereinafter the Draft Directive), defines properly as to what constitutes ‘electronic fund transfer’; “... *any transfer of funds which is initiated by a customer, either totally or partially, through an electronic equipment so as to order, instruct, or authorize a financial institution to debit or credit an account.*”<sup>256</sup> [Emphasis mine]. As per the Draft Directive, three elements are required to say a fund transfer is electronic fund transfer. *First*, there should be a ‘transfer of fund’. Again, what constitutes ‘transfer of fund’ is defined by the Draft Directive, and according to it, ‘transfer of fund’ is the transfer of the fund to or from an account which includes but not limited to withdrawal, transfer between the account, and direct deposit of funds initiated using electronic equipment.<sup>257</sup> *Second*, the fund transfer should be made either totally or partially using electronic equipment. Again, what constitutes electronic equipment’ is defined by the Draft directive, and it defines as any electronic terminal including but not limited to computer, POS, ATM, Television, telecommunication devices (including telephone and internet), credit card, debit card, stored value

---

<sup>254</sup> Circular No. BSD/06/2013, first paragraph.

<sup>255</sup> Circular No. BSD/06/2013, second paragraph.

<sup>256</sup> Draft Electronic Fund Transfer Service Directive, National Bank of Ethiopia, 2017, Art 2.11. [Hereinafter, Draft EFT Directive].

<sup>257</sup> Draft EFT Directive, Art 2.29.

products/devices, and other similar electronic devices used to initiate electronic fund transfer services.<sup>258</sup> *Third*, the fund transfer initiated and made through the electronic channel should cause the debit or credit of the account of the customer. The terms ‘debit’ and ‘credit’ are accounting terms and the debiting of account results the reduction of the amount of money in the financial account, whereas crediting an account result the addition of money to the financial account. When we see the definition given by the Draft Directive, ‘electronic fund transfer’ is equated with ‘e-banking’.

With regard to the use of electronic equipment, two changes which were not in the Regulation of Mobile and Agent Banking Service Directive are introduced: one, in the Regulation of Mobile and Agent Banking Service Directive, the definition given to electronic equipment does not include Television, credit card, debit card and stored value card; and two, in the Regulation of Mobile and Agent Banking Service Directive the transfer of funds partially using electronic channels were not considered as electronic fund transfer but here in the Draft Directive, the partial use of electronic channel to transfer fund is also included as an electronic fund transfer.

By now, all banks introduced a core-banking system and through the system they provide e-banking products and services to their customers, any transfer of fund whether traditional or electronic fund transfer uses the core-banking system as well as the e-banking products and services, this, there is no traditional fund transfer in the banking business of the country; the traditional fund transfer services is only delivered by the microfinance institutions of the country. The definition given by the Draft Electronic Fund Transfer Directive and Draft Commercial Code to the same service is different. Having discussed the ambiguous and discrepant definitions given by the ongoing and draft laws, the next sections discuss the detail issues regulated by the Proclamation and its implementing directives.

### **3.4.2 Entry Regulation**

As per the Regulation of Mobile and Agent Banking Services Directive, it is only a legally established financial institution that can be engaged in the provision of e-banking products and services.<sup>259</sup> And again as per the said Directive, the financial institution is a bank or microfinance institution.<sup>260</sup> Thus, e-banking services can be provided only by banks and

---

<sup>258</sup> Draft EFT Directive, Art 2.13.

<sup>259</sup> Draft EFT Directive, Art 4.1.

<sup>260</sup> Draft EFT Directive, Art 2.7.

microfinance; and to provide such services the financial institutions should get prior approval from the NBE.<sup>261</sup> The entry requirements of the Regulation of Mobile and Agent Banking Directive, which is the ongoing directive, only provides the submission of three documents; business plan, operational policy and procedure, and risk management policy and procedure.<sup>262</sup> But, the Draft Directive added very significant entry requirement including but not limited to customer protection policies and procedures, model terms and conditions of the e-banking products and services, anti-money laundering/counter financing of terrorism policies and procedures, and risk assessment report of the operations to be performed through electronic channels.<sup>263</sup> But one thing that the reader should be notified before indulging to the detail discussion is that the researcher tries all his best to examine the practice, but under the guise of confidentiality both the officers of the NBE and the employees of the commercial banks were not volunteer to access the policy and procedure documents to the researcher,<sup>264</sup> as a result of this, for this section, the researcher is forced to employ doctrinal analysis method. But again, one thing that the reader should be aware is that the researcher did not access the details of the policy and procedure documents, but the researcher has seen the presence of the policy and procedure documents in a distant.<sup>265</sup> The officer of the NBE also assures that all the policy and procedure documents are prepared in accordance with the Regulation of Mobile and Agent Banking Service Directive.<sup>266</sup> Having informed about the reason behind the non-inclusion of the empirical part, the next sub-sections of the research discuss the entry regulations provided by both the Regulation of Mobile and Agent Banking Service Directive and the Draft Directive: in doing so, a comparative analysis method is employed.

### **3.4.2.1 Business Plan**

Like any other business, the startup of e-banking products and services begins with a business plan. It is the roadmap to achieve the end goals of the business. The proverb ‘where you fail to plan, you plan to fail’ describes the essence of the business plan in any businesses

---

<sup>261</sup> Draft EFT Directive, Art 6.1.

<sup>262</sup> Regulation of Mobile and Agent Banking Service Directive, Art 6.3.1, 6.3.2 & 6.3.3.

<sup>263</sup> Draft EFT Directive, Annex-I, p.31.

<sup>264</sup> Ato Kebede Demissie, Banking Examiner at the NBE, is not volunteer to access the policy and procedure documents to the researcher, Again Ato Chernet Kebede from Awash Bank, Ato Berihu Gebru from CBE, let alone to access the policy and procedure documents they are not even volunteer to discuss about the detail contents of such documents.

<sup>265</sup> Ato Kebede Demissie who is the Banking Examiner at NBE shows the researcher about the presence of the policy and procedure documents by a distant.

<sup>266</sup> Interview with Ato Kebede Demssie, Banking Examiner, National Bank of Ethiopia (Addis Ababa, 10 May 2018).

including in the e-banking business. It is through the business plan that the feasibility of the business is tested. That's why both the Regulation of Mobile and Agent Banking Service Directive and the Draft Directive considered it as a milestone to begin e-banking business. The Regulation of Mobile and Agent Banking Service Directive not only mandates the financial institution to prepare a business plan, but it also regulates the minimum requirements of the business plan; and as per the Directive, the business plan should at least include the following five matters:

- i. a brief analysis of the country's economy with particular focus on the financial system;
- ii. operation and financial viability of the intended mobile and agent banking services for at least three years'
- iii. pricing strategy including the initial transaction fee and charges that takes into account the sustainability of the mobile and agent banking service and the affordability of the service to the wider market;
- iv. products and services to be offered, target markets, regional distribution, and coverage of the service; and
- v. agency arrangement to be used. Technology service to be deployed, fee sharing arrangement, stakeholders and their respective role in the delivery of the service, impact of the services in improving financial services accessibility.<sup>267</sup>

The five requirements mentioned in the above are very crucial to determine the feasibility of the e-banking business. Particularly, the first and the second minimum requirements, a brief analysis of the country economy with particular focus to financial markets and the operational viability of the e-banking business are very important to determine the feasibility of the e-banking business. The third and the fourth minimum requirements, pricing and the distribution strategy of the e-banking products and services, are also very critical to determine the affordability and sustainability of the e-banking business. The distribution strategy is also very important to achieve the financial inclusion strategy of the county. The fifth and the last minimum requirement is defining the agency arrangement to be used as well as the rights and the responsibilities of the technology service providers and the possible outcome of the e-banking business in improving the financial accessibility. This part is also very crucial as it determines the obligations of the financial institutions, technology service providers, telecom service providers, agent bankers, and any other stakeholders. As these five requirements are minimum requirements, the financial institutions are allowed to include other issues which they believe that it is relevant in preparing a business plan.

As far as the contents of the business plan are concerned, the Draft Directive provides six minimum requirements in which five of them are what is provided under the Regulation of Mobile and Agent Banking Service Directive mentioned in the above, but with minor

---

<sup>267</sup> Regulation of Mobile and Agent Banking Service Directive, Art 6.3.1(i-v).

changes. The only new minimum requirement which is mandated to be included in the business plan is the global developments of the e-banking products and services.<sup>268</sup> The other five requirements are almost the direct replica of the ongoing directive but with minor changes in the wording; one, the Draft Directive replaces ‘mobile and agent service’ by ‘electronic fund transfer’, and two, it cancels the inclusion of the agency arrangement which is stated under roman number V of Art 6.3.1 of Regulation of Mobile and Agent Banking Service Directive; the agency arrangement (contract of agent bank) is excluded because such issues will be regulated by the Draft Agent Banking Directive.<sup>269</sup>

### 3.4.2.2 Operational Policy and Procedure Manual

As per the Regulation of Mobile and Agent Banking Service Directive, next to the business plan, operational policy and procedure manual are the second entry requirement.<sup>270</sup> Operational policies and working procedures are the policies and practices by which organizations rationalize and continuously improve the work they do through available knowledge and technology.<sup>271</sup> It includes team synergy, decision structure, methods, standards, systems and procedures that yield high performance and respond to changing circumstances.<sup>272</sup> It translates the business plan into operational capabilities. The business plan, which is mentioned in the above, will not have any value unless backed by operational policy: that’s why the Directive makes operational policy and working procedure manual as the second entry requirement to provide e-banking products and services. The Directive not only defines the need of the operational policy and working procedure manual, but it also regulates the minimum content of the operational policy and working procedure; as per the Directive, the operational policy and procedure manual should at least include:

- i. responsibilities of the board and senior management of a financial institution in relation to the new services;
- ii. the organizational structure of the mobile and agent banking functions and associated responsibilities;
- iii. details of products and services to be offered such as product features, fees and charges, and transaction limits for the products;

---

<sup>268</sup> Draft EFT Directive, Annex I, g(i).

<sup>269</sup> By now, both e-banking and agent banking (not e-banking, but a means of facilitation) are regulated by a single directive; Regulation of Mobile and Agent Banking Service Directive. But, the NBE prepares separate draft directives which regulates e-banking and agent banking namely the Draft Electronic Fund Transfer Directive and Agent Banking Directive respectively.

<sup>270</sup> Regulation of Mobile and Agent Banking Service Directive, Art 6.3.2.

<sup>271</sup> Alain Martin, ‘What is Policy? Strategic and Operational Policies and Good Governance’, p.41/110. At <<https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjsrJSb0ZPbAhXBRo8KHdK4DSUQFggjMAA&url=http%3A%2F%2Fwww.executive.org%2FBibliography%2FPolicy.pdf&usq=AOvVaw0nWDF8JOiyGHPaBhoYGAKK>> accessed May 20, 2018.

<sup>272</sup> Ibid.

- iv. detailed narrative description and workflow diagram of the services to be provided (including registration, account opening; cash in transactions, fund transfer/remittance, cash out procedures);
- v. accounting procedures and recording of transactions;
- vi. agent management where applicable;
- vii. internal control procedure;
- viii. the manner of reporting; and
- ix. complaint handling and redressal system.<sup>273</sup>

The Directive properly defines the minimum content of the operational policy and working procedure manual that the financial institutions should frame before they launch the e-banking business. The operational policy is not only important to protect the interest of the consumers but it is also very important to the continuity of the e-banking business. As per the Directive, in formulating operational policy and procedure manual, the role of the board and senior management of the financial institution comes at the forefront. Without clearly defining the responsibilities of the board as an institution and the role of the senior managers both as a management body and as an individual manager, what is planned in the business plan will not be achieved. As an extension of defining the role of the board and the management body of the financial institution, designing a proper organizational structure which defines the functions and associated responsibilities of the managers and the employees comes next. The third minimum content of the operational policy is the forms of the e-banking products and services to be offered with their respective fees and charges, and transaction limits for each product. The fourth content of the operational policy is the detail workflow diagram of the e-banking products and services; registration, account opening, cash in transactions, cash out transactions and electronic fund transfer. The accounting procedure and records, agent management, internal control mechanism, reporting manner, and internal complaint handling and redressal methods are also the important contents which are required to be included in the designing of the operational policy and working procedure of the e-banking business.

As far as operational policies and working procedure are concerned, the Draft Directive comes up with two new minimum contents which are not included in the ongoing Directive. The first is the delivery channel strategy and the second is the manner of overseeing the electronic terminals which are far from the branches of the online branch of the financial institution.<sup>274</sup> In addition to the addition of two new requirements, the Draft Directive incorporates minor changes in the wording of the nine minimum requirements which are

---

<sup>273</sup> Regulation of Mobile and Agent Banking Service Directive, Art 6.3.2(i-ix).

<sup>274</sup> Draft EFT Directive, Annex I h(vi&vii).

mentioned under Regulation of Mobile and Agent Banking Service Directive, but, such minor changes in the wording does not bring substantial changes; it only replaces ‘mobile and agent banking’ by ‘electronic fund transfer’ like what is mentioned under the business plan section in the above.

### **3.4.2.3 Risk Management Policy and Procedure**

Once the business plan, as well as the operational policy, are framed, the next task is how to manage the possible risks that the financial institution may face in doing its day to day activities. The development and implementation of appropriate risk management policy, procedures and actions are very critical to deal with the possible risks before it happens. Risk management policy provides proactive means to avert the dangers of the possible risks; that’s why the Directive mandates the financial institution to formulate risk management policy before they launch the e-banking business. Similar to the above two cases, the Directive not only requires the preparation of the risk management policy, but it also regulates the minimum contents of it; as per the Directive, the risk management policy should at least include:

- i. description of the inherent risks such as operational risks, reputation risks, legal risks and liquidity risks and specific policies, processes and systems that are in place to manage these risks; and
- ii. notwithstanding the provision stated above, description of the inherent risks and the specific policies and processes that are in place to deal with risks shall specifically addresses risks emanating from customer, agent, technology service provider, mobile network operator and financial institution perspective.<sup>275</sup>

As it has already mentioned in the introduction part of this Thesis,<sup>276</sup> e-banking is not free of risk: Thus, the financial institution which likes to launch e-banking should identify the risks associated with the e-banking and devise appropriate proactive measures to avert such risks. It is for this reason that the Directive mandates the financial institutions to identify the possible risks and the appropriate risk averting measures that could be taken by the financial institutions after they have launched their e-banking business. Again, as an extension of risk identification and devising a proper risk averting mechanism, the Directive mandates the financial institutions to identify the risks emanating from customers, agents, internet service providers, mobile network operators, and financial institutions, and devise a mechanism to avert it. As far as risk management policy is concerned, the Draft Directive does not bring

---

<sup>275</sup> Regulation of Mobile and Agent Banking Service Directive, Art 6.3.3(i-ii).

<sup>276</sup> See section 1.1, p.1.

any new things, only makes some changes in the wording of the above-mentioned minimum content requirements.

#### **3.4.2.4 Information Security Policy**

As an extension of the risk management policy, the Directive also mandates the financial institutions to prepare information security policy.<sup>277</sup> The financial institutions are obliged to secure the operating system of the e-banking products and service.<sup>278</sup> Thus, the financial institution is obliged to ensure secure operating system by defining: the user risks; infrastructure and software application risks; communication media risk; agent and third-party service providers risks; business continuity plan; and an interface feature of the application.<sup>279</sup> With regard to user risks, the financial institution is obliged to create adequate awareness to the customers on the information security including how to secure the PIN of the e-banking products and services.<sup>280</sup> Creating an informed user is very important to secure the interests of both the customers and the financial institutions. Customers should be adequately aware of the consequence of the non-secure use of their PIN and other information's related to the e-banking products and service. Again, as part of the infrastructure and software application risk management, the financial institutions are obliged to provide: information security standard; application error, message type and message handling; PIN and user authentication; financial and non-financial data storage; availability of services and backup; confidentiality of user information; data and transaction integrity; maintenance of audit trails, segregation of duties; and authorization control.<sup>281</sup> The proper installation and provision of the infrastructure and software application risk management help the financial institutions to provide secure, safe and efficient e-banking services to their customers.

With regard to the management of communication and media risks, the financial institutions are obliged to provide; communication protocol risk management system, data storage risk management, and availability and quality of the e-banking services.<sup>282</sup> The financial institution should ensure a very secure communication protocol as hackers may using

---

<sup>277</sup> Regulation of Mobile and Agent Banking Service Directive, Art 7.

<sup>278</sup> Regulation of Mobile and Agent Banking Service Directive, Art 7.1.

<sup>279</sup> Regulation of Mobile and Agent Banking Service Directive, Art 7.1.1-7.1.6.

<sup>280</sup> Regulation of Mobile and Agent Banking Service Directive, Art 7.1.1.

<sup>281</sup> Regulation of Mobile and Agent Banking Service Directive, Art 7.1.2 (i-x).

<sup>282</sup> Regulation of Mobile and Agent Banking Service Directive, Art 7.1.3(i-iii).

different software and malware can access the customer's account.<sup>283</sup> The financial institution should be sure that the e-banking service is initiated by the true customer and again the message is not changed at the time of communication to the main server. Effective data storage protection is also very important to protect the financial and non-financial interests of the consumers of the e-banking. As an extension of the security of the communication and media risks management, the financial institutions are also required to provide effective risk management system for agents and third-party service providers by providing tools for data encryption and message integrity, data storage and backup, physical and logical access to system, and authenticity and non-reputability of communications.<sup>284</sup>

According to the Directive, as part of the information security policy, the financial institutions should have a good and workable business continuity plan which at least includes: availability of services, disaster recovery site, standardizes way of the data center, redundancy of the network communication, and antivirus protection.<sup>285</sup> The availability of the e-banking services seven days a week and twenty-four hours a day is a mandatory requirement but sometimes due to system defects, such services may not be available. The existence of a disaster recovery site is also one of the mandatory requirement in providing e-banking and this is a precautionary remedy for the collapse of the operating system due to different reasons. A standardized data center of the operating system of the e-banking is very critical to recover and check any electronic fund transaction made using the operating system. Redundancy of network communication is crucial to the availability of the e-banking services seven days a week and twenty-four hours a day, this is achieved by having alternative network communications that may be used to provide the e-banking service where one of the network communication failed. Last but not least with regard to business plan continuity is antivirus protection, the financial institutions are required to install the latest technology and software to protect the e-banking operating systems from computer viruses.<sup>286</sup> As an extension of the continuity plan, the financial institutions are also required to interface their operating systems with other financial institutions operating the system.<sup>287</sup> The interfacing of the operating system enables the e-banking services provided by different financial institutions to be interoperable. Interoperability of the operating systems enables the

---

<sup>283</sup> The State of Security at < <https://www.tripwire.com/state-of-security/security-data-protection/hackers-steal-60-million-from-taiwanese-bank-using-bespoke-malware/> > accessed 30March 2018.

<sup>284</sup> Regulation of Mobile and Agent Banking Service Directive, Art 7.1.4(i-iv).

<sup>285</sup> Regulation of Mobile and Agent Banking Service Directive, Art 7.1.5(i-v).

<sup>286</sup> Regulation of Mobile and Agent Banking Service Directive, Art 7.1.5(v).

<sup>287</sup> Regulation of Mobile and Agent Banking Service Directive, Art 7.1.6.

customers of one financial institution to use the electronic terminal of another financial institution which in turn helps to achieve the financial inclusive goal of the country.

### **3.4.2.5 Consumer Protection Policy**

Consumer protection policy is also one of the critical policies which are expected to be prepared by the financial institutions before they launch the e-banking products and services.<sup>288</sup> The Directive provides the minimum contents of the consumer protection policies of both e-banking and agent banking services, but since agent banking is outside of the scope of the study, the research only discussed the minimum requirements of consumer protection policy of the e-banking services. And according to the Directive, the minimum requirements of the consumer protection policies associated with e-banking should at least include: customer identification procedure; protection of customer's financial information; mandatory disclosure of the terms and conditions of the e-banking products and services; the risks and responsibilities of the consumers and the internet service providers; transparency in the pricing of the e-banking products and services; help-desk, customer-care telephone lines, and disclosure of the details of the help-desk; the availability of at least the last ten transactions conducted online; notification of the customers on the timeframe and circumstances in which stop-payment orders could be accepted; the complaint handling system; and the reasonable time that the complaints of the customers are addressed which in any case shouldn't be more than thirty working days from the date of lodging of the complaint.<sup>289</sup> As far as the customer protection policy is concerned, the Draft Directive does not add a new minimum requirement, it is the direct replica of the ongoing Directive with the exception that the duty of availability of at least the last ten transactions online lowered to five transactions.<sup>290</sup>

### **3.4.2.6 Minute of the Board of Directors**

The last but not least entry requirement is the minute of the board of directors that indicates that the board has reviewed and endorsed the provision of the e-banking products and services.<sup>291</sup> In deed, all the above-mentioned policies are prepared and approved by the top management body of the financial institution; board of directors. But, as an extension of the above policies, the minute of the board of directors that approves the provision of e-banking products and services is also required to be submitted by attaching with the above-mentioned policies. As far as e-banking is concerned, the minute of the board of directors is the last

---

<sup>288</sup> Regulation of Mobile and Agent Banking Service Directive, Art 12.

<sup>289</sup> Regulation of Mobile and Agent Banking Service Directive, Art 12.1, 12.4, 12.5, 12.7-12.12.

<sup>290</sup> Draft EFT Directive, Art 34 and Annex I, d(v), P.31.

<sup>291</sup> Regulation of Mobile and Agent Banking Service Directive, Art 6.3.4.

entry requirement, but, with regard to agent banking, in addition to the six entry requirement mentioned in the above, the financial institutions are obliged to prepare agent due diligence policy and procedure and declaration of agent suitability assessment;<sup>292</sup> penalty matrix that could be applied on agents who violates the contractual agreements and for malpractices;<sup>293</sup> contractual agreement entered with operators and telecom companies;<sup>294</sup> and such other information required by the NBE.<sup>295</sup> As it has already mentioned somewhere else, agent banking is outside of the scope of the study.

### **3.4.2.7 Pilot Period Test**

Once the financial institution submits all the requirements specified in the above, the NBE shall either approve for a pilot launch or reject the application and communicate the same to the applicant in writing.<sup>296</sup> In the ongoing Directive within how many days the NB may approve or reject the application of the financial institution is not specified. The pilot period is a minimum of two months and a maximum of six months.<sup>297</sup> The pilot period is intended to test the qualification of the financial institution whether it is capable of providing e-banking services or not. Within the pilot period the financial institution is only allowed to provide e-banking services on a limited scale,<sup>298</sup> but again what constitutes 'limited scale' is not defined under the Directive, the NBE is not also delegated to determine what constitutes limited scale, for this reason, the requirement of limited scale which is stated in the Directive is open to interpretation. Again, in the pilot period, the financial institution is not allowed to make a promotion about the launching of the e-banking products and service.<sup>299</sup> Whatever the case, at the end of the pilot period, the financial institution is obliged to make a detailed pilot test report to the NBE which contains at least;

- i. the volume and type of transaction executed,
- ii. the outcome of the pilot transactions, errors, omissions identified,
- iii. complaints received from customers,
- iv. any other issues and deviations identified, and
- v. modifications and changes sought as a result of the pilot.<sup>300</sup>

---

<sup>292</sup> Regulation of Mobile and Agent Banking Service Directive, Art 6.3.5.

<sup>293</sup> Regulation of Mobile and Agent Banking Service Directive, Art 6.3.6.

<sup>294</sup> Regulation of Mobile and Agent Banking Service Directive, Art 6.3.7.

<sup>295</sup> Regulation of Mobile and Agent Banking Service Directive, Art 6.3.8.

<sup>296</sup> Regulation of Mobile and Agent Banking Service Directive, Art 6.4.

<sup>297</sup> Regulation of Mobile and Agent Banking Service Directive, Art 6.5.

<sup>298</sup> Regulation of Mobile and Agent Banking Service Directive, Art. 6.6.

<sup>299</sup> Regulation of Mobile and Agent Banking Service Directive, Art 6.6.

<sup>300</sup> Regulation of Mobile and Agent Banking Service Directive, Art. 6.6.1-6.6.5

As it can be easily seen from the indented paragraph, the financial institutions are mainly obliged to include the problems it has faced in providing e-banking services in the pilot period. Thus, the report is expected to be full-fledged which enables the NBE to examine whether the financial institution is competent enough to run the e-banking services or not.<sup>301</sup> The NBE is not limited to the examination of the pilot test report which is submitted by the financial institution, but it is also obliged to make a business risk assessment on the service rendered in the pilot period on its own initiation.<sup>302</sup> Based upon the pilot test report and business risk assessment made by itself, the NBE shall grant or reject the authorization within a maximum of one month from the date of submission of the pilot test report.<sup>303</sup> If the NBE grant the authorization there is no additional procedure and the financial institution will continue the provision of the e-banking services, but if the NBE rejects the authorization the financial institution shall be given three months to correct its weakness and resubmit a pilot test report at the end of the three months' time.<sup>304</sup> But, where the financial institution failed to correct its weakness within the three months, it shall phase out from providing e-banking products and services launched in the pilot period as per the instruction of the NBE.<sup>305</sup>

Unlike the above-mentioned cases, as far as the pilot period is concerned, the Draft Directive makes very significant changes. As it is mentioned in the above, the current Directive does not define within how many days the NBE is obliged to respond to the application made by the financial institution; having identified this problem, the Draft Directive mandates the NB to approve or reject the application for provision of e-banking services within thirty business days.<sup>306</sup> Again, in the current Directive, the maximum time of the pilot period is six months, but the Draft Directive shortens this into three months.<sup>307</sup> The third change determines what constitutes 'limited scale', as it is mentioned in the above, the current Directive does not define what constitutes 'limited scale', and having identified this problem the Draft Directive defines 'limited scale' for the purpose of the pilot period as, "*...[I]nvolving customers whose number ranges from 100 to 150 and transaction volume ranging from 300 to 450 without taking any promotion.*"<sup>308</sup> Thus, in the pilot period time, first, the financial institution can only provide e-banking products and services for a minimum of 100 customers and a

---

<sup>301</sup> Regulation of Mobile and Agent Banking Service Directive, Art. 6.7.

<sup>302</sup> Regulation of Mobile and Agent Banking Service Directive, Art 6.7.

<sup>303</sup> Regulation of Mobile and Agent Banking Service Directive, Art 6.7.

<sup>304</sup> Regulation of Mobile and Agent Banking Service Directive, Art. 6.8.

<sup>305</sup> Regulation of Mobile and Agent Banking Service Directive, Art. 6.9.

<sup>306</sup> Draft EFT Directive, Art 6.1.

<sup>307</sup> Draft EFT Directive, Art 6.2

<sup>308</sup> Draft EFT Directive, Art 2.22.

maximum of 150 customers. Second, the transaction volume should not be below 300 and above 450. Third, similar to the current regulation, in the pilot period time, no promotion is allowed. The fourth change is associated with the time limit that the pilot test report is submitted. Under the current regulation, no time is specified within how many days the pilot period test should be reported to the NB, and the Draft Directive having identified this drawback mandates the financial institutions to submit such pilot period test report within one month after completion of the pilot period granted by the NBE.<sup>309</sup> The fifth change is the Draft Directive provides the suspension of the pilot period if it is not implemented within three months from the date of authorization.<sup>310</sup> The last but not least change is associated with the addition or replacement of new e-banking services; as per the Draft Directive, where the financial institution likes to add new or replace the existing e-banking products and services, the financial institution should apply to the NBE by submitting the necessary documents including operational policies and procedures, and risk management policies associated with the new additions or changes.<sup>311</sup> But, the Draft Directive does not make any change as to the content of the pilot period test report; it is copy and paste.

### **3.4.3 Operational Regulation**

Once the financial institutions begin the provision of e-banking products and services by fulfilling the entry requirements mentioned in the above, they are not at liberty to provide the said products and services without regulations: there are operational regulations that are aimed to protect the interest of both the institutional investors and the consumers of the e-banking products and service. The operational regulations provided by the National Payment System Proclamation, Regulation of Mobile and Agent Banking Service Directive, Draft Electronic Fund Transfer Service Directive and Commercial Code (including the Draft Commercial Code) are discussed in the following sub-sections.

#### **3.4.3.1 Terms and Conditions of the E-banking Service Agreements**

As we all know, there are three types of traditional banking services; cash in services, cash out services and fund transfer services. The two traditional banking services, namely, cash in and cash out services are only accessed when a customer has a financial account within the financial institution; and this customer-bank relationship is defined by ‘contract of deposit’. But, the third traditional banking service, fund transfer, is accessed by a ‘contract of fund

---

<sup>309</sup> Draft EFT Directive, Art 6.3.

<sup>310</sup> Draft EFT Directive, Art 6.11.

<sup>311</sup> Draft EFT Directive, Art. 6.12.

transfer'. Thus, in the traditional banking services, there are two agreements; namely, contract of deposit and contract of fund transfer; the terms and conditions of such contracts is determined by the free will of the parties but subject to limitations provided by different laws.<sup>312</sup> As it has been noted earlier, the traditional banking services are regulated by the provisions of the Commercial Code, though not adequate, the Code provides some important legal frameworks as to the terms and conditions of the contract of deposit and contract of fund transfer. To begin by the contract of deposit, the Code defined the contract of deposit as follows:

The contract of deposit of funds renders the bank owner of the funds deposited, irrespective of the mode of deposit. The bank may dispose of these funds in respect of its professional activity, ***subject to their repayment under the conditions provided in the contract***: Provided that the bank shall not acquire the title to nor the right to dispose of coins or other individual monetary tokens in respect of which ***there is a provision that they shall be refunded in kind***<sup>313</sup>. [Emphasis mine]

As per the Code, the bank is the owner of the funds deposited by its customers but subject to repayment based the terms and conditions stated under the contract of deposit, but, where the parties agree on the refund of specific coins or monetary coins in kind, the bank does not have the ownership right but refund it in kind as per the agreement. The phrases, "... *subject to their repayment under the conditions provided in the contract...*" and "... *there is a provision that they shall be refunded in kind*" indicates the importance of the terms and conditions of the contract made between the depositor and the bank. Similar to the contract of deposit, the terms and conditions of the traditional fund transfer are determined by the parties: Art 903(2) of the Commercial Code states, "[t]he conditions of the issue of transfer orders shall be as agreed by the parties." Thus, in the traditional banking services, similar to the contract of deposit, the terms and conditions of the fund transfer agreement are determined by the free will of the parties subject to the limitations provided by the mandatory provisions of the law.

In e-banking products and services, similar to the traditional banking services, the agreement of the parties has a paramount importance, but what makes it different from the traditional banking services is it incorporates sophisticated terms that are introduced due to the unique nature of e-banking products and services. The National Payment System Proclamation mandates the commercial banks to issue standard terms and conditions for electronic fund transfers and the stored value cards applicable to all its customers without any

---

<sup>312</sup> Civil Code, Art 1711.

<sup>313</sup> Commercial Code of the Empire of Ethiopia Proclamation No. 166/1966, *Negarit Gazzeta*, 19<sup>th</sup> year, Extra Issue No. 3, Art 896. [Here in after, Commercial Code.]

discrimination.<sup>314</sup> Thus, the commercial banks are obliged to issue separate standard terms and conditions for M-banking, I-banking, ATM banking, POS services, M-money and M-wallet. The standard terms and conditions are subject to approval by the NBE for its use by the banks.<sup>315</sup> Even if the commercial banks want to make changes to the standard terms and conditions of the e-banking, they should get prior approval from the NBE<sup>316</sup>. Over that, the NBE is a delegate to determine the basic terms and conditions of the e-banking service agreements by a directive.<sup>317</sup> But the in issuing the Regulation of Mobile and Agent Banking Service Directive, the NBE failed to incorporate provisions that regulate the basic terms and conditions that financial institutions should consider in preparing standard terms and conditions of e-banking service agreements: the directive only mandates the commercial banks to disclose the standard terms and conditions of the e-banking service agreements to their customers.<sup>318</sup> Having identified the drawbacks of the ongoing directive, the Draft Directive regulates the basic terms and conditions of the e-banking service agreements.

The Draft Directive, which is the direct replica of the US Electronic Fund Transfer Act, adequately regulates the minimum contents of the standard terms and conditions of the e-banking products and services. As per the Draft Directive, the terms and conditions of the e-banking products and service should include: The customer's liability for unauthorized EFT and notice of the advisability of prompt reporting of any loss, theft, or unauthorized means of access; the procedure for reporting; namely, telephone number and address of the person or office to be notified in the event that the customer believes there is unauthorized access to his account or in the case of loss or theft of any loss of the payment instrument; the procedure of verification of the complain/report of the customer to the unauthorized EFT, loss, or theft of the payment instrument and when such complain was made; the type and nature of e-banking products and services in which the customer can access, including any limitations on the frequency or transaction amount of such electronic transfers; the fees and charges of the e-banking transactions; the customer's right to stop payment of preauthorized EFT and the procedure to initiate such stop payment order; the customer right to receive e-banking transaction receipts/documents; summery of error resolution procedure; the conditions of the liability of the financial institution; the circumstances of the disclosure of the personal financial information of the customer; a notice to the customer that additional fees may be

---

<sup>314</sup> National Payment System Proclamation, Art 19(1).

<sup>315</sup> National Payment System Proclamation, Art 19(2).

<sup>316</sup> National Payment System Proclamation, Art 19(2)..

<sup>317</sup> National Payment System Proclamation, Art 19(3).

<sup>318</sup> Regulation of Mobile and Agent Banking Service Directive, Art 12.5.

imposed if the customer uses electronic channels owned by other banks or any other national, regional or local network; any fees for the issuance and use of electronic payment instrument; the procedure to initiate complaint investigation and resolution procedure; the duty of the customer to confidential use of the payment instrument and the liability of the breach of confidentiality of the payment instrument; and the manner and condition of the termination of the EFT.<sup>319</sup> These are the minimum contents that the commercial banks are mandated to include in the standard terms and conditions that are going to be prepared by the commercial banks when the Draft Directive come into effect. But in addition to these minimum requirements defined by the Draft Directive, the inclusion of other terms and conditions is allowed so far as it is not contrary to the minimum conditions mentioned by the Draft Directive.<sup>320</sup>

The standard terms and conditions prepared by the commercial banks should not create liabilities and responsibilities to customers which exceeds to those liabilities and responsibilities set out in the Draft Directive.<sup>321</sup> This is the general standard which is provided by the Draft Directive in additional to the defining of the minimum contents of the terms and conditions of the e-banking service agreements. Over that, the financial institution has the obligation to disclose the standard terms and conditions of the e-banking at the time of conclusion of the e-banking contract free of charge.<sup>322</sup> This obligation of disclosure is extended up to the delivery of the copy of the e-banking service agreement to the customer prior to or at the time of initial use of electronic payment instrument, and at any other time requested to do so by the customer.<sup>323</sup> The banks are also obliged to avail the standard terms and conditions at all branches and their agents.<sup>324</sup> The standard terms and conditions should be also in writing, prepared in Amharic or any other language that the customer understands.<sup>325</sup>

The Draft Directive not only regulates the initial preparation of the terms and conditions of the e-banking agreements but it also regulates the changes that could be made by the financial institutions to the initial terms and conditions of the e-banking agreements.<sup>326</sup> The financial institution can vary the standard terms and conditions of the e-banking agreements after

---

<sup>319</sup> Draft EFT Directive, Art. 7.5(a-o).

<sup>320</sup> Draft EFT Directive, Art. 7.2&36.1.

<sup>321</sup> Draft EFT Directive, Art. 7.2.

<sup>322</sup> Draft EFT Directive, Art 7.5.

<sup>323</sup> Draft EFT Directive, Art 7.3.

<sup>324</sup> Draft EFT Directive, Art 7.4.

<sup>325</sup> Draft EFT Directive, 7.5.

<sup>326</sup> Draft EFT Directive, Art 9.

providing a notice at least fifteen days prior to the effective date of the change, if such variation; imposes or increases charges, increases the customer's liability, adjusts the transaction limits, or any other change that would result in greater cost or liability for the customer or decreased access to the customer's account.<sup>327</sup> The financial institution shall notify such variation to the customer using one or more of the following means: in the periodic statement of the customer's account; notice at ATM, POS or any other electronic terminal; notice by SMS, on the official website of the financial institution for products and services delivered through the internet(I-banking); by voice communications if such product or service is provided entirely by voice communication only; at its branches by traditional notification means, or any other means it deems suitable to the customers of the financial institution.<sup>328</sup> In principle, the Draft Directive obliges the financial institutions to provide prior notice for possible changes that results in the reduction of the interest of the customer, but exceptionally the Draft Directive allows the change of the terms and conditions of the e-banking agreement without prior notification to the NBE if such change is necessitated by an immediate need to restore or maintain the security of the EFT or an individual account.<sup>329</sup> And if such change which is made without prior notification to the customers is permanent change, the financial institution should provide immediate subsequent notification to the NBE.<sup>330</sup>

As it is mentioned in the above, as far as the standard terms and conditions is concerned the ongoing directive does not provide adequate regulations. Again, the coming directive, Draft Directive, has failed to regulate some important issues of the e-banking service agreements; thus, the current regulation is surrounded by the following legal and practical limits:

*First*, as it is mentioned in the above, the NBE is delegated to determine the basic terms and conditions of the e-banking service agreements by a directive, but the NBE has not yet issued a directive. The ongoing directive, Regulation of Mobile and Agent Banking Service Directive, does not regulate the basic terms and conditions of the e-banking service agreements. Having identified the drawback of the ongoing directive, the Draft Directive regulates the minimum contents of the terms and conditions of the e-banking service agreements, but as this directive a mere draft, there is no binding directive that regulates the basic terms and conditions of the e-banking agreements. Thus, by now, the commercial banks

---

<sup>327</sup> Draft EFT Directive, Art 9.1(a-d).

<sup>328</sup> Draft EFT Directive, Art 9.2(a-f).

<sup>329</sup> Draft EFT Directive, Art 9.3.

<sup>330</sup> Draft EFT Directive, Art 9.3.

are arbitrarily preparing the standard terms and conditions of the e-banking service agreements.<sup>331</sup>

*Second*, the Regulation of Mobile and Agent Banking Service Directive mandates the commercial banks to disclose the standard terms and conditions to their customers for signature, but in practice, the commercial banks do not access the basic terms and conditions of the e-banking service agreements; what the banks do is they order the customer to refer the basic terms and conditions to their websites.<sup>332</sup> For example, the CBE orders its customers to refer to its official website for its detail regulations, but in its official website the said documents (basic terms and conditions) are not attached. All commercial banks have standard terms and conditions which are approved by the NBE for accessing to their customers, but in practice the commercial banks only disclose a very short form (application form) to their customers for signature; thus, the commercial banks are not acting in accordance to the regulations. The NBE was required to discover this problem through inspection and take appropriate remedy, but the NBE is not carrying out its obligations properly.

*Third*, even the application form where the commercial banks provide for signature as a standard terms and conditions is prepared only by Amharic and English languages. In dead, as per the ongoing directive, there is no regulation that mandates the commercial banks to prepare the standard terms and conditions by a language other than the Amharic and English, but as the end goal of the basic terms and conditions is to create awareness on the rights and responsibilities of the customers, it would be better if it is prepared by the language that the customers could read and understand; where the customers cannot read and understand the language of the standard terms and conditions, the end goal of its existence will be defeated. As a result of this, to attain its final goal the commercial banks are impliedly obliged to prepare such standard terms and conditions in a language which can be read and understand by its customers, though there is no explicit regulation that mandates the commercial banks to prepare the terms and conditions in a language other than Amharic. But as it is mentioned in the above, in practice the banks prepared the standard terms and conditions only by Amharic and English, this is also one of the drawbacks of the current regulation.

---

<sup>331</sup> Interview with Ato Ephrem Baraki, Senior Legal Expert, National Bank of Ethiopia (Addis Ababa, 09 August 2018).

<sup>332</sup> Interview with Ato Ephrem Baraki, Senior Legal Expert, National Bank of Ethiopia (Addis Ababa, 09 August 2018).

### 3.4.3.2 Preauthorized Electronic Fund Transfer Services

As it is mentioned in the above, preauthorized electronic fund transfer service is a new form of e-banking which is found in its infant stage. But, by now, many customers of the commercial banks are attracted by this service, as a result of this; the number of users of the preauthorized electronic fund transfer is increasing from time to time. One thing that should be clear at this level is that the commercial banks of the country were not providing preauthorized fund transfer services by the traditional mode of delivery. Thus, the absence of experience on the one hand and the sophistication of the technology on the other makes the provision of preauthorized electronic fund transfer problematic; and the presence of such problems calls for the strict regulation of the preauthorized fund transfer services.

As far as the regulation of the traditional preauthorized fund transfer is concerned, the 'Banking Transactions' section of the Commercial Code is silent; the Code neither recognized nor prohibited the provision of the preauthorized fund transfers. Coming to the preauthorized electronic fund transfer, similar to the Commercial Code, the current regulations (National Payment System Proclamation and the Regulation of Mobile and Agent Banking Service Directive) are silent. But, unlike to the current regulations, the Draft Directive provides some important regulations.

As it has already mentioned in the above, the Draft Directive is the direct replica of the US Regulation E; particularly Part V of the Draft Directive, the part which deals with the regulation of 'preauthorized electronic fund transfer service', is the direct copy of Art 1393d(b) and Art 1693e(a) of the US EFT Act. As per the Draft Directive, like any form of e-banking, the customer can by a written terms and conditions authorize his bank to make preauthorized electronic fund transfers to a third party.<sup>333</sup> Once the bank accepted the authorization, it has the obligation to make the said transfers to the said party pursuant to the orders of its customers. As preauthorize EFT service is initiated by the unilateral willingness of the customer, similar to its initiation, the cancellation of such service does not require court orders rather the customer can again unilaterally cancel his authorization without the participation of the beneficiary of the fund transfer.<sup>334</sup> But, the customer cannot arbitrarily cancel his authorization; the customer can only cancel his authorization at least before one

---

<sup>333</sup> Draft EFT Directive, Art 14.1.

<sup>334</sup> Draft EFT Directive, Art 14.3.

working day preceding the scheduled date of the transfer.<sup>335</sup> In addition to the unilateral cancellation, preauthorized electronic fund transfer can be terminated by the mutual agreement of the transferor and the beneficiary of such transfer.<sup>336</sup> In principle the cancellation of the authorization shall be effective immediately, but exceptionally the cancellation of the authorization may be effective after the lapse or the fulfillment of some conditions specified under the terms and conditions of the preauthorized EFT service agreement.<sup>337</sup> Again, for preauthorized EFT services terminated by the mutual consent of the transferor and the transferee, the transferor has automatic and immediate right to dishonor payments.<sup>338</sup> As it is stated in the above, the bank has only the obligation to transfer the said funds regularly based on the authorization received from its customer; but in relation to this, for preauthorized fund transfers made at least once in each successive sixty-day period, the bank has also the obligation to notify the beneficiary whether his account is credited or not.<sup>339</sup> In the end, the absence of regulation on the current regulation is the bold limits of the country's e-banking regulation. Regarding the practice, as it is found in its early stage, though the researcher tries to search users of this service for interview, it has failed to find a user; but, according to the officer of the NBE, as far as regulation issues are concerned no problem is reported.<sup>340</sup>

### **3.4.3.3 Cheque or Other Paper Based Payment Instrument Truncation**

In addition to the fiat money, the Commercial Code recognized some commercial instruments as a payment method. Commercial instruments are one form of negotiable instrument, and negotiable instrument is defined by the Commercial Code as “... *any document incorporate a right to entitlement in such manner that it be not possible to enforce or transfer the right separately from the instrument.*”<sup>341</sup> As we can see from the definition given by the Commercial Code negotiable instrument constitutes three elements; *first*, it is a document(paper-based), *second*, it incorporates a right to entitlement, and third, such entitlement cannot be enforced or transferred by separating from the instrument; the presentment of the negotiable instrument is mandatory for exercising the entitlement

---

<sup>335</sup> Draft EFT Directive, Art 14.3.

<sup>336</sup> Draft EFT Directive, Art 14.5.

<sup>337</sup> Draft EFT Directive, Art 14.4.

<sup>338</sup> Draft EFT Directive, Art 14.4.

<sup>339</sup> Draft EFT Directive, Art 14.2.

<sup>340</sup> Interview with Ato Ephirem Baraki, Senior Legal Expert, National Bank of Ethiopia (Addis Ababa, 09 August 2018).

<sup>341</sup> Commercial Code, Art 715(1).

incorporated in it. The Commercial Code recognizes three class of negotiable instruments; namely, commercial instruments, transferable securities, and documents of title to goods.<sup>342</sup> Commercial instruments are within the compound of the study but the other two classes are not. Again, the Commercial Code defines commercial instruments as, "...*negotiable instruments setting out an entitlement consisting in the payment of sum of money.*"<sup>343</sup> The definition comprises of two elements: one, commercial instrument is a negotiable instrument which fulfilled the three elements of negotiable instrument mentioned in the above; and two, it incorporates an entitlement consisting of in the payment of sum of money. Thus, what makes commercial instruments different from other negotiable instrument is because they are exchanged for nothing but for money and money only. The Commercial Code not only defines what constitutes commercial instruments but it also regulates the kinds of the commercial instruments with their respective legal framework starting from their issuance to their transfer and presentment of such commercial instruments for settlement.<sup>344</sup> The commercial instruments recognized by the Commercial Code are bill of exchange, promissory note, cheque, traveler cheque and warehouse goods certificate.<sup>345</sup> The warehouse goods certificate is a commercial instrument but its detail legal framework is defined under the provisions of the Civil code.<sup>346</sup> Coming to the practice, it is only cheque and warehouse goods certificate which are among the practically used commercial instruments that replaces money. While cheque is used by the customers of commercial banks warehouse goods certificate is usually and mainly used by ECX. Promissory note, bill of exchange and travelers' cheque are not in use. As any negotiable instruments, the settlement of commercial paper is possible only when the paper-based document is presented before the commercial banks.<sup>347</sup> But now through the use of technology, these paper-based commercial instruments can be presented before the bank for payment using electronic channels. The conversion of cheque or other paper-based payment instrument using the electronic channels into electronic form for transmission to the drawee bank is called truncation.<sup>348</sup>

As it is noted in the above, in the traditional banking practice the commercial instruments deposited in the bank were only physically presented to the drawee bank to get the amount of

---

<sup>342</sup> Commercial Code, Art 715(2)

<sup>343</sup> Commercial Code, Art 732(1).

<sup>344</sup> Commercial Code, Art 732- 895.

<sup>345</sup> Commercial Code, Art 732(2).

<sup>346</sup> Civil Code, Art 2813-2824.

<sup>347</sup> Commercial Code, Art 715(1).

<sup>348</sup> Wikipedia 'Cheque Truncation' at < [https://en.wikipedia.org/wiki/Cheque\\_truncation](https://en.wikipedia.org/wiki/Cheque_truncation) > access 25 March 2018.

the money debited to the drawer's account, which was a cumbersome process and resulted in the delay in the clearing of cheques. Cheque or other paper-based payment instrument truncation is developed to overcome the limitations of the traditional clearing system that requires several days. By doing so, the time and cost of the clearance process is reduced substantially. Having recognized these benefits, the national payment system law of Ethiopia recognizes and regulates the truncation of commercial instruments into electronic form for settlement.<sup>349</sup>

According to Proclamation, a check or other paper-based payment instrument may be converted into electronic form using the electronic channels for transmission to the payee bank.<sup>350</sup> Again, according to the Proclamation, the conversion of the cheque or other payment instrument into electronic form should fulfill the following three elements to validly submit for settlement using the electronic channels: **First**, it must be a cheque or other paper-based payment instrument recognized as a commercial instrument under the Ethiopian laws. As it mentioned in the above, the Commercial Code lists down the types of commercial instruments that entitles a holder to a sum of money; these are bill of exchange, promissory note, cheque and traveler cheque. The phrase “[a] cheque or other paper-based payment instrument...”<sup>351</sup> should be interpreted in light of the legally recognized commercial instruments stated under the Commercial Code. Therefore, according to the Ethiopian context, the payment instruments which can be truncated using the electronic channels for transmission to the payee bank are bill of exchange, promissory note, cheque and traveler cheque. **Second**, it must be converted into electronic form by storing its image and inserting its corresponding information to the system. **Third**, the stored image and corresponding information should be transmitted to the bank for clearance. Once you stored the image and its corresponding information, it is a simple click that the paper-based instrument transmitted to the bank and the payee account will be credited within T+1. In dead, this e-banking service has not yet begun by the commercial banks of the country.

Upon the submission of the paper-based payment instrument using the electronic channel and withdrawing or transferring money to an account, the original paper-based document is not negotiable, and it is to be destroyed;<sup>352</sup> once payment is made using the electronic channels, no second payment by presenting the physical paper-based instrument before the issuing

---

<sup>349</sup> National Payment System Proclamation, Art 24.

<sup>350</sup> National Payment System Proclamation, Art 24(1).

<sup>351</sup> National Payment System Proclamation, Art 24(1).

<sup>352</sup> National Payment System Proclamation, Art 24(3).

bank. But where a payment is not made using the electronic channel due to some errors or malfunction of the system, the original (physical) paper-based instrument can be presented for payment before the issuing bank.<sup>353</sup> The paper-based payment instrument submitted using the electronic channels by imaging and storing the corresponding information shall be considered as the equivalence of the paper that it represents.<sup>354</sup> The NBE is delegated to issue a directive on the imaging of paper-based payment instruments and their processing<sup>355</sup>. But, the NBE has not yet issued a directive that regulates cheque truncation. Even the Draft Directive does not say anything with regard to the regulation of cheque truncation. As it is mentioned in Chapter Two of this Thesis,<sup>356</sup> the EBA is working to introduce the cheque truncation service in the near time, and the cheque truncation services is expected to provide services starting from the next year.<sup>357</sup> But having aware of the cheque truncation project which is handled by the EBA, the NBE is not working to issue a directive that regulates the cheque truncation services; and this might repeat the wrong happened in the introduction of the e-banking services.<sup>358</sup> The very limit of cheque truncation regulation is though there is an initiation to begin the cheque truncation services by the commercial banks of the country, the NBE has not yet issued a directive that regulates the cheque truncation. Even the coming directive, Draft Directive, does not provide provisions that regulate the cheque truncation. Thus, though there is the hope that the cheque truncation service to be introduced in the near time, the NBE not yet issued a directive for it and even is not working to issue a directive that regulates it.

#### **3.4.3.4 Interoperability of E-Banking Products and Services**

The interoperability of payment systems and services addresses several challenges regarding financial access and financial inclusion. Interoperability of payment systems enables people to withdraw money or make payments to anyone in a convenient, affordable, fast, seamless

---

<sup>353</sup> National Payment System Proclamation, Art 24(4).

<sup>354</sup> National Payment System Proclamation, Art 24(2).

<sup>355</sup> National Payment System Proclamation, Art 24(1-5).

<sup>356</sup> See section 2.2.2.8, p.26.

<sup>357</sup> Interview with Ato Solomon Damitew, Principal Manager Payment Systems Over Sight and Development, National Bank of Ethiopia (Addis Ababa, 04 May 2018).

<sup>358</sup> The provision of e-banking services is allowed by a circular latter, and the Regulation of Mobile and Agent Banking Services is issued after the commercial banks have already introduced e-banking products and services to their customers. The commercial banks introduce the e-banking products and services without passing clearly defined entry requirements and later on the commercial banks are asked to get an approval from the NBE for the e-banking products and services in which they have already introduced.

and secure way via a single bank account.<sup>359</sup> Establishing a shared payment system is therefore a tough task of the commercial banks. Over that, efficient, accessible retail payment systems and services are necessary to achieve the financial inclusive goal of the country. For the purpose of sharing of these benefits, the National Payment System Proclamation recognizes the ownership of shared payment systems by two or more commercial banks of the country.<sup>360</sup> The interoperability of the payment systems represents both an important input for the efficiency of the payment system and, at the same time, a critical source of risk.<sup>361</sup> The risks of the interoperability of the e-banking products and services includes inequitable risk sharing among the shared payment system owners, actual losses to both the participants of the national payment system and to the consumers of the participants, and loss of confidence in the financial system and of public trust in the very use of money.<sup>362</sup> The cooperation of banks for making their payment systems interoperable also raises competition issues.<sup>363</sup>

To minimize the risks arise with the interoperability of a payment system, the National Payment System Proclamation provides regulations that protect the interests of both the consumers of the e-banking and the commercial banks. The Proclamation begins by defining who could be the parties to the shared payment systems; and according to it, the parties to the shared payment system includes operators, participants, retailers, communication service providers, and other entities which are engaged in the provision of electronic fund transfer.<sup>364</sup> The rights and responsibilities of the parties is determined by the freewill of the parties; however, the NB may, by a directive, define the basic terms and conditions to be incorporated in the contract.<sup>365</sup> But, the NBE has not yet issued a directive which defines the basic terms and conditions of the shared payment systems.

As far as the protection of consumers is concerned, the Proclamation defines that the owners of a shared payment system; namely, operators, participants or issuers of payment instrument

---

<sup>359</sup> ITU-T Focus Group Digital Financial Services: Payment System Oversight and Interoperability, p.7. at <[https://www.google.com/url?sa=t&rcrt=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKewjS0K2ihfvcAhVMdcAKHStuClMQFJA AegQIAxAC&url=https%3A%2F%2Fwww.itu.int%2Fen%2FITU-T%2Ffocusgroups%2Fdfs%2FDocuments%2F10\\_2016%2FITUFGDFS\\_REPORT%2520ON%2520Payment%2520System%2520Oversight%2520and%2520Interoperability.pdf&usq=A0vVaw3Bm1A8KKqkTe9VQvoc61KQ](https://www.google.com/url?sa=t&rcrt=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKewjS0K2ihfvcAhVMdcAKHStuClMQFJA AegQIAxAC&url=https%3A%2F%2Fwww.itu.int%2Fen%2FITU-T%2Ffocusgroups%2Fdfs%2FDocuments%2F10_2016%2FITUFGDFS_REPORT%2520ON%2520Payment%2520System%2520Oversight%2520and%2520Interoperability.pdf&usq=A0vVaw3Bm1A8KKqkTe9VQvoc61KQ)> accessed 25 March 2018.

<sup>360</sup> National Payment System Proclamation, Art 22.

<sup>361</sup> ITU-T Focus Group Digital Financial Services: Payment System Oversight and Interoperability, P. 7-8.

<sup>362</sup> ITU-T Focus Group Digital Financial Services: Payment System Oversight and Interoperability, P. 10

<sup>363</sup> Ibid.

<sup>364</sup> National Payment System Proclamation, Art 22(1).

<sup>365</sup> National Payment System Proclamation, Art 22(2).

are not relieved from the obligation owed to their customers by the mere reason that they are party to a shared payment system and that another party to the system has actually caused the failure to meet obligations.<sup>366</sup> Again, the owners of the shared payment systems are obliged to solve complaints and disputes of their customers in relation to the processing of electronic fund transfers, or stored value cards promptly through its internally established internal complaint handling systems and in no means such parties may require their customers to present their complaints to any other party of the shared payment system, or to have those complaints or dispute investigated by any other party to the shared payment system.<sup>367</sup> With regard to ownership of shared payment systems (interoperability of e-banking), both the Regulation of Mobile and Agent Banking Service Directive and the Draft Directive does not say anything. In deed, the interoperability of the e-banking products and services is among the issues which is expected to be regulated under the operators' directive, such directive is being drafted, but in its early stage. At this juncture, the current regulation of interoperability of a payment system has the following legal and practical limits:

*First*, the NBE is delegated to issue a directive that defines the basic terms and conditions of the shared payment system, though the NBE have not yet issued a directive for it. Over that, neither the Proclamation nor the directive mandates the shared payment system owners to get prior approval for the terms and conditions that defines their respective rights and responsibilities. Thus, the absence of a directive that specifies the minimum terms and conditions on the one hand and the absence of prior approval requirement from the NBE on the other hand opens a room for the arbitrarily determination of the terms and conditions of the shared payment systems even against the interest of the consumers of the e-banking.

*Second*, it is not clear whether the interoperability of the e-banking products and services could be regulated by the electronic fund transfer directive or by the operators' directive. As it is mentioned in the above, the interoperability of the payment systems is determined by the contractual agreements of the payment system owners, commercial banks, but it highly influences the rights of the customers of the e-banking, as a result of this, it is problematic to locate in which directive it should be regulated. In relation to this, three arguments may be raised; first, as interoperability of the payment system is determined by the contractual relationship of the participants of the national payment system (mainly commercial banks), the regulation of the interoperability is a matter that should be included in the operators'

---

<sup>366</sup> National Payment System Proclamation, Art 22(3).

<sup>367</sup> National Payment System Proclamation, Art 22(4).

directive which is expected to be issued in the near time by the NBE. Second, as the interoperability of the payment system highly affects the users of the e-banking products and services, it should be regulated under the electronic fund transfer directive. And the last argument is as it affects both the rights and responsibilities of the customers of the commercial banks and the relationship between the commercial banks, it should be regulated in both directives depending upon its affection. The researcher recommends the third argument as the regulation of the interoperability of the payment system is determined based upon their affection to both the consumer and non-consumer e-banking users.

*Third*, the commercial banks are obliged not to require their customers to present their complaints to any other party of the shared payment system, but in practice, the commercial banks are requiring their customers to submit their complaints against the owner of the shared payment system which causes the problem/complain (ATM owner).<sup>368</sup> The customers of the bank wait up to two months to get back their monies.<sup>369</sup>

### **3.4.3.5 Privacy and Confidentiality of Customers' Accounts Information**

The National Bank Establishment(amended) Proclamation, which applies to both traditional and e-banking products and services, states that a banker may not disclose to third party any document or any other information it has obtained in the course of relationship with customer without the consent of the customer.<sup>370</sup> This duty of confidentiality is, however, not absolute but subject to discloser upon three important exceptions stated under Art 22(3) of the National Bank Establishment Proclamation(as Amended): *first*, when the NBE requested pursuant to the provisions of the law; *second*, when any other legally authorized person requests for the disclosure of the financial information of a particular customer, for example FIC; and *third*, when ordered by the court.<sup>371</sup> These three limited exceptions apply for both traditional and modern banking (e-banking) business.

The same duty is imposed on the part of financial information in e-banking transactions; the National Payment System Proclamation regulates the confidentiality of customer's information in e-banking transactions: it obliges the commercial banks to make their payment

---

<sup>368</sup> Interview with Ato Natan Lemma, Meseret Fikadu, Tebeje Hailu, and Yonas Mokenen, consumers of e-banking (Jun, 2018).

<sup>369</sup> Interview with Yonas Mokenen and Tebeje Hailu, consumers of e-banking (June 2018).

<sup>370</sup> National Bank of Ethiopia Establishment (as Amended) Proclamation, Art 22(3).

<sup>371</sup> National Bank of Ethiopia Establishment (as Amended) Proclamation, Art 22(3)(a-c).

systems safe and secured.<sup>372</sup> However, similar to the above, the Proclamation provides four excusable disclosure of the financial information of the customer: *first*, where it is ordered by court; *second*, where it is provided to do so by any other law; *third*, where it is requested by legally authorized person; and *fourth*, where it is requested by the NBE.<sup>373</sup> In substance, the exceptions provided under the National Payment System Proclamation is the same with those exceptions which are stated under the Amended National Bank Establishment Proclamation. But one thing that both laws fails to incorporate is that though in many jurisdictions the consent of the customer is also one exceptional ground to disclose the financial information of the customer, both laws are silent about this. In reality, once the customer is volunteer to disclose his/her financial information, the bank may not required to bother about confidentiality issue.

As far as the confidentiality of customer's financial information is concerned, the Regulation of Mobile and Agent Banking Service Directive provides very limited regulation: it only mandates the commercial banks to keep the secrecy and confidentiality of the customer's financial information.<sup>374</sup> To address the limits of the said Directive, the Draft Directive provides a very detail regulation, and as per the Draft, the financial institution is obliged not to disclose the financial information of the customer to third parties unless expressly authorized to do so by a law;<sup>375</sup> but exceptionally the financial information of the customer may be disclosed to third parties on three grounds: *first*, for the authorized personnel of the financial institutions; *second*, when the financial institution is obliged to disclose by a law; and *third* when the customer expressly consents the disclosure of his/her financial information to third party.<sup>376</sup> Over that, the Draft Directive defines the applicability of the traditional banking laws which regulates the disclosure of information to the e-banking transactions.<sup>377</sup>

With regard to security of the system from disclosure to hackers, the National Payment System Proclamation is delegated to issue a directive as to the use of the best available technologies by the commercial banks to combat the operational risks of the e-banking.<sup>378</sup> The Regulation of Mobile and Agent Banking Service Directive does not say anything about

---

<sup>372</sup> See the Preamble of the National Payment System Proclamation.

<sup>373</sup> National Payment System Proclamation, Art 35(2)(e).

<sup>374</sup> Regulation of Mobile and Agent Banking Service Directive, Art 12.4.

<sup>375</sup> Draft EFT Directive, Art 13.1.

<sup>376</sup> Draft EFT Directive, Art. 13.2 & 13.4(a&b).

<sup>377</sup> Draft EFT Directive, Art. 13.5.

<sup>378</sup> Draft EFT Directive, Art. 4(2)(j).

the use of latest technologies to protect the customer's financial information from hackers. But the Draft EFT Service Directive regulates the use of updated technologies to secure the financial data's of the customers; as per the Draft Directive, the financial institution is obliged to make sure that the electronic channels used to provide e-banking transactions are not to provide any information relating to the access of e-banking transaction unless; (1) the electronic terminal is operated by some authorized personnel, or by the agent appointed by the financial institution, and (2) the request for e-banking transaction is made by the correct customer's accepted means of access.<sup>379</sup> The Draft Directive also regulates the minimum contents of the information security policy of the financial institutions.<sup>380</sup> The Draft Directive address the limits of the Regulation of the Mobile and Agent Banking Services Directive in relation to privacy and confidentiality issues, but still it is surrounded by the following limits:

*First*, with the exception of very few ATMs, almost all ATMs of the country are open and the person who initiate electronic fund transfer using the ATM terminal can be easily observed by third-parties; this open a room for the unauthorized access of the customers' account by the third-parties who were observed the customer in keying his/her password. With regard to the disclosure of the ATM terminals to observation by third-parties even the coming regulation, Draft Directive, fails to provide a regulation that mandates the commercial banks to provide secured ATM terminals by constructing a cover.

*Second*, many of the ATM terminals have a camera that protects the security of the e-banking transaction, but very few ATM terminals do not have a camera,<sup>381</sup> and the absence of camera may disclose to the unauthorized access of customers' account. Thus, the absence of a regulation that mandates the commercial banks to install camera in each ATM terminal is disclosing the consumers of the e-banking to unauthorized access of their accounts.<sup>382</sup>

*Third*, the commercial banks notify the effect of disclosure of password to third-parties including to friends and relatives, but in practice, many customers are getting financial losses due to the lack of awareness on the effect of the disclosure of password of the accessing devices to third-parties. And sometimes this problem is worsened due to the absence of a regulation that mandates the commercial banks to notify about each transaction undertaken

---

<sup>379</sup> Draft EFT Directive, Art. 13.3(a&b).

<sup>380</sup> Draft EFT Directive, Art. 29.3.

<sup>381</sup> Interview with Ato Ephirem Baraki, Senior Legal Expert, National Bank of Ethiopia (Addis Ababa, 09 August 2018).

<sup>382</sup> Interview with Ato Ephirem Baraki, Senior Legal Expert, National Bank of Ethiopia (Addis Ababa, 09 August 2018).

by the electronic channels. For example, one customer of the CBE discloses the password of her ATM card to her sister, and her sister using the ATM terminal withdraws Birr120,000 within two months.<sup>383</sup> Had the CBE notified the customer about the withdrawal starting from the first unauthorized withdrawal, the second, third and the following withdrawals would not be happened. Thus, the absence of a regulation that mandates the notification of about the e-banking transaction through SMS and other means is causing customers to get significant financial losses.

#### **3.4.3.6 Authentication of Electronic Banking Signatures**

In any banking services, either traditional or electronic based, the authentication of the signature of the person who initiates the banking transaction is indispensable. In the traditional banking services, if a person mistakenly submits a different signature, the bank denies him/her the banking services. The authentication of signatures is very important in traditional banking services, but not as a fundamental as the authentication of electronic signatures of the e-banking transactions. In the traditional banking, the physical appearance of the account holder before the premises and cashiers of the bank may barred the unauthorized person from accessing banking services fraudulently. But in e-banking transactions, as the physical appearance of the person is not required, the requirement of authentication is somewhat very strict than the standard of authentication required in the traditional banking.

As it has already mentioned in the above, the traditional banking transactions is regulated by the 'Banking Transaction'<sup>384</sup> section of the commercial Code; but the said section of the Commercial Code does not say anything as to the authentication of the traditional signatures. The 'Banking Transaction' section of the Commercial Code is silent about the authentication of signatures, but the 'Commercial Instruments'<sup>385</sup> section of the Code regulates the authentication of signatures; and as per said section, the endorsement of commercial instruments is possible both through handwritten and machine-based signatures, stamp.<sup>386</sup> By analogy, we can say that both the handwritten and machine-based(stamp) signatures are possible to authenticate the signatures of the customers in the traditional banking transactions. Besides, the Civil Code regulates the authentication of handwritten signatures; and according to the Civil Code, where the law provides the contract to be in a written form,

---

<sup>383</sup> Interview with Ato Tebeje Hailu, consumer of e-banking (15 June 2018).

<sup>384</sup> Commercial Code, from Art 896-

<sup>385</sup> Commercial Code, from Art 732-

<sup>386</sup> Commercial Code, Art 734(2).

such contract cannot be proved by witnesses or presumption unless the written document is destroyed, stolen or lost;<sup>387</sup> and if the signatory party to the contract denies the making of the contract, the court shall order for verification.<sup>388</sup> The verification of the handwritten signature is made through the testimony of witness and sometimes through the scientific forensic verification method.

Coming back to the e-signature of e-banking transaction, the National Payment System Proclamation does not say anything as to the authentication of the electronic signatures. Similarly, as far as e-signature is concerned, both the Regulation of Mobile and Agent Banking Service Directive and Draft Directive are silent. The National Payment System Proclamation is silent about the authentication of e-signatures, but it regulates the electronic communication between the banks and their customers. According to the Proclamation, where a law provides a written form to have a legal effect for any communications(including contracts), such written form requirement deemed to have been satisfied if the communication or information is rendered or available in electronic form.<sup>389</sup> But, such electronic communication or information satisfies the written form requirements only if; first, the information or matter is made available in an electronic form, and second, it is accessible for subsequent use.<sup>390</sup> As far as electronic communications(messages) is concerned, the Electronic Signature Proclamation provides the same regulation with the National Payment System Proclamation; it is copy and past.<sup>391</sup>

Unlike the National Payment System Proclamation, the Electronic Signature Proclamation regulates the authentication of e-signatures; in the first place, the Proclamation defines what constitutes e-signature, and the Proclamation defines e-signature as follows;

...information in electronic form, affixed to or logically associated with, an electronic message, which may be used to identify the signatory in relation to the electronic message and to indicate the signatory's approval of the information contained in the electronic message.<sup>392</sup>

As you can easily understand from the wording of the definition, to consider an information is electronic signature it should fulfill three elements: *first*, the information must be in an electronic form; *second*, the information must be affixed or logically associated with the

---

<sup>387</sup> Civil Code, Art 2003.

<sup>388</sup> Civil Code, Art 2008.

<sup>389</sup> National Payment System Proclamation, Art 21(1).

<sup>390</sup> National Payment System Proclamation, Art 21(1).

<sup>391</sup> See Art 5(2) of the Electronic Signature Proclamation and Art 21(1) Of the National Payment System Proclamation.

<sup>392</sup> Electronic Signature Proclamation No. 1072/2018, *Federal Negarit Gazzeta*, 24<sup>th</sup> year No. 25, Art 2(6). [Hereinafter, Electronic Signature Proclamation]

electronic communication (message), and *third*, the information must be unique that is used to identify the signatory in relation to the electronic communication and to indicate the signatory's approval of the electronic communication initiated using any of the electronic devices. Where one of the elements is missed, there is no more e-signature; the cumulative presence of such elements is required to say particular information is an e-signature. Once the Proclamation clarifies what constitutes e-signature, in the next place, the Proclamation explains that an e-signature will not be denied legal effect solely on the ground that it is in electronic form<sup>393</sup>; and thereby it recognizes the validity and admissibility of the e-signatures before any legal proceeding.<sup>394</sup> But, such e-signature will be reliable e-signatures only if: *first*, it is appropriate to use electronic signature for the said electronic communication; *second*, the parties agreed to use electronic signature in doing the electronic communication; and *third*, it is used in consideration of the other conditions such as the nature, extent, and type of transaction, capability of identifying contracting parties, and the necessity of the electronic communication.<sup>395</sup> If all the three requirements are fulfilled, such electronic signature used is considered as a reliable electronic signature. The issue of reliability is directly related with the issue of authentication; therefore, the requirements for reliable electronic signatures are the requirements for the authentication of the electronic signatures. And finally, as per the Proclamation, in any civil proceeding, unless to the contrary is proved, such reliable electronic signature is presumed that: *first*, the e-signature is the signature of the true subscriber, *second*, the e-signature was inserted by the real subscriber with the intention of approving the electronic communication, and *third*, the electronic communication and the signature has not been altered since the particular point of time to which the e-signature is inserted.<sup>396</sup> From this we can conclude that, once the e-signature of passes the reliability test stated in the above, such electronic communications (messages) are presumed as initiated, processed and executed by the real subscriber.

As it is mentioned in the above, the current e-banking regulation is silent about the authentication of e-banking signatures, but the general electronic signature law provides an adequate regulation for it.

---

<sup>393</sup> Electronic Signature Proclamation, Art 6(1).

<sup>394</sup> Electronic Signature Proclamation, Art 6(1).

<sup>395</sup> Electronic Signature Proclamation, Art 6(2).

<sup>396</sup> Electronic Signature Proclamation, Art 7(1-3).

### 3.4.3.7 Admissibility of Electronic Banking Records

As it has been already noted in the above, e-banking records, like bank statements and terminal receipts issued by ATMS and POS's are electronic evidences that a customer will rely upon in case there is a dispute regarding whether a certain electronic banking transaction is authorized or not.<sup>397</sup> As we all know, Ethiopia has not yet issued a comprehensive evidence law, but this does not mean that Ethiopia does not have evidence law at all. By now, the Ethiopian evidence law is scattered in the substantive and procedural codes as well as in the subsequently issued proclamations. To examine the admissibility of the electronic banking transactions, it is better to begin with the provisions regulating the traditional banking transactions. With regard to admissibility of the handwritten signature of the customers, the Commercial Code stated nothing. But, when we referred to the provisions of the general contract provisions, there are significant provisions which regulate the admissibility of the traditional banking transaction records by one or another means. The general contract law states, "*A written instrument shall be **conclusive evidence**, as between those who signed it, of the agreement therein contained and of the date it bears.*"<sup>398</sup> [Emphasis mine]. Thus, the written instruments which are using in the traditional banking transaction are admissible evidence between the customer who signed to access banking transaction and the bank who receives the request of the customer and process banking transaction accordingly.

Coming back to the e-banking products and services, the question of admissibility of the electronic banking records is very sensitive and attracts high attention than the traditional banking transaction records due to the unique features of the electronic banking transactions; that's why the National Payment System Proclamation provides distinct provisions for the admissibility of the electronic banking records. According to the Proclamation, the electronic record as to any e-banking transaction through a system which is contained in any document, computer print-out, hard copy, microfilm, floppy or hard disc or any other electronic media or electronic form shall be admissible as an evidence before the law.<sup>399</sup> Again, photographic images of original documents of cheques, securities, certificate of deposits, account ledgers, government securities and other commercial payment instruments are admissible as prima facie evidence of the matters or transactions of the original instrument.<sup>400</sup> And very importantly the Proclamation recognizes the admissibility of the e-communications and fund

---

<sup>397</sup> Lukumay 214.

<sup>398</sup> Civil Code, Art 2005(1).

<sup>399</sup> National Payment System Proclamation, Art 23(1).

<sup>400</sup> National Payment System Proclamation, Art 23(2).

transfer that are initiated, processed or executed through electronic devices.<sup>401</sup> Having defining the general legal framework, the Proclamation mandates the NBE to issue a directive that regulates the detail issues of the admissibility of the e-banking records,<sup>402</sup> but the NBE has not yet issued a directive for it. As far as the admissibility of the electronic communication is concerned, the Electronic Signature Proclamation provides a similar regulation with the National Payment System Proclamation.<sup>403</sup> Coming to the secondary legislations, the Regulation of Mobile and Agent Banking Service Directive does not say anything about the admissibility of e-banking records. But unlike to the ongoing directive, the Draft Directive impliedly recognizes the admissibility e-banking records. As per the Draft Directive, computer printed-out documents of the e-banking transaction that is given to the customer upon his request is admissible as evidence of such transfer and shall constitute prima facie proof that such transfer was made.<sup>404</sup> Thus, the Draft Directive does not provide adequate regulations concerning the admissibility of the e-banking records, but it impliedly recognizes the admissibility of the e-banking records. At this juncture, the current regulation is surrounded by the following limits:

*First*, the NBE is delegated to issue a directive that regulates the standards, formats and the conditions for the medium of transmission of the e-banking records, though the NBE has not yet issued a directive for it. Thus, currently, there is no regulation that regulates; the standard formats of the e-banking records, the obligation of the banks to provide the copy of the e-banking to their customers either by paper-based or electronically, and the grounds and procedures of contrary proof of the e-banking records.

*Second*, and more importantly, scientifically the proper functioning of the system at the time of issuance of the electronic receipt is required for the validity of the e-banking record, but both the National Payment System Proclamation and the Electronic Signature Proclamation fails to include it. Thus, currently, whether the system issues the electronic receipt correctly or erroneously, such electronic record is admissible. The absence of a regulation on the contrary proof in general and the absence of the proper functioning of the system as a parameter in validating the electronic evidence is causing significant losses to the consumers of the e-banking.

---

<sup>401</sup> National Payment System Proclamation, Art 23(3).

<sup>402</sup> National Payment System Proclamation, Art 23(4).

<sup>403</sup> See Art 5(1) of the Electronic Signature Proclamation & Art 23 of the National Payment System Proclamation.

<sup>404</sup> Draft EFT Directive, Art 12.

### 3.4.3.8 Irrevocability of Electronic Fund Transfer

Finality of fund transfer is not only an issue that evolves because of the introduction of technology in the banking business, but it is also one of the guiding rules in the traditional banking transactions. The old aged Commercial Code regulates the finality of fund transfer; and it states, “[t]he beneficiary under a transfer obtains title to the sum to be transferred at the time when the bank debits the account of the person who orders transfer.”<sup>405</sup> The transferee exercise ownership right over the fund when the bank debits the account of the transferor and at the same time credits the account of the transferee. Defining the exact actual time of transfer of fund from the transferor to the transferee is very crucial to determine the time that the transferor may exercise his right to cancel the fund transfer order. The fund transfer order can be cancelled unless the account of the transferor is debited.<sup>406</sup> But, once the account of the transferor is debited, the fund transfer is in principle final and irrevocable. Another issue in relation to finality of fund transfer is when the account holder agrees with the bank to make fund transfer upon the presentment of a fund transfer order by the beneficiary, this early authorization of the bank to make fund transfer upon presentment of fund transfer order by the beneficiary is considered as a waiver of the right to cancel the fund transfer.<sup>407</sup> Thus, the fund transfer even in the traditional banking transaction is final and irrevocable. But for exceptional and limited grounds, the transferor may cancel the fund transfer order even after his account is debited by the bank, these grounds are; (1) judgment declaring the bankruptcy of the beneficiary, and (2) when the beneficiary is granted with the benefit of a composition with creditors.<sup>408</sup> Once transferor proved the existence of one of these grounds, the transferor has the right to oppose the fund transfer order and the bank is obliged to cancel the fund transfer order though the account of the transferor is debited. Similarly, the fund transfer which is made after the declaration of bankruptcy or granting of the transferor the benefit of a composition with creditors is revocable.<sup>409</sup>

Coming back to the finality of the e-banking transaction, the Proclamation only regulates the finality of the payment, clearing and settlements made between the participants of the national payment system, EATS.<sup>410</sup> According to the Proclamation, any payment, clearing and settlement made between the participants of the national payment system is final and

---

<sup>405</sup> Commercial Code, Art 906(1).

<sup>406</sup> Commercial Code, Art 906(2).

<sup>407</sup> Commercial Code, Art 906(3)&907(1).

<sup>408</sup> Commercial Code, Art 906(3)&910.

<sup>409</sup> Commercial Code, Art 911.

<sup>410</sup> National Payment System Proclamation, Art 14(1&2).

cannot be revoked, reversed or set-aside for any reasons.<sup>411</sup> Thus, the payment, clearing and settlement made using the RTGS and ACH is final and irrevocable. But with regard to the finality of the consumer based e-banking transactions, the Proclamation is silent. Similarly, the Regulation of Mobile and Agent Banking Service Directive does not say anything as to the finality of the e-banking transactions.

Having identified the above-mentioned drawbacks, the Draft Directive transplanted by directly copying Art 5(irrevocability) of the Bangladesh Regulations on Electronic Fund Transfer; and as per the transplanted provision, “*A payer may not revoke a payment order once it has been received by the financial institution, unless otherwise provided by agreement.*”<sup>412</sup> [Emphasis mine]. This article has three important points: *First*, this regulation looks like as it is intended to regulate the traditional banking services, the phrase “*received by the financial institution*” indicates that the payment order which is made by the payer is paper-based; as there is no receipt for electronic fund transfer orders. *Second*, if there is contrary agreement between the customer and the financial institution, the payer can revoke his orders even after the receipt of the payment/transfer order by the financial institution. *Third*, this revocation of payment order by agreement is possible only after receipt of the payment order and before the debiting of the account of the payer/transferor.<sup>413</sup> Again, the second sub-article of the same article states, “[*w*]here the payment order is initiated by or through the payer, the payer **shall not** revoke the payment order after **transmitting** the payment order or giving his consent to execute the payment transaction to the payee.”<sup>414</sup> [Emphasis mine]. As per this Sub-article, where the payment is initiated by the payer, the payer loses his/her right to cancel the payment order once he/she transmitted the order to the bank or delivered such payment order to the payee for execution. Additionally, the Draft Directive states that the payer may only revoke his/her payment instruction at the latest by the end of the business day preceding the day agreed for debiting the account of the payer/transferor.<sup>415</sup> The cumulative reading of the said sub-articles indicates that once the account of the payer is debited, such payment/transfer order is final and irrevocable. The last but not least issue addressed by the Draft Directive is the rules regulating the finality of the

---

<sup>411</sup> National Payment System Proclamation, Art 14(1) & (2).

<sup>412</sup> Draft EFT Directive, Art 18.1.

<sup>413</sup> The cumulative reading of Art 18.1 and 18.3 of the Draft Directive indicates that cancellation of payment order is only possible before the account of the payer (transferor) is debited.

<sup>414</sup> Draft EFT Directive, Art 18.2.

<sup>415</sup> Draft EFT Directive, Art 18.3.

payment orders equally applies to the communications cancelling or amending a payment instruction.<sup>416</sup>

In the end, in practice, even in the absence of a clear regulation, the commercial banks and the officers of the NBE believe that the e-banking transactions are final and irrevocable.<sup>417</sup> As per the response of the interviewees, once a customer erroneously transfer a fund using the e-banking service to unintended recipient, the customer can refund his money where the unintended recipient is volunteer, but where the unintended recipient is not volunteer to refund the money, the customer can only use the court litigation means to refund his/her money.<sup>418</sup>

### **3.4.3.9 Cross-Border E-banking Transactions**

As it is mentioned in the above,<sup>419</sup> by now, cross-border e-banking transactions are provided to both foreigners who are the VISA and MasterCard cardholders and to the Ethiopian 'dollar accountholders'. Again, as it is mentioned in the above,<sup>420</sup> the cross-border e-banking transactions are facing many problems including the fraudulent transactions of the VISA and MasterCard cardholders. Though the Ethiopian businessmen are suffering significant losses due to the fraudulent cross-border transaction, both the current and the upcoming regulation do not provide a mechanism where the businessmen can be cured from such losses. The cross-border e-banking problems become worse as there is the participation of intermediary bank between the consumer and his/her bank. The involvement of foreign banks as intermediary requires a strict regulation, but both the current and the upcoming regulation are silent about such involvement of foreign banks as intermediaries. The domestic banks can determine the terms and conditions of the interbank transfers, thus, the Draft Directive should provide a devise to make sure that the consumers of the e-banking are adequately protected. Even the minimum terms and conditions of the Ethiopian banks and the intermediary banks have not yet regulated.

---

<sup>416</sup> Draft EFT Directive, Art 18.4.

<sup>417</sup> Interview with Ato Solomon Damitew and Ato Ephirem Baraki.

<sup>418</sup> Focus group discussion with Ato Birhane Gebrecherkos, Ato Berihu Gebru, Ato Endalle Tessema, Ato Bahire Birhane and Ato Anteneh Gebriye, Commercial Bank of Ethiopia (Addis Ababa, 12 May 2018).

<sup>419</sup> See section 2.2.2.1 & 2.2.2.2, p.14&15.

<sup>420</sup> See section 2.3.8, p.35.

### 3.4.3.10 Fraud, Error and Improper Handling of Payment Instruments Related Liabilities

As it has been already mentioned in the above, the consumers of e-banking are suffering financial losses happened due to fraud, error and improper handling of payment instruments. As far as fraud, error and improper handling of payment instruments are concerned, the current regulations, NPSP and Regulation of Mobile and Agent Banking Service Directive, are silent. But, unlike to the Regulation of Mobile and Agent Banking Service Directive, the Draft Directive provides some very important regulations. The regulations provided by the Draft Directive are discussed in the below sub-sections.

#### A. Fraud

As it is mentioned in the above, the current regulation is silent about fraudulent transactions, but the Draft Directive implicitly regulates the fraudulent e-banking transactions. According to the Draft Directive, banks are obliged to reimburse the losses occurred due to: unauthorized electronic fund transfer services; acts not attributed to or not contributed by the customer; fraudulent or negligent conduct of the bank, technology service provider, or agents of the bank; forged, faulty, or expired payment instruments (cards); and before the customer has received the payment instrument.<sup>421</sup> And for the purpose of clarification, the Draft Directive defines ‘unauthorized electronic fund transfer’ as, “...*an electronic fund transfer service from an accountholder’s account initiated by a person other than the accountholder without actual authority to initiate such services and from which the accountholder receives no benefit.*”<sup>422</sup>[Emphasis mine]. This is the general standard that the Draft Directive provides as a means to differentiate the authorized transactions from the fraudulent transactions. It is obvious that once the true cardholder withdraws or transfers funds using the true card and its corresponding password, there is no more fraudulent transaction. In practice, some cardholders falsely deny that an ATM/POS cash or fund transfer shown on his account was not made by him, but the CCTV camera of the ATM terminal proved that such e-banking transaction is made by them.<sup>423</sup> It is to deter this type of fraud that the Draft Directive dictates that a cardholder cannot claim compensation under the guise of fraudulent transaction for withdrawals made by him. Similarly, in the second case, once the cardholder expressly or impliedly authorizes to a third-party (agent) to withdraw or transfer a fund to another party by

---

<sup>421</sup> Draft EFT Directive, Art 25.1-25.5.

<sup>422</sup> Draft EFT Directive, Art 2.30.

<sup>423</sup> Interview with Ato Damitew Weldetekle, Attorney, CBE (13 May 2018).

using his card and its corresponding password, according to the Draft Directive, such e-banking transaction is not considered as a fraudulent transaction. Again, in the third case, the cash withdrawal may be initiated, processed and executed by a third-party without having an authorization from the cardholder, but once it is proved that the cardholder has benefited from such an unauthorized withdrawal, it is unauthorized, but not fraudulent transaction. Therefore, according to the Draft Directive, a given e-banking transaction is considered as unauthorized (fraudulent) only if the following three conditions cumulatively exists: *first*, the e-banking transaction should be initiated by a person other than the true accountholder; *second*, such other person who initiated the e-banking transaction does not have the authority to do so; and *third*, the true accountholder receives no benefit from such e-banking transaction.

In addition to the general standard stated in the above, the Draft Directive excludes the following e-banking transaction from ambit of unauthorized electronic fund transfer(fraudulent e-banking transaction): (1) the e-banking transactions which are initiated by a third-party who is authorized to access the payment instrument by the true accountholder; (2) e-banking transactions initiated by the fraudulent intent of the customer or any other person working in concert with the customer; and (3) any other act which is considered as an error committed by the bank.<sup>424</sup> As far as the e-banking transaction made by the cardholder himself and by its agent is concerned, the cases mentioned above in analyzing the general standard equally applies, no more difference, the directive defines it again as an extension of elaborating the general standard discussed in the above. Again, the directive explains that the withdrawal or transfer of fund made by a third-party in concert with the cardholder is not considered as a fraudulent transaction.<sup>425</sup> The phrase “... *in concert with the customer*” is a controversial issue that needs clarification; how we can know that the said unauthorized transaction is made in concert with the cardholder? Unless we provide an answer for this question, we cannot apply such requirement. What makes the concert requirement difficult for application is the Draft Directive does not expressly define the circumstances/conditions that may help us to know the existence of the act of concert or not. In relation to this, the Draft Directive is silent about the conditions that show the concert practice, but it generally regulates that any e-banking transaction is considered as an authorized e-banking transaction so far as the person initiates, process and executes such e-

---

<sup>424</sup> Draft EFT Directive, Art 2.30(a-c).

<sup>425</sup> Draft EFT Directive, Art 2.30(b).

banking transaction using the accepted means of access (card or SIM Card) and its correspondent PIN or password.<sup>426</sup> Thus, in determining the authorization of the e-banking transaction, the identity of the person is not required rather the identity of card and its correspondent password is required. From this, we can say that where a cardholder intentionally or negligently accesses or cause to be accessed his payment instrument and its correspondent password, such transaction is considered as an authorized transaction and the bank is relieved from the losses occurred due to such problems. Therefore, as any transaction made using the accepted means of access and its correspondent is considered as a transaction made by the true cardholder, irrespective of the identity of the person who initiates, process and executes the e-banking transaction, the existence or non-existence of concert on the side of the cardholder is not as such necessary. But unlike, to the fraud case mentioned above, the bank is liable for losses occurred due to: acts not attributed to or not contributed by the customer; namely, fraudulent or negligent conduct of the bank, technology service provider, or agents of the bank; use of forged, faulty, or expired payment instruments.<sup>427</sup>

In practice, where an accountholder claims that an e-banking transaction debiting his account does not represent a cash withdrawal made by him, the bank is obliged to prove the cash withdrawal is made by the true accountholder using the true card and its corresponding password. Again, as it is mentioned in the above, with regard to the ATM transaction, as almost ATM terminals have CCTV camera that automatically stand the photo of the person initiating and executing the transaction, there is no problem of proving. In this regard, when the cardholder claims unauthorized transaction, the bank has only the obligation to notify the identity of the person who withdraw cash from the cardholder's account using the true card and its corresponding password: once the bank proves that the true card and its corresponding password is used in debiting the account of the cardholder, it is relieved from liability. Similar to the above mentioned for ATM banking, where a third-party access the financial account of a customer using the true SIM card and its corresponding password, the bank is relieved from liability. Again, if a third party access the financial account of the I-banking user using the two-factor authentication method mentioned in Chapter-Two, the bank is relieved from liability. In other words, irrespective of the identity of the person, once the bank proves that the transaction is initiated and executed using the true card/SIM card and its correspondent password, it is relieved from liability: by now, it is through the terms and

---

<sup>426</sup> Draft EFT Directive, Art 26.1(a).

<sup>427</sup> Draft EFT Directive, Art 25.1-25.5.

conditions of the e-banking service agreements that the bank relieves itself from such liabilities.

As far as fraudulent e-banking transaction is concerned, both the practice and the upcoming regulation have a similar stand; both relived the liability of the bank where the fraudulent transaction is made using the accepted means of access and its corresponding security code. But, the allocation of the losses occurred due to fraudulent e-banking transaction is not as such easy: it is very hard to prove that a fraud committed by a third-party who has not been apprehended was caused by such actions of the customer as leaving password in a desk drawer or writing the PIN on the plastic card. And even it is almost impossible for a customer to show that a bank had designed an inadequate security system or had failed to follow its own authorization and security procedures. Thus, the coming fraud regulation creates a cumbersome to the customers by relieving the banks for any fraud transaction committed by a third-party using the accepted means of access and its correspondent password.

**B. Error**

Similar to the above, as per the Draft Directive, the commercial banks are liable for any financial losses occurred due to erroneous e-banking transactions.<sup>428</sup> Unlike to the fraud cases mentioned above, the Draft Directive defines the circumstances that constitutes erroneous e-banking transactions, and accordingly erroneous transactions includes the occurrence of one or more of the following circumstance: unauthorized electronic fund transfer services; where a payee receives an incorrect amount; failure to enter the e-banking transactions which affects the customer’s account within the periodic statement; arithmetic or bookkeeping error in executing the e-banking transactions; the dispensing of incorrect of amount of cash to the customer’s transacting using the electronic terminals; failure to avail funds on time when instructed by a customer; failures in relation to the execution of the countermand orders in accordance to their contractual agreements; and any other customary error prescribed by the NBE.<sup>429</sup>

As far as ‘unauthorized electronic fund transfer’ is concerned, the Draft Directive erroneously categorized it as an erroneous e-banking transaction, but the US EFT Act, where the Draft Directive copied its provisions, states that unauthorized electronic fund transfer is considered as an erroneous e-banking transaction only for the purpose of the error resolution

---

<sup>428</sup> Draft EFT Directive, Art 19.

<sup>429</sup> Draft EFT Directive, Art 20(a-h).

procedure.<sup>430</sup> The US EFT Act does not classified unauthorized electronic fund transfer as an erroneous e-banking transaction rather it considers as an erroneous e-banking transaction for the purpose of the application of the erroneous resolution process provided by the said act. Similarly, as unauthorized electronic fund transfer is a fraudulent transaction, the Draft Directive should be corrected so as to classify it in fraudulent e-banking transaction but to consider it as an erroneous for the purpose of error resolution process. With the exception of erroneous classification of the unauthorized electronic fund transfer as an erroneous e-banking transaction, all other circumstances mentioned above are directly copied from the US EFT Act with some minor changes in their wording.

With regard to the e-banking transactions initiated by the payee, the bank is at fault where: the payment order/authorization of the fund transfer does not specify the exact amount of money; and the amount of the fund transfer exceeds the amount that the customer has set within the terms and conditions of the e-banking agreement, breaches the conditions specified under the framework contract, or breaches any other circumstances of the fund transfer.<sup>431</sup> Once the bank ascertains the occurrence of one or more of the above mentioned errors, it has the obligation to correct the errors free of charge.<sup>432</sup> Such obligation of correcting the errors includes the obligation to reimburse the principal amount, fees and taxes associated with the principal and other remedies (most probably damages) ordered by the NBE.<sup>433</sup>

As it is mentioned repetitively, by now there is no regulation that defines the circumstances that constitute error and the procedures that should be followed to address such errors by the banks. As a result of this, where a customer claims the occurrence of error to his account, the banks are resolving such allegation through their internal complaint handling system. For example, if the customer's card is attached by the ATM terminal, the customer whose card is attached claims to the nearby branch of the banks, and the officers of the bank unlock the ATM terminal and if the claimed card is there, they give to the claiming customer after disproving his identity. The commercial banks usually, but not always, write the name and the phone number of the officer that the customers could call for help. Whatever the case, by now, there is no mandatory regulation that defines error and its resolving process.

---

<sup>430</sup> See 15U.S. Code 1693f(f)(1).

<sup>431</sup> Draft EFT Directive, Art 22.3 (a & b).

<sup>432</sup> Draft EFT Directive, Art 22.2.

<sup>433</sup> Draft EFT Directive, Art 22.2 (a & c).

### **C. Improper Handling of Payment Instrument**

There is no any means that the banks could be responsible for any losses happened due to the improper handling of the payment instruments; therefore, unlike to the above two cases, the liability caused because of the improper handling of the payment instrument lies with the customer. Thus, the Draft Directive provides two cases whereby the customer is responsible for financial losses happened due to improper handling of payment instruments: (1) where the fraudulent third-party makes the e-banking transaction using the true payment instrument with its agreed means of authentication; (2) where the customer has delayed in notifying the lost, misused, or theft of the payment instrument.<sup>434</sup> But, for the second cases, the customer shall not be liable for financial losses exceeding; the daily transaction limits of the said means of access or account, and/or the amount of money standing on the customer's account.<sup>435</sup> In relation to this, the burden to proof that the third-party intruder uses the accepted means of access with its agreed means of authentication lies with the commercial banks.<sup>436</sup>

#### **3.4.3.11 Documentation and Periodic Statements of E-Banking Transactions**

Once we say that the e-communications made through the electronic channels are admissible before the law, the next question is how the customer whose rights are affected due to the problems of e-banking products and services can access the e-communications that he/she has exchanged with his/her bank. As far as the access of the e-banking transaction documents by the customer is concerned, both the National Payment System Proclamation and the Regulation of Mobile and Agent Banking Service are silent. But, unlike to the Proclamation and the ongoing directive, the Draft Directive provides the detail regulation of the documentation of the e-banking transactions. According to the Draft Directive, for each e-banking transaction initiated by the customer, the bank is obliged to provide a document that proves the transfer of such fund either electronic or paper-based receipt.<sup>437</sup> The receipt should at least include; the amount of Birr transacted, the date and time of the transaction, the form of the transfer (credit or debit transfer), the partial identification of the customer's account from which and to which the e-banking transaction is made, the identification of the electronic equipment or the agent involved, and any other information which describes the

---

<sup>434</sup> Draft EFT Directive, Art 26.1 (a & b).

<sup>435</sup> Draft EFT Directive, Art 26.2(a&b).

<sup>436</sup> Draft EFT Directive, Art 27.

<sup>437</sup> Draft EFT Directive, Art 10.1.

details of the e-banking transactions.<sup>438</sup> For e-banking transactions made through voice communications, the bank is required to provide the said information through voice communications at the time of the initiation of the e-banking transaction.<sup>439</sup> The banks have also the obligation to provide such documents to its customers free of charge.<sup>440</sup> In relation to this, the bank should provide a system that gives the option to the customer about the delivery of the printout of the electronic channels.<sup>441</sup>

In addition to the obligation of documentation at the time of initiation of the e-banking transaction, according to the Draft Directive, the banks are obliged to provide periodic statement upon the written or electronic request of their customers.<sup>442</sup> The periodic statement should at least include; the minimum contents of documentation specified in the above paragraph, the amount of transaction and/or maintenance fee charged by the bank during the period, the balance of the customer's account both at the beginning and the at the end of the period, and finally the address and the telephone number of the call center of the bank that the customer can complain or call for the inquiry or notify of account error.<sup>443</sup> As it is stated in the introduction of this section, the very end objective of the documentation and periodic statement regulation is to enable the customer to exercise the available remedies for financial losses caused due to errors, malfunction and unauthorized transactions against his bank, but in addition to that, as per the Draft Directive, the documentation and periodic statement could be also used as a prima facie proof that a fund is transferred from the customer to third-party (transferee).<sup>444</sup> Thus, the customer (transferor) can use such documents and periodic statements as an evidence to allege his/her rights against a third-party (transferee).<sup>445</sup>

### **3.4.3.12 E-Banking Transaction Limits**

As it has already mentioned above, e-banking is disclosed to various risks including to the unauthorized access of customer's account; unless properly managed, the demerits of the e-banking may outweigh its merits. But, there are mechanisms to minimize the possible losses that could happen due to the fraudulent transactions, and one of the mechanisms is providing transaction limits. Transaction limits cannot eliminate the fraudulent transactions, but it can

---

<sup>438</sup> Draft EFT Directive, Art 10.1.

<sup>439</sup> Draft EFT Directive, Art 10.2.

<sup>440</sup> Draft EFT Directive, Art 10.4.

<sup>441</sup> Draft EFT Directive, Art 10.3.

<sup>442</sup> Draft EFT Directive, Art 11.

<sup>443</sup> Draft EFT Directive, 11(a-d).

<sup>444</sup> Draft EFT Directive, Art 12.

<sup>445</sup> Draft EFT Directive, Art 12..

minimize the financial loss of the fraud.<sup>446</sup> The Ethiopian legal framework also appreciates the financial loss mitigation role of the transaction limit, and it provides regulations accordingly. As per the Regulation of Mobile and Agent Banking Service Directive, the maximum amount of money which can be deposited in a ‘mobile account’<sup>447</sup> of the customer is Birr 25,000, and the maximum amount of money which can be transferred and/or withdrawn within a day is Birr 6,000.<sup>448</sup> But, these limits are repealed by Circular No. FIS/02/2014, and as per such circular, the financial institutions shall set both the deposit limit and daily transaction limits by their internal policies.<sup>449</sup> But, with regard to the deposit and transaction limits of the agent banking services, the regulation provided by the said directive is still effective.<sup>450</sup> These are the only regulations provided by the Regulation of Mobile and Agent Banking Service Directive.

As far as transaction limit is concerned, the Draft Directive maintains what is provided by Circular No. FIS/02/2014; and accordingly, the financial institutions shall determine the transaction limits of the ATM banking, POS transaction, m-banking, I-banking, m-money and m-wallet based on risk assessment and business suitability.<sup>451</sup> But, unlike to the Circular, the Draft Directive obliges the financial institutions to notify the NBE about the transaction limits.<sup>452</sup> Over that, as per the Draft Directive, the NBE may set the transaction limits of the e-banking transactions based on the risk assessment made by its own initiation.<sup>453</sup> As an extension of the transaction limit regulation, the Draft Directive obliges the financial institution to include the transaction limits of the e-banking products and services under the terms and conditions of the e-banking agreements.<sup>454</sup> The financial institutions are also obliged to notify the customers about the changes made to the transaction limits.<sup>455</sup> And finally, as the very end objective of transaction limits is to mitigate the financial losses that

---

<sup>446</sup> UNCITRAL Legal Guide on Electronic Fund Transfer, P.50, paragraph 16.

<sup>447</sup> It looks like that an account that deposits mobile money, but as per Art 2.10 of the Regulation of Mobile and Agent Banking Service Directive, it is to mean financial account maintained in a financial institution in which its debit and credit transactions are made through electronic channels (an account used to make e-banking transactions).

<sup>448</sup> Draft EFT Directive, Art 5.1 & 5.2.

<sup>449</sup> Circular No. V/GOV/017/2014.

<sup>450</sup> Circular No. V/GOV/017/2014.

<sup>451</sup> Draft EFT Directive, Art 35.1.

<sup>452</sup> Draft EFT Directive, Art 35.1.

<sup>453</sup> Draft EFT Directive, Art 35.2.

<sup>454</sup> Draft EFT Directive, Art 7.5(d).

<sup>455</sup> Draft EFT Directive, Art 9.1(c).

could occur due to fraudulent transaction, the customer of the bank is not liable for financial losses which exceeds the daily transaction limit.<sup>456</sup>

### 3.4.3.13 Price Regulation

There are no free lunches in this world and everything comes with prices. The e-banking business would not be different from this; the commercial banks provide the e-banking products and services by collecting charges from their customers. In relation to e-banking products and services, there are four kinds of fees; (1) issuance fee, (2) renewal fee, (3) transaction fee and (4) convenient fee. While the first two fees are related with the issuance and renewal of payment instruments (debit, credit, or stored-value card), but the third and the fourth fees are charges imposed for the e-banking transaction service and the interoperability of the payment systems respectively. Once it is clear that the banks collect different charges to gain profits and ensure their continuity, the next question is ‘how much’? It is here that the issue of price regulation comes to view: though the degree of price regulation is different from country to country due to various reasons, in almost all countries of the world, price regulation is acceptable. Ethiopia, as a country promoting the ideologies of developmental state theory, has the experience of regulating the prices of goods and services by one or another means.

As far as charges of e-banking products and services are concerned, the NBE is mandated to prescribe the charges of the e-banking products and services,<sup>457</sup> the NBE has not yet explicitly prescribes the charges of the e-banking transactions, but implicitly it tries to regulate the price of the e-banking products and services by mandating the commercial banks to submit their price strategy with the policy documents specified in the above.<sup>458</sup> The pricing strategy should include the initial fees and charges taking into account the sustainability and the affordability of the e-banking product and services.<sup>459</sup> Again, the ongoing directive only mandates the financial institution to disclose the prices of the e-banking products and services at the time of conclusion of the e-banking contract.<sup>460</sup> Thus, the ongoing regulation is not enough adequate.

Having recognized the drawbacks of the current regulation, the Draft Directive, provides a detail regulation for the prices of the e-banking transactions. As per the Draft Directive, the

---

<sup>456</sup> Draft EFT Directive, Art 26.2(a).

<sup>457</sup> National Payment System Proclamation, Art 4(2)(d)(3).

<sup>458</sup> Regulation of Mobile and Agent Banking Services Directive, Art 6.3(iii).

<sup>459</sup> Regulation of Mobile and Agent Banking Services Directive, Art 6.3(iii).

<sup>460</sup> Regulation of Mobile and Agent Banking Services Directive, Art 12.7.

financial institution has the obligation to notify to the NBE about the initial amount of fee and any change thereof imposed on any e-banking products and services.<sup>461</sup> The financial institution has also the obligation to notify the imposition of fees and its amount to the customer.<sup>462</sup> The fees imposed by the financial institution should be disclosed to the customers by posting in one or more of the following means: in prominent and conspicuous location at which the customer initiates the e-banking transactions; for e-banking transactions made through ATM terminals, on the screen of the ATM, or on a paper notice issued from such machine; for any other electronic channel, in the screen of the electronic channel used.<sup>463</sup> The notification should be after the initiation of the e-banking transaction and before the customer confirms the e-banking transaction.<sup>464</sup> These are the only issues regulated by the Draft Directive, at this juncture, the price regulation is surrounded by the following limits:

*First*, the NBE is delegated to issue a directive as to the amount of charges associated with the provision of e-banking products and services, but till this time the NBE has not yet issued a directive that regulates the said charges. Thus, as it is mentioned in the above, the NBE is only using the price strategy to regulate the price of the e-banking products and services. But, once the bank passes the entry regulation, as per the current regulation, the NBE does not have a regulatory power in relation to the changes of the charges specified under the initial price strategy or for new charges which are not included in the price strategy but imposed later on by the banks.

*Second*, as per the Draft Directive, the banks have only the obligation to notify the initial fees and the changes made thereof to the NBE; thus, the NBE is only entrusted to accept the notification: it is not empowered to reject the charges where it believes that such charges are unreasonable. The upcoming regulation, Draft Directive, is not only failed to empower the NBE to regulate at least the price floor and price ceiling of the charges associated with the e-banking products and services, but it also fails to specify the tests (like sustainability and affordability) that the NBE should take into consideration in approving or denying the charges notified to it by the banks before imposing such prices to their customers.

---

<sup>461</sup> Draft EFT Directive, Art 8.1.

<sup>462</sup> Draft EFT Directive, Art 8.2(a&b).

<sup>463</sup> Draft EFT Directive, Art 8.3(a&b).

<sup>464</sup> Draft EFT Directive, Art 8.3(b).

### 3.4.3.14 Competition Regulation

The competition issues of the Ethiopian financial markets, the objectives, areas, instruments and enforcement of competition regulation, is discussed in detail under Dr. Solomon Abay Dissertation.<sup>465</sup> Thus, the researcher don't like to discuss it, but one thing that should be clear at this level is that the competition issues of the financial markets is regulated by the general competition law as well as by the sector specific financial laws of the country.<sup>466</sup>The competition issues of the e-banking transaction also share the competition regulation provided to the traditional banking transactions discussed under Dr. Solomon's Dissertation. In addition to the sharing of the competition issues of the traditional banking, the e-banking raises new competition issues which are not regulated under the traditional banking laws; and among the technological product which raises competition issues is the interoperability of the e-banking products and services.

Cooperation among the commercial banks by making the payment systems interoperable is very important to provide safe and efficient e-banking services to their customers; however, unless there is a balance between the cooperation and competition within the shared payment system owners; mainly, commercial banks, the demerits of the interoperability of the payment systems may be greater compared to its merits. The interoperability of the payment systems represents both an important input for the efficiency of the payment system and, at the same time, a critical source of risk.<sup>467</sup> As far as the interoperability of payment system is concerned, the National Payment System Proclamation only regulates the consumer protection issues<sup>468</sup>, but it does say nothing as to the competition issues. Again, both the Regulation of Mobile and Agent Banking Service Directive and the Draft Directive are silent on the regulation of competition issues of the interoperability of the payment systems. Thus, the competition issue of the e-banking products and services is surrounded by the following limits.

*First*, the NBE is entrusted with the discretion to define the minimum contents of the terms and conditions of the contract of shared payment systems (interoperability) of the e-banking products and services, though the NBE has not yet issued a directive for it. Thus, currently, the shared payment system runners, EthSwitch, is not volunteer to disclose the terms and

---

<sup>465</sup> Solomon Abay 84-87.

<sup>466</sup> The general competition law is Proc. No. 813/2014, whereas the specific competition law is the banking, insurance and microfinance business proclamations, and the Council of Ministries.

<sup>467</sup> ITU-T Focus Group Digital Financial Services: Payment System Oversight and Interoperability, P. 7-8.

<sup>468</sup> See section 3.4.3.4, p.69.

conditions of the shared-payment system, but it is obvious that in the absence of adequate regulation that business men's could abuse the market to sustain their own benefit. And this is even witnessed under the complaint handling system of the practical cases related to the interoperability of the payment systems.<sup>469</sup>

*Second*, both the current and the upcoming regulations do not say anything as to the requirements of approval from the NBE for both integrating the payment systems, and the terms and conditions of the shared payment systems.

*Third*, EthSwitch, the company which is running the shared payment system, is established by the consortium of all commercial banks of the country. In dead, the commercial banks are allowed to invest in the financial infrastructure by holding equities,<sup>470</sup> however, as the commercial banks are the owners of the company which runs the interoperability of the payment system, this may create a conducive environment to arbitrarily determine the terms and conditions of the shared payment systems.

### **3.4.3.15 Dispute Settlement System**

As far as dispute settlement system is concerned, the National Payment System Proclamation provides two regulations; one, it mandates the commercial banks to issue internal complaint handling procedure, and two, it provides the dispute settlement system of the participants of the national payment system.<sup>471</sup> As per the Proclamation, the commercial banks are mandated to issue internal complaint handling procedure, and even they are required to advise the customers on the procedures of lodging complaints.<sup>472</sup> In relation to this, the NBE may prescribe by a directive the internal complaint handling procedure.<sup>473</sup> One thing that should be in mind is that the internal complaint handling procedure is employed to address the complaints in relation to consumer e-banking only, not non-consumer e-banking. The second regulation is related to the non-consumer e-banking transactions; and the Proclamation states, *“Disputes among parties involved in the national payment system concerning any civil matter arising under this Proclamation shall be resolved by mediation.”*<sup>474</sup>[Emphasis mine]. As we can easily understand from the wording of the article, mediation as a settlement system is only applied to resolve disputes in relation to the participants of the national

---

<sup>469</sup> See section 3.4.3.4, p.69.

<sup>470</sup> *Limitation on Investment of Banks (as Amended) Directive*, National Bank of Ethiopia, October 2015.

<sup>471</sup> National Payment System Proclamation, Art 20 and Art 31.

<sup>472</sup> National Payment System Proclamation, Art 20(1).

<sup>473</sup> National Payment System Proclamation, Art 20(2).

<sup>474</sup> National Payment System Proclamation, Art 31(1).

payment system: the parties which involves in the national payment system are the financial institutions and operators who have a ‘payment and settlement account’ within the NBE.<sup>475</sup> Thus, the dispute settlement system provided by the Proclamation applies to disputes arising in relation to the non-consumer e-banking which is stated under Chapter Two of this Thesis.<sup>476</sup> But, as far as the dispute settlement system of consumer e-banking is concerned, the Proclamation is silent.

As it is mentioned in the above,<sup>477</sup> the Regulation of Mobile and Agent Banking Service Directive regulates the minimum contents of the consumer protection policy, and as part of the consumer protection policy, the directive regulates some issues of the internal complaint handling procedure. According to the Directive, commercial banks are obliged to organize a help desk and dedicated customer care call center and disclose the details of such help desk and call center to the customers.<sup>478</sup> The commercial banks are also obliged to provide a timeframe to resolve customer complaints within reasonable time and in any case such timeframe should not be exceeding thirty working days.<sup>479</sup> In relation to this, according to the current directive, the commercial banks are obliged to avail at least the last ten transactions conducted by a customer online.<sup>480</sup> The commercial banks are also obliged to keep the records of the complaints and the resolution given to such complaints.<sup>481</sup> Besides, the commercial banks are also obliged to notify the customers about the timeframe and circumstances in which the countermand of the electronic fund transfer could be accepted.<sup>482</sup> Similarly, the Draft Directive regulates only the contents of the customer protection policy, and the minimum contents provided by the Draft Directive are the direct replica of the contents of the customer protection policy provided in the Regulation of Mobile and Agent Service Directive with the exception of lowering of the obligation of the commercial banks to avail at least ten transactions online into five transactions.<sup>483</sup> But, unlike the Regulation of Mobile and Agent Banking Directive, the Draft Directive regulates the error notification,

---

<sup>475</sup> National Payment System Proclamation, Art 2(19).

<sup>476</sup> See section 2.2.1, p. 14

<sup>477</sup> See section 3.4.2.5, p.55.

<sup>478</sup> Regulation of Mobile and Agent Banking Directive, Art 12.9.

<sup>479</sup> Regulation of Mobile and Agent Banking Services Directive, Art 12.12.

<sup>480</sup> Regulation of Mobile and Agent Banking Services Directive, Art 12.8.

<sup>481</sup> Regulation of Mobile and Agent Banking Services Directive, Art 12.11.

<sup>482</sup> Regulation of Mobile and Agent Banking Services Directive, Art 12.10.

<sup>483</sup> Draft EFT Directive Art 23, 34 and Annex I(d), p.31.

complaint handling procedure and finally the remedies of such erroneous e-banking transactions.<sup>484</sup>

As far as the internal complaint handling procedure is concerned, the Draft Directive obliges the commercial banks to prescribe the procedures of lodgment, investigation and resolution of any complaint made by a customer.<sup>485</sup> The internal complaint handling procedure shall include the following three matters: the right of the complainer to appeal against the outcome of the investigation, most probably against the resolution made by the bank; the appeal procedure to the senior management of the bank; and the right of the complainer to submit his/her complaint to the NBE, after the exhaustion of the internal remedies provided by the bank.<sup>486</sup> In relation to this, the commercial banks are obliged to keep the number of complaints made by their customers with their respective resolution so as to avail to the NBE, or any other authorized body.<sup>487</sup>

As per the Draft Directive, a customer shall notify the commercial banks for any system error (malfunction) carrying out e-banking transactions.<sup>488</sup> For errors happening in transacting e-banking online using the electronic terminals, the customer can notify forthwith to the nearby branch of the bank. But, in cases the customer fails to appreciate the existence of error in making the e-banking transactions, the customer should notify orally or in writing within 15 working days after having received the documentation or receipt offered by the commercial banks.<sup>489</sup> The written notification of the customer shall include; the name and account number of the customer, the happening of error and the amount of the error, and the belief of the customer regarding to the causes/sources of the error.<sup>490</sup> For notification made orally by a customer, the bank may ask written confirmation to be provided to it.<sup>491</sup>

Once the customer notifies to the bank about the existence of an error, the bank shall investigate the alleged error, and notify the result of the investigation to the customer with not more than five working days.<sup>492</sup> Where the result of the investigation ascertains the existence of the error, the bank shall reimburse; (1) the principal, (2) fees and taxes associated with the

---

<sup>484</sup> Draft EFT Directive, Art 21-24.

<sup>485</sup> Draft EFT Directive, Art 23.1(a-b).

<sup>486</sup> Draft EFT Directive, Art 23.2(a-c).

<sup>487</sup> Draft EFT Directive, Art 24.

<sup>488</sup> Draft EFT Directive, Art 21.1.

<sup>489</sup> Draft EFT Directive, Art 21.3.

<sup>490</sup> Draft EFT Directive, Art 21.4(a-c).

<sup>491</sup> Draft EFT Directive, Art 21.5.

<sup>492</sup> Draft EFT Directive, Art 22.1(a-c).

transfer, and if any, (3) and other remedies (most probably damages) ordered by the NBE.<sup>493</sup> In correcting the errors, the bank shall not require additional costs to the customer.<sup>494</sup> Where the result of the investigation shows that there is no error occurred at all or an error occur in a manner and in amount which is different from what is alleged by the customer, the bank shall notify the customer such finding within ten working days from the receipt of the notification.<sup>495</sup>

In practice, the dispute settlement system provided for customers and the commercial banks is different. If the complainer is a customer, the customer shall first exhaust the internal remedies provided by the internal complaint handling procedure of the banks, and where the customer is not satisfied by the internal remedies of his/her bank, he/she can bring his case before the attention of the NBE. And where the NBE finds fault on the side of the bank, it gives a public remedy. Again, if the bank of the customer fails to take a correction based on the recommendation of the NBE, the customer can claim against his bank before the regular dispute settlement mechanism by attaching the finding of the NBE.<sup>496</sup> But, if the complainer is a bank, it cannot complain to the NBE rather it submits the case to the regular courts. Once the case is submitted to the regular courts, the cases shall be litigated based on the ordinary procedures applied for civil cases. This is all about what is provided about the dispute settlement system of e-banking transactions, and at this juncture, the dispute settlement system has the following limits:

*First*, as it is mentioned in the above, the National Payment System Proclamation fails to say anything about the settlement of disputes in relation to the consumer e-banking, even the Proclamation does not mandate the NBE to define the dispute settlement system of consumer e-banking by a directive. Similarly, the current directive, Regulation of Mobile and Agent Banking Directive, is silent about the settlement of disputes of the consumer e-banking.

*Second*, as it is mentioned in the above, in practice, the dispute settlement procedure for complains made by a customer and a bank is different; and this is occurred due to the absence of clear legal framework on the dispute settlement of consumer e-banking. Again, in relation to this, the NBE is reviewing the resolutions given by the banks to their customers without having the power to do so.

---

<sup>493</sup> Draft EFT Directive, Art 22.2(a&c).

<sup>494</sup> Draft EFT Directive, Art 22.2.

<sup>495</sup> Draft EFT Directive, Art 22.5.

<sup>496</sup> Interview with Ato Ephirem Baraki, Senior Legal Expert, NBE (Addis Ababa, 09 August 2018).

*Third*, as it is mentioned in the above, under the National Financial Inclusive Strategy, the NBE is entrusted to conduct a diagnostic to consider options for an effective dispute resolution mechanism (e.g financial sector ombudsperson) for the financial sector.<sup>497</sup> The Draft Directive is expected to be coherent with the policy intervention (National Financial Inclusive Strategy), but the directive totally disregards the possibility of the resolution of disputes by financial ombudsperson which is expected to be established by the NBE. Thus, the Draft Directive is not coherent with the policy framework of the country.

*Fourth*, as it is mentioned in the above, there are fraudulent transaction in relation to the cross-border e-banking transactions; and a number of Ethiopian business persons mainly hotel owners have experienced financial losses. But, as far as the dispute settlement system of cross-border e-banking is concerned, the current legal framework, both the National Payment System Proclamation and the Regulation of Mobile and Agent Banking Directive, are silent. Even the Draft Directive which is expected to include the dispute settlement system of the cross-border e-banking transaction is also silent. Thus, both the current and the forthcoming regulation are silent concerning the dispute settlement system of the cross-border e-banking transactions.

*Fifth*, in practice, as the interview collected from the customers of the banks indicates that the customers do not have a knowledge on the internal complaint handling procedures of their banks, and the main reason for this is the failure of the commercial banks to disclose their internal complaint handling procedure to their customers. Over that, no commercial bank has attached its internal complaint procedure in its official website. In relation to this, the NBE is not also carry out its inspection and monitoring mandate given by the Proclamation.

*Sixth*, with regard to complaints relating to the use of shared payment systems (interoperability of the e-banking products and services), the commercial banks mandated not to order their customers to submit its complaints to the other member of the shared payment system, but in reality, the commercial banks are ordering to their customers to submit their case to the bank which owns the ATM terminal which causes financial losses due to different reasons including error and malfunction.

*Seventh*, as far as jurisdiction issues is concerned, as it is mentioned in the above, the legislative power over e-banking is vested with the Federal Government; due to the principle that 'legislative power implies adjudicative power'; the adjudicative power over e-banking

---

<sup>497</sup> See section 3.3, p. 41.

cases lies with the federal courts. But, as per the delegation given by the constitution to state courts, state high and supreme courts can entertain cases relating to e-banking products and services.<sup>498</sup> As far as the local jurisdiction is concerned, both the current and the forthcoming regulations are silent, but, the researcher argues that the local jurisdiction issues of the e-banking products and services should be regulated properly. Mainly, the question, where is the location of e-banking transaction for the purpose of local jurisdiction should get an appropriate regulation.

### **3.4.4 Exit Regulation**

Similar to the granting of a license, the revocation of a license is among the stringently regulated issues of the banking business. The grounds and procedures of the revocation of the license of the traditional banking business is properly addressed under Dr. Solomon's Dissertation,<sup>499</sup> therefore, no more explanation is required. Some of the traditional banking rules on the revocation of a license apply for the revocation of the authorization of the e-banking products and services, but the unique features of e-banking products and services requires separate and comprehensive regulation. Having acknowledged the distinct features of the e-banking products and services, the Regulation of Mobile and Agent Banking Service Directive empowers the NBE to suspend or withdraw the authorization and order the e-banking product and service off on sufficient grounds including on the breach of the provisions of the Directive or in anticipation of any perceived or actual risk occurring in relation to the services.<sup>500</sup> But, the said directive does not properly defines the grounds and procedures of the revocation of the authorization of the e-banking products and services what it does is it only defines the powers of the NBE with regard to the revocation of the authorization of the e-banking products and services. Though the inclusion of the grounds and procedures of the revocation of the authorization of the e-banking products and services under the Draft Directive is expected, the Draft Directive does not say anything about the grounds and procedures of the revocation of the authorization of the e-banking products and services. The NBE has not yet revoked the authorization of any of the financial institution of the country, but where it likes to do so, it should have clear predetermined provisions that regulate the grounds and procedures of the revocation of the authorization of the e-banking product or services.

---

<sup>498</sup> FDRE Constitution, Art 78(2).

<sup>499</sup> Solomon Abay 44-46 & 290-296.

<sup>500</sup> Regulation of Mobile and Agent Banking Service Directive, Art. 6.10.

### 3.5 Regulatory Issues of E-Banking

The enforcement of the e-banking regulation is not left to one institution, instead by one or another means significant number of government institutions participate in the enforcement of such regulations. As we all know, there are two enforcement institutions; general and sector specific enforcement institutions; INSA and FIC are among the general enforcement institutions which are engaged in the enforcement of the e-banking regulations in carryout their day to day activities, whereas the NBE and the National Payment System Council are the sector specific institutions in which the NBE is the primary organ which is entrusted to enforce the e-banking regulations, but the function of the National Payment System Council is only limited to advise the NBE. In the next sub-sections, the detail enforcement and advisory roles of these two sector specific institutions is discussed.

#### 3.5.1 National Bank of Ethiopia

According to the Amended National Bank Establishment Proclamation, the NBE is the primary organ that regulate and supervise payments, clearing and settlement systems.<sup>501</sup> As an extension of this, the National Payment System Proclamation entrust the NBE with law-making [enacting directives]<sup>502</sup> and administrative powers [monitoring, investigating, and sanctioning].<sup>503</sup> But, as far as dispute settlement power is concerned, the relevant legislations—Amended National Bank Establishment Proclamation and the National Payment System Proclamation—are silent, but in practice, the NBE is exercising adjudicative power on some selected issues.<sup>504</sup>

As it has already mentioned repetitively in the above sections, the primary legislations delegate the NBE to issue directives for detail regulations, but such primary legislations failed to define the legislative process of the directives to be issued by the said institution. Again, as Ethiopia does not have a comprehensive administrative law, that determines among other things the administrative rule making procedure of the directives issued by the administrative organs, the NBE by its own discretion determine the rule-making process of the directive that it issues. Even within the NB itself which directorate/s is/are responsible for

---

<sup>501</sup> National Bank of Ethiopia Establishment (as Amended) Proclamation, Art 5(15).

<sup>502</sup> National Payment System Proclamation, Articles 6(6), 10(5), 14(3), 19(3), 20(2), 23(4), 24(5), 31(4), and Art 37(2). See also National Bank of Ethiopia Establishment (as Amended) Proclamation, Art 27(2).

<sup>503</sup> For further discussion on power of NBE See chapter five of Solomon Abay, *Financial Market Development, Policy and Regulation: The International Experience and Ethiopia's need for Further Reform*, P.282-. With regard to the detail monitoring, investigation and sanctions powers of the NBE for matters relating to e-banking, see Chapter Three of this Thesis.

<sup>504</sup> Interview with Ato Ephirem Baraki, Senior Legal Expert, NBE (Addis Ababa, 09 August 2018).

the drafting of e-banking directives is not clear. In practice, the directives related with e-banking are drafted mainly by the Payment and Settlement Directorate with the participation of the Banking Supervision Directorate and the Legal Directorate of the of the NB.<sup>505</sup> The Draft Electronic Fund Transfer Service Directive is prepared by the Payment and Settlement Directorate with the participation of the Banking Supervision Directorate and the Legal Directorate of the NB.<sup>506</sup> But, the Draft Agent Banking Directive is prepared by the Banking Supervision Directorate with the participation of the Payment and Settlement Directorate and the Legal Directorate of the NBE.<sup>507</sup> Once the directives are drafted by the said directorates, the drafts are submitted to the Vice-Governor of the NB, and the Vice-Governor distributes the draft for comment to all directorates of the NBE.<sup>508</sup> Again, after commented by the top management of the NB, it has sent to the commercial banks, Ethiopian Banker's Association and the two switches, Premier Switch Solutions (PSS) and EthSwitch.<sup>509</sup> The comments of the two directives is not yet collected from the banks and the operators; it is very early to say anything as to the inclusion of the comments forwarded by the stakeholders, but the initiation of the NB to include the comments of the stakeholders is commendable.

The last not least issue with drafting of directives is the publication issue of the directives. As we all know, directives are not publicized in Ethiopia, similarly, the directives issued by the NB do not publicized by a official publication channel like what we know 'Negarit Gazzet' but what the NB do is it allow the access of the directive by providing such directive in its official website. In addition to the access through the official website, the NB notifies to each banks, microfinances, operators and the Ethiopian Banker's Association about the issuance of a new directive.<sup>510</sup> With regard to publication of directives through web, the NB has a good experience which should be shared by other ministries of the country.

With regard to the dispute-settlement power (quasi-judicial), for complaint of the customers in relation to e-banking and disputes among the participants of the national payment system

---

<sup>505</sup> Interview with Ato Solomon Damitew, Principal Manager Payment Systems Over Sight and Development, NBE (Addis Ababa, 04 May 2018).

<sup>506</sup> Interview with Ato Solomon Damitew, Principal Manager Payment Systems Over Sight and Development, NBE (Addis Ababa, 04 May 2018).

<sup>507</sup> Interview with Ato Solomon Damitew, Principal Manager Payment Systems Over Sight and Development, NBE (Addis Ababa, 04 May 2018).

<sup>508</sup> Interview with Ato Solomon Damitew, Principal Manager Payment Systems Over Sight and Development, NBE (Addis Ababa, 04 May 2018).

<sup>509</sup> Interview with Ato Solomon Damitew, Principal Manager Payment Systems Over Sight and Development, NBE (Addis Ababa, 04 May 2018).

<sup>510</sup> Interview with Ato Solomon Damitew, Principal Manager Payment Systems Over Sight and Development, NBE (Addis Ababa, 04 May 2018).

the NBE has tried to exercise investigative and adjudicative power.<sup>511</sup> For complains of customers of the banks in relation to financial loss happened mainly due to malfunction and system error and disputes among the participants EATS, the NBE investigate both the consumer and non-consumer e-banking systems and pass a public remedy based on its finding.<sup>512</sup> But, there is no separate directorate or committee which is entrusted with investigating and adjudicating of the disputes arise in relation to the e-banking.<sup>513</sup> If the complain is in relation to participants of the EATS and to the use of electronic channels of the banks, the Directorate for Payment and Settlement receives the complains and provides a public remedy based upon its findings, but, where the dispute is in relation to agent banking, the Banking Supervision Directorate is responsible to receive the complains and provide a public remedy based upon its finding.<sup>514</sup> Public remedy is to mean that once the NBE finds that a customer has lost his money due to malfunction or error, it recommends to the bank of the customer to refund the said money, but it cannot forced it; where the bank denies the recommendation of the NBE, the NBE will give the results of the investigation to the customer and the customer can claim his rights before the court by attaching the investigation result.<sup>515</sup> But, the NBE does not receive complaints from the banks; where a bank is the victim because of the irresponsible act of its customers, it has to sue before the regular courts.<sup>516</sup> By now, there is no separate directorate or committee which is entrusted with investigating and adjudicating of e-banking disputes.<sup>517</sup>

As you can see from the above paragraphs, the current regulation provides significant issues of the institutional framework of the NBE, but it is not adequate enough; thus, the institutional framework of the NBE has the following limits:

*First*, the National Payment System Proclamation delegates the NBE to issue directives on many issues of the e-banking, but similar to the other primary legislations of the country, it has failed to define the legislative process of the directives. In dead, it is not usual to define

---

<sup>511</sup> Interview with Ato Solomon Damitew, and interview with Ato Kebede Demissie.

<sup>512</sup> Interview with Ato Solomon Damitew, and interview with Ato Kebede Demissie.

<sup>513</sup> Interview with Ato Ephirem Baraki, Senior Legal Expert, National Bank of Ethiopia (Addis Ababa, 09 August 2018).

<sup>514</sup> Interview with Ato Ephirem Baraki, Senior Legal Expert, National Bank of Ethiopia (Addis Ababa, 09 August 2018).

<sup>515</sup> Interview with Ato Ephirem Baraki, Senior Legal Expert, National Bank of Ethiopia (Addis Ababa, 09 August 2018).

<sup>516</sup> Interview with Ato Ephirem Baraki, Senior Legal Expert, National Bank of Ethiopia (Addis Ababa, 09 August 2018).

<sup>517</sup> Interview with Ato Ephirem Baraki, Senior Legal Expert, National Bank of Ethiopia (Addis Ababa, 09 August 2018).

the legislative process of directives and or regulations under the primary legislations, but what is usual is the legislative process of secondary legislations is defined under the administrative laws. As we all know, Ethiopia has not yet proclaimed administrative law and due to this the administrative organs including the NBE arbitrary determines the legislative process of the directives. Over that, the NBE does not have a directive or a working procedure issued by it which defines the legislative process of the directives in which it is delegated to issue directives.

*Second*, once the legislative organ delegates to the NBE Ethiopia to issue directives on different matters of e-banking, it does not have a mechanism to check whether the said directives are issued or not. It was before seven years ago that the legislative organ delegates to the NBE to issue directives on different matters of e-banking, but till now the NBE failed to issue the said directives. Over that, the absence of limit within which time should the NBE issue a directive makes the NBE to be dormant.

*Third*, the two relevant primary legislations—Amended National Bank Establishment Proclamation and the National Payment System Proclamation—and its implementing directives are silent on the dispute settlement power of the NBE, but in practice, as it is mentioned in the above, the NBE is exercising *quasi-judicial* power. It is through the law that the powers and functions of the government institutions are defined: and where a government institution exceeds from what is entrusted to exercise, it is *ultra-vires*. Thus, as the NBE is exercising *quasi-judicial* power without having a power to do so, therefore, such acts of the NBE constitutes *ultra-vires*.

*Fourth*, the National Financial Inclusive Strategy directs the establishment of financial ombudsperson which is primarily entrusted to adjudicate the e-banking disputes between customers and banks as well as the disputes between the participants of the national payment system, but the said organ has not yet established. Thus, the failure of the NBE to establish the said organ negatively affects consumer's right to get speedy justice.

*Fifth*, in practice, the NBE is calling to the TCCPA to accept the customer's claim, but the authority rejects under the guise that it has no material jurisdiction to entertain e-banking disputes though consumers of the e-banking products and services needs equal protection with the consumers of other goods and services. Thus, by now, even the authority which is entrusted to protect the consumers is not carrying out its obligation; as a result of this, the consumers of the e-banking are left unprotected.

*Sixth*, with regard to competition issues of the e-banking, similar to the above-mentioned, the powers and functions of the NBE and the TCCPA are not properly defined. Whether all competition issues of the banking business including the competition issues of the interoperability e-banking products and services and price are still within the compound of the NBE or not is not clear.

### 3.5.2 National Payment System Council

According to the National Payment System Proclamation, the government may establish National Payment System Council which has advisory role to the NBE on issues related to the national payment system.<sup>518</sup> The establishment of the council is not mandatory, but where the government believes that it is necessary, it has the discretion to establish the said Council. Over that, the Proclamation also fails to define the qualification and composition of the National Payment System Council. But the minute of the National Payment System Proclamation defines the composition of the Council; and according to the minute of the NPSP, the members of the Council are Ethio telecom, EEP Co, MOFED, ERCA, ECX and ECC.<sup>519</sup> The government is given the discretion to establish National Payment System Council, though it has not yet established the said Council. At this juncture, the organization of the NPSC has the following limits:

*First*, the Proclamation gives a discretionary power to the government to establish the said Council, but the provision which delegates the government to establish National Payment System Council has some ambiguities. It states, “*The government may establish a National Payment System Council which shall have an advisory role to the National Bank with regard to the national payment system.*”<sup>520</sup> [Emphasis mine]. Who is the ‘government’ the executive or the legislative organ; it is not clear whether the National Payment System Council will be established by a proclamation or a regulation. In spite of that, the government neither by a proclamation nor by a regulation establishes the said Council.

*Second*, though it is early to comment on the composition of the NPSC by referring to the minute of the NPSP, we can say that the composition of the Council failed to include some of the important agencies and ministries who have a say on the national payment system; these agencies and ministries include TCCPR, INSA, FIC, EBA, operators, consumer’s associations, and Office of General Attorney.

---

<sup>518</sup> National Payment System Proclamation, Art 32.

<sup>519</sup> See the minute of the National Payment System Proclamation, 16.

<sup>520</sup> See the minute of the National Payment System Proclamation.

## **CHAPTER FOUR**

### **CONCLUSION AND RECOMMENDATION**

#### **5.1 Conclusion**

The unprecedented technological development in general and the birth of the internet in particular has changed the way banking services has been delivered for years. Now days, the success of a bank is measured against its innovation to deliver innovative products and services to its customers. Thus, banks are forced to introduce technologies in performing their day to day activities and e-banking is one of the innovative services which enables the banks to provide banking products and services through electronic channels: the introduction of technology is not an option to the traditional banks rather it is an obligation that is imposed by the central banks of many countries including National Bank of Ethiopia. However, electronic banking is not without risks: it is disclosed to many risks including to strategic, operational, legal and reputational risks. Consequently, such risks associated to the electronic banking causes the loss of millions of dollars yearly. To counter these problems the global community has been trying to deal with those risks by establishing international, regional and national legal and institutional framework that aims to ensure among other things secured, prudent and predictable e-banking services to the users.

The main purpose of this research has been to make an analysis of the limits of e-banking regulation in Ethiopia. It sought to make an investigation on the adequacy and efficacy of the current policies, laws and institutional frameworks governing the provision of the e-banking products and services. To achieve the said objective, three specific objectives were set to define the contribution of this research: The first was to examine the practice and problems of e-banking in Ethiopia. The second specific objective was to examine and analyze the limits of the current policies, laws and practices in regulating e-banking. The third and the last specific objective were to propose a suitable and responsive policy, legal and institutional framework.

As far as the first research objective is concerned, both consumer and non-consumer e-banking services are currently practiced in Ethiopia. The main actors of the non-consumers e-banking services are the National Bank of Ethiopia, commercial banks, Premier Switch Solution and EthSwitch S.C. The National Bank of Ethiopia as the owner, operator and participant of the EATS, which comprises the RTGS and ACH, is the main non-consumer e-banking service provider followed by the two share (Premier Switch Solution and EthSwitch)

companies established by consortium of the private and government commercial banks. With regard to consumer e-banking, by now, the Ethiopian banks are providing four kinds of e-banking services; namely, ATM banking, mobile banking, POS banking and Internet banking. In addition to these, recently, the Ethiopian banks begun to provide M-money and M-wallet services. As both the ATM and POS banking is handled using payment instruments, the commercial banks are also issuing payment instruments that enables to their customers to access the ATM and POS banking services; and the payment instruments that are used to access such e-banking products and instruments are debit and stored-value cards; the issuance of credit card is not yet legalized. Over that, the Ethiopian banks are providing electronic bill presentment and payment services through the e-banking products and services. But, with regard to cheque truncation, there is a project which is working on the introduction of such services, but till final writing of this research, the project is not finalized and the banks have not yet begun the provision of cheque truncation services.

Coming to the problems of e-banking products and services, by now, the Ethiopian e-banking business is surrounded by many problems including unauthorized access of customer's account (fraudulent transaction), system malfunction, human error, failure to execute the electronic fund transfer, non-execution of e-banking transaction, loss of various rights including the right to countermand the electronic fund transfer, privacy and confidentiality of customer's financial information, cross-border fraudulent transactions, absence of clear law that defines the allocation of losses, unfair terms and conditions of e-banking service agreements, and absence of cost-effective dispute settlement system.

As far as the second research objective is concerned, Constitution, primary legislations (National Payment System proclamation), secondary legislations (Regulation of Mobile and Agent Banking Service Directive No. FIS/01/2012, Fraud Monitoring Directive No. SBB/59/2017, Circular No. BSD/06/2013, Circular No. FIS/02/2014 and Circular No. FIS/01/2014) are the major laws that determine the legal framework of e-banking business of the country. And according to the Constitution, the power to enact policies and laws on matters relating to e-banking lies with the Federal Government, again, from among the Federal Government organs, it is the HOPR who has the power to issue the policies and laws relating to e-banking regulations. Moreover, both the Council of Ministries and the National Bank have a delegated legislative power to enact regulations and directives that regulate the e-banking products and services respectively. With regard to the enforcement institutions,

Article 77(4) of the Constitution as well as proclamation No.591/2008 empowers the Council of Ministers and National Bank of Ethiopia to enforce the laws issued by the legislative organ of the government.

Like any other country payment systems, the Ethiopian payment system law classified the payment systems into two; large value funds transfer system and retail funds transfer system. While 'large value fund transfer system' consists of inter-bank funds transfer system, high priority and time critical government fund transfers, clearing and settlement of securities of the government and any other fund transfer system prescribed by the NBE as a large value, but, 'retail funds transfer system' is defined as a cheque clearing system administered by the NBE or by a person authorized by the NBE. And again, according to the Ethiopian payment system law, 'fund transfer' includes POS transfers, ATM transactions, and transfers initiated by telephone, internet, card and other devices. Thus, e-banking products and services is one form of retail fund transfer that is regulated by the National Payment System proclamation. However, the NPSP delegates most aspects of e-banking to be regulated by directives that was expected to be issued by the NBE. But, most of the supposedly implementing directives that was expected to be issued by the NBE has not yet issued with the exception of Regulation of Mobile and Agent Banking Service Directive and some circular letters which clarifies such directive. But, by now, the NBE prepared a Draft Electronic Transfer Service Directive, and this directive is distributed to the commercial banks and Ethiopian Banker's Association for comment. Thus, the legal and regulatory framework of the e-banking business is governed by the national payment system law and it's implementing directives.

As per the Regulation of Mobile and Agent Banking Service Directive, it is only a legally established financial institution that can be engaged in the provision of e-banking products and services, again as per the same directive, financial institution is a bank or microfinance institution. Thus, e-banking services can be provided only by banks and microfinances; and to provide such services the financial institutions should get prior approval from the NBE. The entry requirements of the Regulation of Mobile and Agent Banking Service Directive, which is the ongoing directive, only provides the submission of three documents; business plan, operational policy and procedure, and risk management policy and procedure. Once the NBE proves the fulfillment of these policy and procedure documents, it authorizes the financial institution to provide e-banking products and services. Once the financial institution gets an authorization, it can begin the provision of the e-banking services to its customers.

Once it begins operation, the operational regulations provided by the laws come to view. The Ethiopian national payment system law and its implementing directives once again regulates the following matters; standard terms and conditions of the e-banking service agreements, preauthorize electronic fund transfer, cheque truncation, interoperability of the e-banking products and services, privacy and confidentiality of the electronic account, authentication e-signatures, admissibility of the e-banking records, finality of e-banking transactions, fees and charges of e-banking transactions, and the allocation of losses. The breach of one or more of the obligations provided in operational regulations may call the NBE to take corrective measures including suspension and revocation of the authorization of the financial institution. The NBE may suspend or revoke the authorization of the financial institution on sufficient grounds including on the breach of the provisions of the national payment system law and it's implementing directives or in anticipation of any perceived or actual risk occurring in relation to the services.

As far as the regulatory framework is concerned, the National Payment System Proclamation entrust the NBE with law-making and administrative powers. The Proclamation delegates the NBE to issue directives on numerous matters of the e-banking business, but the said Proclamation does not say anything about the law-making process of the directives to be issued by the NBE. In practice, the directives related with e-banking are drafted mainly by the Payment and Settlement Directorate with the participation of the Banking Supervision Directorate and the Legal Directorate of the of the NB. With regard to settlement of disputes, the NBE is not entrusted adjudicatory power by the relevant laws, but in practice the NBE is exercising adjudicatory power on some selected e-banking disputes, but, in practice, the NBE is exercising investigative and adjudicative power for complains submitted to it by the consumers of the e-banking. But, the NBE does not accept a claim by the banks against their customers; such cases are by now adjudicated by the regular litigation process.

As far as the establishment of advisory body is concerned, though the National Payment System Proclamation gives discretion to the government to establish a National Payment System Council which acts as advisor of the NBE, the government neither by a proclamation nor by a regulation establishes the said Council. In relation to this, the minute of the National Payment System Proclamation defines the composition of the council; and according to it, the members of the council are Ethio telecom, EEPCo, MOFED, ERCA, ECX and ECC. Thus, the minute fails to include the EBA and TCCPR from being members of the said Council.

## 5.2 Findings

The analysis of both the primary and secondary data reveals that the Ethiopian e-banking regulation has the following limits:

- i. The first theme that appears out of the primary data collected through interview from officials of NBE is that there are initiations to formulate the national retail payment strategy in cooperation with the World Bank, but such initiation is in its early stage and is not expected to end in the near time; thus, by now, the country does not have a retail payment strategy that defines the objectives, strategic guidelines, and regulatory intervention activities of the NBE in regulating the e-banking business. The existence of a retail payment strategy (policy framework) should preclude the legal and regulatory frameworks of the e-banking business, but till the end of this paper the country has not yet come up with separate and comprehensive national retail payment strategy.
- ii. The second emerged theme is that the NBE receives excessive delegation to issue directives even on matters which should be regulated by a primary legislation; it is through a primary legislation, not by a directive, that the basic rights and obligation of citizens is defined. But, in spite of the delegation given to it, with the exception of Regulation of Mobile and Agent Banking Service Directive, the NBE has not yet issued a comprehensive directive that regulates all matters that it has delegated to issue a directive. But this time, the NBE prepares a Draft Directive by directly copying the provisions of the US EFT Act and the Bangladesh electronic fund transfer law; almost all provisions of the draft are copied from the US EFT act but very few articles of the Bangladesh EFT law is also copied. The drafters of the directive copied the US EFT Act without considering the difference in development and customers' awareness. Thus, the ignorance of the level of knowledge of both the e-banking service providers and the customers of such e-banking products and services may make the implementation of the directive difficult. In addition to the problems caused by transplantation, the Draft Directive does not provide a regulation for cheque truncation, issuance of payment instruments, dispute settlement system (it only provides internal complaint handling procedure), cross-border e-banking, authentication of e-banking signatures, and admissibility of e-banking records.
- iii. The NBE Ethiopia has not yet issued a directive for the basic terms and conditions of the e-banking service agreements; thus, the absence of directive on the basic standard

terms and conditions of the e-banking service agreements opens a room for the commercial banks to determine the terms and conditions arbitrarily. In relation to this, in practice, the commercial banks do not disclose the standard terms and conditions to their customers, what they do are they only disclose a very short form (application form) to their customers for signature. As a result of this, customers do not have knowledge on the terms and conditions of the e-banking service agreements. The NBE was required to discover this problem through inspection and take appropriate remedy, but the NBE is not carrying out its obligations properly. Over that, the short form applications provided to customers for signatures are prepared by Amharic and in some banks both in Amharic and in English side by side. Thus, those customers who do not read and understand the Amharic and English languages are only putting their signatures without understanding what the terms and conditions of the agreement say.

- iv. The commercial banks are obliged not to require their customers to present their complaints to any other party of the shared payment system, though in practice the commercial banks are requiring their customers to submit their complaints against the owner of the shared payment system which causes the problem/complain (ATM owner). In getting back their money, the customers of the bank are waiting up for long period of time.
- v. By now, there is no regulation that regulates; the standard formats of the e-banking records, the obligation of the banks to provide the copy of the e-banking to their customers either by paper-based or electronically, and the grounds and procedures of contrary proof of the e-banking records. And more importantly, scientifically the proper functioning of the system at the time of issuance of the electronic receipt is required for the validity of the e-banking record, but the National Payment System Proclamation fails to include it. Thus, by now, whether the system issues the electronic receipt correctly or erroneously, such electronic record is admissible. The absence of a regulation on the contrary proof in general and the absence of the proper functioning of the system as a parameter in validating the electronic evidence in particular is causing significant losses to the consumers of the e-banking.
- vi. By now, there is no clearly stipulated provisions that regulates the allocation of losses arises out of fraudulent e-banking transactions, error and improper handling of payment instruments.

- vii. According to both the current and upcoming directives, the commercial banks have the discretion to determine the transaction limit of the e-banking transactions without the intervention of the regulator, NBE. Even the regulations do not mandate the commercial banks to notify the regulator about the transaction limits. The information gathered from the NBE officials reveal that in practice the NBE only assures the existence of the transaction limits, but it does not have the power to order or even recommend about the amount of the transaction limits of each e-banking products and services. Thus, the absolute discretion given to the commercial banks to determine the transaction limits of the e-banking products and services may defeat the very goal of transaction limit regulations.
- viii. The NBE has not yet issued a regulation that regulates the prices of the e-banking products and services, though it is mandated to do so, but the information gathered from the officers of the NBE reveal that the NBE is regulating the price of the e-banking products and services through the price strategy submitted to it by the commercial banks at the time of the authorization of the e-banking products and services.
- ix. There are fraudulent transaction in relation to the cross-border e-banking transactions; and a number of Ethiopian business persons mainly hotel owners have experienced financial losses. Again, the dollar accountholders can access the electronic terminals of foreign banks outside of Ethiopia, the researcher not discovered a problem in relation to this, but how it can be settled if a dispute arises in relation to this is also a question that needs an answer. As far as the dispute settlement system of cross-border e-banking is concerned, the current legal framework is silent. Even the Draft Directive which is expected to include the dispute settlement system of the cross-border e-banking transaction is also silent.
- x. The Regulation of Mobile and Agent Banking Service Directive dictates that the authorization of the financial institution could be suspended or revoked on sufficient grounds, though it fails to define what constitutes 'sufficient ground'. Again, the procedures of suspension and revocation of a license is not defined by the said directive. The Draft Directive is expected to address this gap, but similar to the ongoing directive the Draft Directive is silent about the grounds and procedures of the suspension and revocation of the authorization of the financial institutions.
- xi. The National Payment System Proclamation delegates the NBE to issue directives on many issues of the e-banking, but similar to the other primary legislations of the

country, it has failed to define the legislative process of the directives. In relation to this, it was before seven years ago that the legislative organ delegates to issue directives on different matters of e-banking, but till now the NBE failed to issue the said directives. This indicates that how much the legislative control is weak. Over that, the absence of limit within which time should the NBE issue a directive makes the NBE to stay dormant.

**xii.** The current regulation does not entrust the NBE to settle e-banking disputes, but in practice the NBE is exercising *quasi-judicial* power; as the NBE is exercising *quasi-judicial* power without having a power to do so, therefore, such acts of the NBE constitutes *ultra-vires*. In relation to dispute settlement power, the TCCPA rejects the claim of the customers of the bank by saying it has no material jurisdiction to entertain e-banking disputes.

**xiii.** The National Payment System Proclamation says that the ‘government’ may establish National Payment System Council, but this is ambiguous, who is the ‘government’ the executive or the legislative organ; it is not clear whether the National Payment System Council will be established by a proclamation or a regulation. In spite of the discretion given to it, the government neither by a proclamation nor by a regulation establishes the Council. Again, though it is early to comment on the composition of the NPSC, but by referring to the minute of the NPSP, we can say that the composition of the Council failed to include some of the important agencies and ministries who have a say on the national payment system; these agencies and ministries include TCCPR, INSA, FIC, EBA and Office of General Attorney.

## **5.2 Recommendation**

Based on the above findings the following measures of actions are provided as recommendations:

**i.** As it is legally mandated, the NBE should facilitate the drafting process of the national retail payment strategy that provides guidelines regarding the e-banking business of the country. The early formulation of the national retail payment strategy not only guides the Draft Directive and other subsequent e-banking laws, but it also directs the regulator in regulating the e-banking business. The policy document should include the main objectives, guidelines and regulatory interventions of the country’s

retail payment. In formulating the national retail payment strategy, the country needs to consider the objectives, guiding principles and regulatory interventions recommended by the the World Bank National Retail Payment Strategy Consultative Report. As the policy framework should preclude the legal and regulatory frameworks of the e-banking regulation, the drafting process of the national retail payment strategy should be finalized early so as to use as a basis for laws that regulates the e-banking business of the country.

- ii.** To address the problems of uncertainty in the law as well as to define basic rights and duties of both the banks and the users of the e-banking products and services, the country needs a separate and comprehensive primary legislation that regulates the e-banking business. It is through a primary legislation, not by a directive, that the basic rights and obligation of citizens is defined; for this reason, the Draft Directive prepared by the NBE should be developed and proclaim as a primary legislation, not as a directive. Thus, in addition to the issues regulated by the Draft Directive, the primary legislation should provide a regulation for: authentication of e-banking signatures, admissibility of e-banking records, cheque truncation, issuance of the payment instrument, dispute settlement system, cross-border e-banking, and price issues of the e-banking business. Again, to address the arbitrary suspension and revocation of authorization by the regulator, the primary legislation is also required to define the grounds and procedures of the suspension and revocation of the authorization of the commercial banks.
- iii.** By now, there is no law that regulates; the basic terms and conditions of the e-banking service agreements, preauthorized e-banking transactions, internal complaint handling procedure, finality of e-banking transactions, interoperability of e-banking, and the allocation of losses happened due to fraudulent and erroneous e-banking transactions, but with all its limits the Draft Directive provides a regulation for such matters. Thus, the primary legislation should also regulate these matters by addressing the limits of the Draft Directive.
- iv.** The upcoming regulation should reconsider the absolute discretion of the commercial banks to determine the transaction limits of each e-banking products and services. The NBE should be empowered to determine the circumstances which should be taken into consideration in determining the transaction limits of the e-banking products and services. Over that, considering the flexible and dynamic nature of the e-banking products and services, the NBE should be empowered to determine the maximum

limit (ceiling) of the e-banking products and services by a circular letter. The close regulation of the regulator helps to attain the very goal of the transaction limits, mitigating the possible losses of the fraudulent e-banking transactions.

- v. To ensure the competitiveness, sustainability and affordability of the e-banking products and services, the NBE should be empowered to define the circumstance that should be taken into consideration in fixing the charges and fees associated with e-banking products and services. And over that, the researcher recommends that the NBE should be entrusted to determine the minimum and maximum fees and charges associated with the e-banking products and services. In doing so, both the competition and financial inclusive objectives should be considered.
- vi. To avert the financial losses happening due to the fraudulent cross-border e-banking transaction and provide a means where by the losers can get justice, the country needs to provide a regulation for the cross-border e-banking. The country needs also to provide the minimum requirement for the contract between the Ethiopian banks and their intermediary banks. In providing regulation to the cross-border e-banking, the country should consider the principles and guide lines provided by the BCBS Management and Supervision of the Cross-Border Electronic Banking Activities. Besides, the needs to enable and require the NBE to work with other country's regulators and international organizations including the BCBS and ITU in order to provide a coordinated regulation that minimize and averts the dangers of the cross-border fraudulent e-banking transactions.
- vii. The consumers of the e-banking has the right to get speedy justice, but in practice, the commercial banks are denying this right by ordering their customers to submit their claims against the bank who owns the electronic terminal, though they are prohibited by the law to do so; therefore, the NBE is required to properly carry out its inspection and monitoring obligation so as to ensure the enforcement of such right provided by the law.
- viii. The administrative law-making process is not yet regulated, and Ethiopia needs to consider the enactment of a comprehensive administrative law that regulates among other things the administrative law-making process. But, as the country experience witnessed the enactment of a law takes long years; therefore, up to the coming the comprehensive administrative law that fills the gap, the NBE should at least enact a directive that regulates the law-making process of the directives with full participation of the stakeholders including the commercial banks, EBA and the

operators. In relation to this, the legislative organ which delegates the NBE to issue directives on different matters of the e-banking should use its legislative control system to check whether the NBE issued a directive as per its delegation or not. Over that, the legislative organ should provide a time limit within how many days/months/years the NBE should issue the directives.

- ix. To make coherent with the National Financial Inclusive Strategy as well as to legitimize the current initiations of the NBE, Ethiopia needs to establish a financial ombudsperson which is entrusted to settle e-banking disputes; the composition, appointment, adjudicative power and its working procedures should be also properly defined by a law. In relation to this, the adjudicative power of the financial ombudsperson and the TCCPR should be also clearly demarcated.
- x. To facilitate the issuance of the National Retail Payment Strategy as well as to gain the benefits of the advisory roles of the National Payment System Council, the country needs to establish the said institution that not only provides advices to the NBE, but also minimizes the dangers of the discretionary power of the regulator. It does not matter whether the Council is established by a proclamation or a regulation, what matter is the government should establish the Council so as to advise the NBE. In relation to this, it is early to comment on the composition of the NPSC, but by referring to the minute of the NPSP, the researcher argue that the composition of the Council failed to include some of the important agencies and ministries who have a say on the national payment system, and to have an excellent Council that carries out its obligations properly, TCCPR, INSA, FIC and EBA should be included as members of the Council..

## Bibliography

### I. Books

1. Apostolos Gkoutzini, *Internet Banking and the Law in Europe: Regulation, Financial Integration and Electronic Commerce*, Cambridge University Press, Cambridge, New York, 2006.
2. Ato Gezu Ayele Mengistu, 'የኢትዮጵያ የባንክ እና የሚተላለፉ የንግድ ሰነዶች', Far East Trading PLC Press, Addis Ababa, 2009.
3. Ato Kefani Gurmu., 'የባንክ ስራና ሕጎች', Aster Nega Printing Press, Addis Ababa, 2010.
4. Tilahun Teshome, *Basic Principles of Ethiopian Contract Law*, Addis Ababa University, Addis Ababa, 2007.

### II. Articles

1. Ayana Gemechu Bultum, 'Factors Affecting Adoption of Electronic Banking System in Ethiopian Banking Industry', *Journal of Management Information System and E-commerce*, Vol. 1, No. 1, 2014. <[http://jmisenet.com/journals/jmisenet/Vol\\_1\\_No\\_1\\_June\\_2014/1.pdf](http://jmisenet.com/journals/jmisenet/Vol_1_No_1_June_2014/1.pdf)> [Last accessed 5, November 2017].
2. Daniel Fluhmann e tal, Regulation of Electronic Payment Service Providers in Switzerland: An overview with a Focus on Retail Payment Services, 2017, <[https://www.baerkarrer.ch/publications/Fluhmann\\_Hsu\\_Ender\\_Aufsatz.pdf](https://www.baerkarrer.ch/publications/Fluhmann_Hsu_Ender_Aufsatz.pdf)> [Last accessed 5, November 2017].
3. ITU, Digital Financial Services: Regulating for Financial Inclusion – An ICT Perspective, 2016, <[https://www.itu.int/dms\\_pub/itu-d/opb/pref/D-PREF-BB.REG\\_OUT02-2016-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.REG_OUT02-2016-PDF-E.pdf)>, [Last accessed 5, November 2017].
4. Kinfu Micheal Yilma e tal, 'The Internet and Regulatory Responses in Ethiopia: Telecoms, Cybercrimes, Privacy, E-commerce, and the New Media', *Mizan Law Review*, 2015, Vol. 9, No. 1.
5. Wondwossen Tadesse e tal, E-payment: Challenges and Opportunities in Ethiopia, United Nations Economic Commission for Africa, 2005.
6. Dr. Arun Korath e tal, A study on the Consumer Adoption Electronic Banking Technology with Reference to Ethiopian Banking sector, *International Journal of Science Technology and engineering*, vol. 2, Issue 10, April 2016.
7. Gardachew Werku, Electronic-Banking in Ethiopia- Practices, Opportunities and Challenges, *Journal of Internet Banking and Commerce*, Vol. 15 No. 2 August 2010.

8. Rupa Rege Nitsure, 'E-Banking: Challenges and Opportunities', *Economic and Political weekly*, 2003, Vol. 38, No. 51/52, PP. 5377-5381, p. 5377. < <http://www.jstor.org/stable/4414436> > [Accessed 19-04/2018]

### III. Legal Instruments

#### a. International Treaties, Declarations and Resolutions

1. Basel Committee on Banking Supervision, Management and Principles of Cross-Border Electronic Banking Activities, July 2003, at <<https://www.bis.org/publ/bcbs99.htm>>, [Last accessed 5, November 2017].
2. Basel Committee on Banking Supervision, Principles of Risk Management on Electronic Banking, May 2003, at <<https://www.bis.org/publ/bcbs82.htm>>, [Last accessed 5, November 2017].
3. Basel Committee on Banking Supervision, Sound Management of Risks Related to Money Laundering and Financing of Terrorism, February 2016, <<https://www.bis.org/bcbs/publ/d353.htm>>, [Last accessed 5, November 2017].
4. Basel Committee on Payments and Market Infrastructure, Charter of the Committee on Payments and Market Infrastructure, <<https://www.bis.org/cpmi/charter.pdf>>, [Last accessed 5, November 2017].
5. OECD, Online Payment Systems for E-Commerce, 8 April 2006, <<https://www.oecd.org/sti/ieconomy/36736056.pdf>>, [Last accessed 5, November 2017].
6. UNCITRAL Legal Guide on Electronic Funds Transfers, New York, 1987, at <[http://www.uncitral.org/pdf/english/texts/payments/transfers/LG\\_E-fundstransfer-e.pdf](http://www.uncitral.org/pdf/english/texts/payments/transfers/LG_E-fundstransfer-e.pdf)>, [Last accessed 5, November 2017].
7. UNCITRAL Model Law on Electronic Commerce, 1996, at <[http://www.uncitral.org/uncitral/en/uncitral\\_texts/electronic\\_commerce/1996Model.html](http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html)>, [Last accessed 5, November 2017].
8. UNCITRAL Model Law on Electronic Signature, 2001, at <[http://www.uncitral.org/uncitral/en/uncitral\\_texts/electronic\\_commerce/2001Model\\_signatures.html](http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html)>, [Last accessed 5, November 2017].
9. UNCITRAL Model Law on Electronic Transferable Records, 2017, at <[http://www.uncitral.org/uncitral/en/uncitral\\_texts/electronic\\_commerce/2017model.html](http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2017model.html)>, [Last accessed 5, November 2017].

#### b. Domestic Laws

##### i. Primary Legislations

1. Banking Business Proclamation, 2008, Proclamation No. 592/2008, Federal Negarit Gazeta ,14th Year No 57.
2. Banking Business Proclamation, 2008, *Federal Negarit Gazzeta*, Proc. No. 591, 14<sup>th</sup> year No. 57.
3. Civil Code of the Empire of Ethiopia of 1960, Negaret Gazeta, Extraordinary issue, ProclamationNo.165, 19th year No. 2.
4. Commercial Code of the Empire of Ethiopia, 1960, *Negarit Gazzeta*, Extraordinary issue, Proc. No. 166, 19<sup>th</sup> year No. 3.
5. Computer Crime Proclamation, 2016, *Federal Negarit Gazzeta*, Proc. No. 958, 22<sup>th</sup> year No. 83.
6. Constitution of the Federal Democratic Republic of Ethiopia, 1995.
7. FDRE, Constitution of the Federal Democratic Republic of Ethiopia Proclamation No 1/1995, *Federal NegaritGazeta*, Year 1, No 1 Addis Ababa, 21st August 1995.
8. Information Network Security Agency Establishment Regulation, 2006, *Federal Negarit Gazzeta*, Regu. No. 130, 13<sup>th</sup> year No. 5.
9. Information Network Security Agency Re-establishment Proclamation, 2013, *Federal Negarit Gazzeta*, Proc. No. 808, 20<sup>th</sup> year No. 6.
10. Information Network Security Agency Re-establishment Proclamation Execution Council of Ministries Regulation, 2014, *Federal Negarit Gazzeta*, Regu. No. 320, 20<sup>th</sup> year No. 78.
11. Information Network Security Agency Re-establishment Regulation, 2011, *Federal Negarit Gazzeta*, Regu. No. 250, 17<sup>th</sup> year No. 90.
12. National Bank of Ethiopia Establishment (as Amended) Proclamation, 2008, *Federal Negarit Gazzeta*, Proc. No.591, 14th Year No 50.
13. National Payment System Proclamation, 2011, *Federal Negarit Gazzeta*, Proc. No. 718, 17<sup>th</sup> year No. 84.
14. Prevention and Suppression of Money Laundering and Financing of Terrorism Proclamation, 2013, Federal Negarit Gazette, Proc. No.780, 19<sup>th</sup> Year, No. 25.
15. Prevention and Suppression of Money Laundering and the Financing of Terrorism Proclamation, 2009, *Federal Negarit Gazzeta*, Proc. No. 657, 16<sup>th</sup> year No. 1.
16. *Regulation of Mobile and Agent Banking services*, National Bank of Ethiopia, 2012.
17. Telecom Fraud Offence Proclamation, 2012, *Federal Negarit Gazzeta*, Proc. No. 761, 18<sup>th</sup> year No. 61.

18. The National Bank of Ethiopia Establishment (as amended), 2008, *Federal Negarit Gazzeta*, Proc. No. 591, 14<sup>th</sup> year No. 50.

*Transparency in Foreign Currency Allocation and Foreign Exchange Management Directive*, National Bank of Ethiopia, February 10, 2016.

## ii. Secondary Legislations

1. *Regulation of Mobile and Agent Banking Services*, National Bank of Ethiopia, Directive No. FS/01/2012.
2. *Licensing and Supervision of Banking Business Fraud Monitoring*, National Bank of Ethiopia, Directive No. SBB/59/2014.
3. *Clarification for Regulation of Mobile and Agent Banking Services*, National Bank Ethiopia, Circular No. FS/01/2014.
4. *Prohibition of Mobile top up*, National Bank Ethiopia, Circular No. FS/02/2014.
5. *Fraud Monitoring Directive*, National Bank of Ethiopia, 2014.
6. *Draft Electronic Fund Transfer Service Directive*, National Bank of Ethiopia, 2017.

## c. Foreign Laws

1. US Electronic Transfer Act.
2. Bangladeshi Electronic Fund Transfer Regulation.

## IV. Cases

1. Dashen Bank S.C Vs Ato Abebayehu Girma, Meskerem 27, 2006E.C, Case No 96309, FSC Cassation Decision V.7, pp. 248-250.

## V. Dissertation, Thesis and Senior Essays

1. Alebachew B. Enyew, *Regulatory Legal Regime on the Protection of Privacy and Personal Information in Ethiopia*, MS Thesis, University of Oslo, Law Faculty, 2009. <<https://www.duo.uio.no/bitstream/handle/10852/22947/Binder1%5B1%5D.pdf?sequence=1>> [Last accessed November 5, 2017].
2. Away Samuel, *Legal Aspects of Electronic Banking in Kenya*, LLB Thesis, Moi University, School of Law, 2013. <[https://www.academia.edu/14486191/LEGAL\\_ASPECTS\\_OF\\_ELECTRONIC\\_BANKING\\_IN\\_KENYA](https://www.academia.edu/14486191/LEGAL_ASPECTS_OF_ELECTRONIC_BANKING_IN_KENYA)> [Last accessed 5, November 2017].
3. Endale Genene, *Barriers and Benefits of Adopting E-Banking System in Ethiopia*, MS Thesis, St. Mary's University, School of Graduate Studies, 2015, <<http://repository.smuc.edu.et/bitstream/123456789/2231/1/ENDALET%20GENIE.pdf>>, [Last accessed 5, November 2017].

4. Senait Wondafrash Mulgeta, *Regulating E-commerce in Ethiopia: Lessons from the Rules of Ethiopian Commodity Exchange*, LLM Thesis, Addis Ababa University School of Law, 2015, [Available at Addis Ababa university research depository].
5. Fayyad Algudah, *The Liability of Banks in Electronic Fund Transfer Transactions: A study in the British and the United State*, Ph.D. Thesis, University of Edinburgh, 1992.
6. Zakayo Ndobir Lukumay, *An Analysis of the Legal Basis for Electronic Banking in Tanzania*, Phd Dissertation, University of Dar es Salaam, 2011, [Unpublished available at <<http://41.86.178.4/xmlui/bitstream/handle/1/736/Zakayo%20Ndobir%20Lukumay.pdf?sequence=1&isAllowed=y>> [Last accessed March 21, 2018].

## VI. Reports, Policy Documents and Others

### a) Domestic

1. *Monetary Policy Framework of the Federal Republic of Ethiopia*, National Bank of Ethiopia, February 2009.
2. *National Information Security Policy of the Federal Democratic Republic of Ethiopia*, Addis Ababa, September, 2011.
3. *National spatial Information and Technology Policy of the Federal Democratic Republic of Ethiopia*, Addis Ababa, October, 2016.
4. *Critical Mass Cyber Security Requirement Standard Version 1.0*, Federal Democratic Republic of Ethiopia Information Security Agency, Addis Ababa, September, 2009E.C.
5. NBE, Bank Risk Management Guidelines (Revised), May 2010
6. NBE, Annual Report, 2016/17.

### b) International

1. Developing a Comprehensive National Retail Payments Strategy', World Bank Financial Infrastructure Series, October 2012. At <<http://documents.worldbank.org/curated/en/839121469729131991/Developing-a-comprehensive-national-retail-payments-strategy>>. [Last accessed May 18, 2018].
2. ITU-T Focus Group Digital Financial Services: Payment System Oversight and Interoperability.at<[https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKewjS0K2ihfvcAhVMDcAKHStuC1MQFjAAcgQIAxAC&url=https%3A%2F%2Fwww.itu.int%2Fen%2FITU-T%2Ffocusgroups%2Fdfs%2FDocuments%2F10\\_2016%2FITUFGDFS\\_REPORT%2520ON%2520Payment%2520System%2520Oversight%2520and%2520Interoperability.pdf&usg=AQVaw3Bm1A8KKqkTc9VQyoc61Ko](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKewjS0K2ihfvcAhVMDcAKHStuC1MQFjAAcgQIAxAC&url=https%3A%2F%2Fwww.itu.int%2Fen%2FITU-T%2Ffocusgroups%2Fdfs%2FDocuments%2F10_2016%2FITUFGDFS_REPORT%2520ON%2520Payment%2520System%2520Oversight%2520and%2520Interoperability.pdf&usg=AQVaw3Bm1A8KKqkTc9VQyoc61Ko)> . [Last accessed March 25, 2018].

## VII. Internet Sources

1. Online fraud costs global economy many times more than \$100bn at <<https://www.theguardian.com/technology/2013/oct/30/online-fraud-costs-more-than-100-billion-dollars>> [last accessed March 18, 2018]
2. CBE's Core banking project to become operational at <<http://capitalethiopia.com/2012/01/09/cbes-core-banking-project-to-become-operational/#.Wq4dZZdRXWV>> [last accessed March 18, 2018].
3. The Council of Europe Convention on Cyber Crimes, Budapest Conventions 23.11.2001 available at <[http://www.europarl.europa.eu/meetdocs/2014\\_2019/documents/libe/dv/7\\_conv\\_budapest/7\\_conv\\_budapest\\_en.pdf](http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest/7_conv_budapest_en.pdf)> [Last accessed March 25, 2018].
4. Dawit Taye, Reporter Amharic, 8 October 2017, <<https://www.ethiopianreporter.com/article/1801>>, [Last accessed 6 November 2017].
5. EthSwitch, BPC Partner to Create National Switch Infrastructure for Ethiopia', <<https://www.atmmarketplace.com/news/ethswitch-bpc-partner-to-create-national-switch-infrastructure-for-ethiopia/>>. [Last accessed May 12, 2018]
6. 'Mobile Banking', Wikipedia, at <[https://en.wikipedia.org/wiki/Mobile\\_banking](https://en.wikipedia.org/wiki/Mobile_banking)>. [Accesses 20 March 2018].
7. 'Mobile Payment', Wikipedia, at <[https://en.wikipedia.org/wiki/Mobile\\_payment](https://en.wikipedia.org/wiki/Mobile_payment)>. [Accessed 20 march 2018].
8. Biniam, 'CBE Launches Mobile Money Platform', 2018. <<http://www.combanketh.et/More/CBENews.aspx?p=articles&news=86&title=CBE%20launches%20mobile%20money%20platform>> [Last accessed 19 March 2018]
9. Meron Teklebirhan, 'Commercial Bank of Ethiopia Launches E-banking', online, 2Merkato.com. <<http://www.2merkato.com/news/banking-and-finance/1345-commercial-bank-of-ethiopia-launches-e-banking>>
10. Hon. Alan Pendleton, 'Admissibility of Electronic Evidence: A new Evidentiary Frontier', Bench & Bar of Minnesota, 2013. At <<http://mnbenchbar.com/2013/10/admissibility-of-electronic-evidence/>>. [Accessed 21 March 2018]
11. Dawit Endeshaw, 'North Korea-linked hackers target Ethiopian banks', The Reporter English,(8 April 2017), at<<http://www.thereporterethiopia.com/content/north-korea-linked-hackers-target-ethiopian-banks>> [Last accessed April 27, 2018].
12. Alain Martin, 'What is Policy? Strategic and Operational Policies and Good Governance', p.41/110. At <<https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKewjSrJSb0ZPbAhXBRo8KHdK4DSUQFggjMAA&url=http%3A%2F%2Fwww.executive.org%2FBibliography%2FPolicy.pdf&usq=AOvVaw0nWDF8JOiyGHPaBhoYGAKK>> [Last accessed May 20, 2018].
13. The State of Security at <<https://www.tripwire.com/state-of-security/security-data-protection/hackers-steal-60-million-from-taiwanese-bank-using-bespoke-malware/>> [Last accessed March 30, 2018]

## VIII. Interview

1. Focus group discussion with Ato Birhane Gebrecherkos, Ato Berihu Gebru, Ato Endalle Tessema, Ato Bahire Birhane and Ato Anteneh Gebriye, *on the practice and problems of e-banking*, May 12, 2018.

2. Interview with Aster Cheru, POS Expert at Oil-Libya Finfine Branch, *on the problems of the POS banking*, August 06, 2018.
3. Interview with Ato Berihu Gebru, Business support Officer at CBE, *on the practice and problems of e-banking*, May 12, 2018.
4. Interview with Ato Chernet Kebede, E-banking Expert at Awash Bank, *on the practice and problems of e-banking*, May 12, 2018.
5. Interview with Ato Damitew Weldetekle Attorney at CBE, *on the practical legal implementation of the e-banking regulations*, May 13, 2018.
6. Interview with Ato Elias Mitiku, Unit Head of Clearing and Settlement at Premier Switch Solution, *on the national payment system and its interoperability*, August 12, 2018.
7. Interview with Ato Ephirem Baraki, Senior Legal Expert at NBE, *on the regulation of e-banking business in general*, August 09, 2018.
8. Interview with Ato G/hiwot Guesh, ATM banking user, *on the problems of ATM banking*, August 05, 2018.
9. Interview with Ato Kebede Demssie, Banking Examiner at NBE, *on the policy and procedure documents of e-banking*, May 10, 2018.
10. Interview with Ato Mintesinot Seyum, Manager of Mobile and Internet Banking at CBE, *on the practice problems of e-banking*, May 03, 2018.
11. Interview with Ato Natan Lemma, ATM banking user, *on the problems of ATM banking*, August 07, 2018.
12. Interview with Ato Solomon Damitew, Principal Manager Payment Systems Oversight and Development at NBE, *on the national payment system of Ethiopia*, May 04, 2018.
13. Interview with Ato Tebeje Hailu, ATM banking user, *on the problems of ATM banking*, August 07, 2018.
14. Interview with Ato Yonas Berhe, ATM banking user, *on the problems of ATM banking*, August 07, 2018.
15. Interview with Ato Yonas Mekonen, ATM banking user, *on the problems of ATM banking*, August 05, 2018.
16. Interview with Elsabet Alemayoh, Sales Manager at Ethiopian Electronics PLC, *on the problems of the POS banking*, August 06, 2018.
17. Interview with Meseret Fikadu, Front Office Manager at Ethiopia Hotel, *on the problems of the POS banking*, August 06, 2018.
18. Interview with Tiegist Zeleke, Computer Operator at Glorious PVT. LTD, Beherawi Branch, *on the problems of the POS banking*, August 06, 2018.

19. Interview with W/rit Meseret Fikadu, ATM banking user, *on the problems of ATM banking, August 05, 2018.*



**More  
Books!** 



**yes**  
**I want morebooks!**

Buy your books fast and straightforward online - at one of the world's fastest growing online book stores! Environmentally sound due to Print-on-Demand technologies.

Buy your books online at  
**[www.get-morebooks.com](http://www.get-morebooks.com)**

Kaufen Sie Ihre Bücher schnell und unkompliziert online – auf einer der am schnellsten wachsenden Buchhandelsplattformen weltweit!  
Dank Print-On-Demand umwelt- und ressourcenschonend produziert.

Bücher schneller online kaufen  
**[www.morebooks.de](http://www.morebooks.de)**

SIA OmniScriptum Publishing  
Brivibas gatve 197  
LV-103 9 Riga, Latvia  
Telefax: +371 68620455

[info@omniscryptum.com](mailto:info@omniscryptum.com)  
[www.omniscryptum.com](http://www.omniscryptum.com)

OMNIscriptum 





