CONSUMER PROTECTION in ELECTRONIC PAYMENT SYSTEM in ETHIOPIA

By: BehailuTewabe

ADDIS ABABA UNIVERSITY

COLLEGE OF LAW AND GOVERNANCE STUDIES

MASTERS OF LAWS (LL.M) PROGRAM IN BUSINESS LAW

Advisor: - Solomon Abay (PhD.)

September, 2024

Approval Sheet by the board of Examiners

Consumer Protection in Electronic payment System in Ethiopia

I hereby certify that this is my original work. Works of others included in this thesis are properly cited.

Behailu Tewabe Tsegaye / ID Number GSE/2421/12 ----------

A thesis submitted in partial fulfillment for the award of Masters of laws (LL.M) at the College of Law and Governance studies, Addis Ababa University

Advisor

Solomon Abay (PhD)----------

Examiners Signature

Name

1. ---------- 1.----------

2 ---------- 2. ----------

Contents

Acronyms

CBE- Commercial Bank of Ethiopia

EP- Electronic payment

EPS- Electronic Payment system

NBE- National Bank of Ethiopia

NPDS- National Payment Digital Strategy

NPS- National Payment System

NPSP- National Payment System Proclamation

MOTRI- Ministry of Trade and Regional Integration

OECD-Organization for economic co-operation and development

PI- Payment Instrument

PII- Payment Instrument Issuer

PSPS-payment service providers

UN- united nation

Acknowledgment

First and foremost, I would like to thank the almighty God and St Mary for the guidance in every step of my life including this one.

Second I would like to extend my deepest gratitude to my advisor Dr Solomon Abay for your constructive advice. Next I would like to thank my families and my beloved wife Helen Aklilu who always supports me in every step of my journey.

Last but not least I am also indebted to thank my friends Getahun G/meskel and Birhanu Tassew for their support and cooperation.

Abstract

The advancement of technologies nowadays affects an overall economy of the world. Financial sectors also affected by these technologies. Ethiopia lately introduced a reform in its payment system laws. This helps in modernizing payment and enhancing financial inclusion.

However due to its unique feature this electronic payment systems also pose a treat for customers. Thus there is a need to adjust general consumer protection laws to this effect. The NBE in this regard is the main regulatory body in Ethiopia to issue consumer protection laws. However these regulatory schemes are found in different legislations. Ethiopia therefore in this regard does not have a consolidated consumer protection legal frame work. These scattered laws also seem to lack clarity in safeguarding the interests of consumers.

Furthermore the consumer protection legal frame work seems inadequate when we compare it to the international good practices. In addition there is a need for a coordinate effort of different regulatory organs in order to strengthen consumer protection.

This paper, among other things, recommends that there is a need to develop the regulatory capacity of different regulatory organs and additional legal frameworks should also be incorporate in order to protect consumers.

CHAPTER ONE

1.1 Back ground of the study

The use of technology in financial products and services is resulting in a wide array of new approaches to financial sectors. The internet, mobile devices, big data and other technologies are impacting the way we borrow, make payments and manage our money.[1]

The proliferation of the internet led to the birth of electronic commerce, a business environment that allows the transfer of electronic payments as well as transactional information via the internet. Electronic commerce now a day's become an integral part of everyday life. Thus electronic payment system (here in after EPS) recently becomes one of the disruptive changes to payments business model.[2]

Business and financial activities require secure deposits and withdrawal of money to and from bank accounts, secure data, application programs and data bases, secure transactions and payments, secure communication networks and network management.[3] Among these, the security in business transactions and payments is of utmost concern for companies and consumers.

[1] Lauren saunders, **Fintech and consumer protection**, National consumer Law center, March 2019, P.2

[2] Amitabh Saxena, Electronic payment system,2011, p. 2

[3]Zon-yau lee, Hsiao-chengyu, pej-jenkuo, **Analysis and comparison of different Types of electronic payment systems** , institution of management of technology, Chiao-Tung University, Taiwan, p. 38

As EPS comprise banking and telecommunication activities, different perspectives exists on the appropriate regulatory frame work as well as which authority should regulate it.[4]

The creation of a united body of law for payment systems has so far been unsuccessful in most developing countries.[5]In part, the failure is due to the assumption that the existing law works well for the traditional paper based check systems and problems have been created only by the evolution of new technologies. On the other hand, there is unfortunately and perhaps understandably a limit to the ability of the law to adopt itself to emerging technologies: timely legislative intervention to supplement the existing law and to fill in the existing lacunae is often needed to ensure that the law remains current and relevant.[6]

Thus, the governments to enhance the benefits from this EPS need to make complementary adjustments to domestic banking and financial regulations by offering specific regulations to it. In so doing, certain questions should be asked in establishing a strong consumer protection regime as the EPS has brought forth new entrants and various stake holders.

Here it is important to note the fact that EPS is mainly about ensuring a fair exchange between providers and consumers of financial services. This understanding is crucial for the reason that there is a need to maintain a delicate balance of protecting the interest of the providers of these financial services while at the same time ensure protection of consumers from the excesses and misconduct of financial institutions which take advantage of the regulatory gaps that make consumers susceptible.[7]

This research paper is a review of Ethiopian EPS with a specific focus on consumer protection. The research aims to discuss the risks to consumers due to a lack of an established regulatory frame work for electronic payment. It will do so by first identifying the different players in electronic payment chain, then presenting the existing legal and institutional frame work through

[4] Joy Malala , **consumer protection for mobile payments in Kenya**, An examination of the fragmented legislation and complexities it presents for mobile payments , KBA center for research on financial markets and policy working paper series, Kenyan Bankers association, 2013, p. 1

[5] Ibid, p. 9

[6] ibid

[7]Lempere Solomon, **Consumer protection in the Kenyan financial sector: A case for a twin peaks model of financial regulation, thesis,** university of the western cape, August 2019, p.12

which these players are currently operating. It will then discuss the gaps that have been left by the current regulatory frame work where consumer protection issues have not been adequately addressed.

1.2 preliminary review literatures

As will be discussed below, even if it is not as such many, some authors tries to address about the legal and institutional problems related with the regulation of electronic banking system in Ethiopia.

Bikila Ababu in this regard argue that the adequacy of the mobile and agent banking service directive to regulate all electronic banking service platform is not practically tested in Ethiopia and all e-banking delivery platforms do not present similar regulatory issue and concerns.[8] Hence he suggests that the regulatory frame work needs to be reformed to accommodate the new developments in the e-banking sectors and to address the regulatory issues and concerns different e-banking delivery channels pose and harness the opportunities the e-banking sector presents to the consumers, the banking organizations and the economy as a whole.[9] However, his paper does not concentrate on consumer protection rather it focuses on the regulation of electronic banking.

Simret Zewdie has written in 2013 on electronic funds transfer and the case for consumer protection in Ethiopia. He points out that legislative regulation of electronic funds transfer in Ethiopia in the context of consumer protection is characterized by scattered rules which do not sufficiently address the issues at hand. In addition, the rights of consumers that arise from these scattered rules are uncertain and in most cases applicable by way of interpretation by courts.[10]

He, therefore, suggests that new systems that are not only beneficial to the concerned parties (consumers and banks) but also to the overall economy must be supported by strong legislative and regulatory measures.[11]There is however no focus on addressing the solutions how to limit

[8]BikilaAbabu**, Regulation of electronic banking in Ethiopia, The analysis of legal frame work**, Thesis, Addis Ababa University, June 2019, P. 62

[9] Ibid

[10]Simret Zewdie**, Electronic Funds transfer and the case for consumer protection in Ethiopia** , University of Oslo, August 6,2013, p. 45

[11] ibid

those problems relate with consumer protection and does not have any recommendation on how regulatory and institutional challenges in connection with consumer protection can be solved.

Ashenafi Lemecha Moti in 2017 has written on consumers and third parties protection under the national payment system proclamation No. 718/2011. He argues that besides having contractual rules there is a need to have some minimum standards in order to protect consumers who uses electronic payment product. [12] He basically focuses on the national payment system proclamation and argues that the proclamation has not prescribed terms and conditions which should be mandatorily disclosed to consumers. He also questions the legality of the contract which does not provide the terms and conditions of ATM and mobile banking. In addition he addresses and makes recommendation about dispute settlement mechanisms and rules of evidence in connection with consumer protection of electronic payment system enshrined under the National payment system. However, he only concentrate from the perspective of national payment system proclamation and does not address whether the proclamation stipulates adequate legal protection for consumers in light of international consumer protection standards. However this proclamation is amended recently[13]. Moreover, there is a recent development in enacting additional laws after the writer publishes his paper in 2017. This includes Financial Consumer Protection Directive No.FCP/01/2020, payment instrument issuer directive No.ONPS /01/2020, and its amendment Directive No. ONPS /06/2022. National bank of Ethiopia also issued a new national digital strategy (2021-2024) in which it aims to create a digital Ethiopia by 2025.[14]

This study is therefore distinct in the sense that it is a specific review of consumer protection from the perspective of EPS with its recent development and tries also to incorporate the international standards of consumer protection in light of electronic payment system and practices in Kenya and Tanzania.

[12]Ashenafi Lemecha Moti , **Consumers and third parties protection under the national payment system proclamation No. 718/2011**, thesis , Addis Ababa University, February 2017, p.65

[13]National payment system (amendment) proclamation No.1282/2022,Negarit Gazeta Communication service proclamation No. 1148/2019, **NEGARIT GAZETA**, 25 year. No.82

[14] National digital strategy(2021-2024),p.1

1.3 Statement of the problem

The development of innovative and easy to use electronic payment systems by financial institutions and other businesses (including mobile operators) has helped to support rapid growth in e-commerce in large and small businesses by providing consumers with more effective, convenient and secure ways to purchase and expanding variety of goods and services.[15]

The development of mobile and online payment systems has brought numerous benefits to consumers. On the contrary there are a number of areas identified where these systems could be strengthened to better address consumer interest. Here consumers generally need to know more about their rights and obligations when they make such payments, especially when a number of parties (such as mobile operators, internet service providers and social media) are involved in a transaction. [16]

Furthermore, the situation is complicated as payment systems may be subject to different regulatory schemes, which may have important implications with respect to the level of consumer's protection afforded. Consumers may, in this context, have difficulty in determining what their rights are and how these may vary depending on factors, such as 1) payment mechanisms used 2) the device being used. Determining which parties are responsible for addressing any problems that arise, the procedures for seeking redress, and the types of remedies that may be obtained, can also be problematic for consumers.

Electronic payment system is a recent phenomenon in Ethiopia. The national bank of Ethiopia has the mandate to regulate financial sectors and also empowered to enact different legislations in connection with consumer protection. But unlike conventional financial regulations, EPS and its regulation of consumer protection has its own unique character. Thus, Ethiopia needs a comprehensive legal framework in order to protect consumers. The legal and institutional frame work of Ethiopia should also meet the minimum standards set by international guidance principles on consumer protection of EPS. As a result, this study is distinct in the sense that it is a specific review of the regulatory schemes and institutional frameworks of Ethiopia in relation

[15] OECD, **Consumers policy guidance on mobile and online payments**, OECD digital economy papers, No.236, p.4

[16] ibid

with consumer protection of EPS and addresses those legal gaps with the recent development of technology.

1.4 Research questions

This research work seeks to answer the following three questions:

- What are the regulatory challenges and problems of protecting consumers of electronic payment systems in Ethiopia?
- What are the legal and institutional problems of electronic payment system in Ethiopia?

1.5 Objective of the study

The general objective of this study is to determine the viability of the Ethiopian legal, institutional and regulatory framework in regard of consumer protection with particular emphasis to EPS.

It also has the following specific objectives

- To assess the strength and weaknesses of the current legal and regulatory schemes in addition to institutional frame work.
- To determine if regulatory, institutional and legal reform is necessary in order to further modernize it.
- Evaluates the practice of consumer protection in connection with electronic payment system.

1.6 Significance of the study

The significance of this research can be seen from the perspective of further strengthening the legal, regulatory and institutional frame work of Ethiopian consumer protection on EPS. Furthermore, by showing the practical problems and the inadequacy of Ethiopian legal system governing the topic it will facilitate Ethiopia to take further action in enacting the latest international standards on consumer protection of EPS.

1.7 Scope of the study

The thesis examines the adequacy of the current legal regime of consumer protection with particular emphasis of the use of EPS. In order to do so the writer basically used OECD principles of customer protection on mobile and online payment system, UN Guidelines for consumer protection and the practice of African countries to evaluate the adequacy of Ethiopian legal regime. The selection is made by taking into consideration the members of OECD are developed countries who contributed 80% of the world trade and investment. In addition as most of the members of OECD are European countries they have a better technological advancement in the area. The researcher also takes the UN guideline as Ethiopia is also a member of this institution.

1.8 Limitation of the study

The research has the following limitations. One of the limitations the writer encountered is the scarcity of available materials from domestic legal sources. Since the area of the research is a recent development in Ethiopia, the writer had to rely on relevant foreign sources. The second limitation is due to time constraint the writer had to heavily rely on internet and articles of journal.

1.9 Research Methodology

The researcher used qualitative method to meet the objective of the study. The techniques employed are: data obtained through semi-structured interviews from national bank of Ethiopia and telecom authorities and academicians in the legal discipline. Review of documents and laws, both foreign (including international principles) and domestic, as the case may be, was employed.

The research is a synthesis of both primary and secondary sources. Data collected through interview and review of the domestic laws, international standard principles and policy documents of Ethiopian Government make up the primary sources. Previous works on this topic in the form of journal articles, textbooks and Internet based literature are used as secondary sources.

1.10 Organization of the Study

This paper has a total of four chapters. Chapter one consists of the introduction of the research that gives its background , statement of the problem, research objectives and questions , significance of the study, methodology adopted, a preliminary review of the literature, scope and limitation of the study. The second chapter starts with defining consumer and deals about the different types of EPS and the rationale, benefits and challenges of having consumer protection law for electronic payment system, it then discuss about international standards for consumer protection of EPS and African best practices. It also addresses the legal and regulatory challenges encountered by consumer protection schemes in the area of EPS. The third chapter examines consumer protection of EPS in Ethiopia. In doing so it makes an assessment about the different types of EPS employed in Ethiopia. It then discusses about the regulation of EPS with special emphasis of consumer protection and examines the institutional framework set by the government in order to protect consumers in using EPS. It also evaluates the different legislations enacted by the government in order to achieve consumer protection of EPS and problems associated with Ethiopian consumer protection of EPS. Finally chapter four concludes the research paper by drawing conclusion and making recommendation.

Chapter Two

Regulation of Electronic Payment System and Consumer Protection: A General Discussion

2.1 Introduction

The major force behind the changes occurring globally is thought to be information technology. With growing knowledge of computer and internet use over the past few years, electronic transactions, particularly e-commerce, have become a buzzword for businesses.[17]

In this case, electronic payment systems are regarded as the foundation of e-commerce and among its most important elements. EPS can be defined as a payment service that utilizes the information and communication technologies.[18]With the development of technology, EPS has taken on several forms, including as digital wallets, smart cards, debit cards, electronic cash and check systems, and credit cards.[19]

Since money and goods are transmitted without direct contact between the parties engaged in the transaction, the primary concern with electronic payment is the level of security at each stage of the transaction.[20]If even the slightest possibility exists EPS may be insecure, consumers', Merchants' and bankers' confidence in this system might erode and consequently, destroy the foundation of electronic commerce.[21]

Therefore, the electronic transfer of value, or EPS, is dependent upon a secure ICT infrastructure, an effective legal and regulatory framework, and widespread public and business understanding.

This chapter covers the benefits of EPS as well as challenges that users may have when utilizing it due to unresolved legal and regulatory issues. Furthermore, it will critically evaluate global norms for the protection of consumers' of EPS including the experience of developing countries.

---

[17]Gardachew work, **Electronic-Banking in Ethiopia practices, Opportunities and challenges**, Journal of internet and commerce, August 2010, Vol. 15. No.2.p. 1 (http://www.auvaydev.com/commerce/jibc)

[18]Zlatko Bezhovski**, the future of the mobile payment as electronic payment system**, European Journal of Business and management , Vol.8, 2016, P.127

[19] ibid

[20] Supra note 3. P.38

[21] Ibid

2.2 Rationale for consumer's protection of EPS

In the legal literature, consumer's protection is generally explained and justified, by the concept of the "weaker party".[22]It is claimed that because they have less bargaining power than professionals and contracting partners, consumers are "weaker" and hence unable to defend their interests.

In recent times consumers are now seen as economically vulnerable and in need of protection as it is believed that they are less knowledgeable about contracts and products than experts are.[23]

The protection of consumers can lessen information asymmetry and guarantee that the interests of financial service end users are upheld. It can also contribute to improve efficiency, transparency, competition, and access to retail financial markets.[24]

Consumer protection essentially entails: protecting the consumers from fraud or exploitation by providers with significant market power, ensure minimum disclosure and quality standards for clients, support confidence in the financial system.[25]

2.3 Benefits and challenges of EPS

EPS has its own benefits and challenges. In summary the benefits includes

- More relevance, which boosts consumer and merchant satisfaction: enabling a client to transfer funds to another, irrespective of the recipient's platform [26]
- Offer consumers several benefits, such as location fee access, an extensive selection of options for purchases, a simple substitute for cash payments, and prompt contracting with their financial resources.[27]
- Faster, safer, more affordable, and more convenient transactions[28]

[22] Supra note 4, p.22

[23] ibid

[24] ibid

[25] ibid

[26] Supra note 2, p.7

[27] Supra note 17, p. 129

- By using digital interfaces, financial service providers and consumers can have more options for productive contact.[29]

EPS also presents some challenges which differ from offline commercial transaction. Such challenges include

- Vulnerable to hacking which provide access to the victims personal and financial information [30]
- Emerging risks also entail the use of this payment mode in terrorist funding and money laundering while traditional risks involve the theft of data and services , loss of revenue , customer base and brand reputation[31]
- Consumers have less bargaining position when there is a dispute which arises from electronic device interactions.[32]
- There is no specific regulatory framework concurrently engaging the main partakers in the provision of EPS, i.e. the bank, the network provider and electronic device manufacturer.[33]
- Electronic payment technical platforms are not properly standardized or regulated. This is due to lack of universal and cohesive mode of payment.[34]
- Lack of interoperability between various electronic payment interfaces has also raised concerns over privacy and security when confidential details are shared through fragmented version of electronic payment platforms.[35]

---

[28] Supra note 21, p. 10

[29] ibid

[30]Amanjain,Challenges online payments are facing and how to solve them, accessed at, https://finance.yahoo.com/news/challenges-online-payments-facing-solve-152910966.html, October 7,2021, p.1

[31] Supra note 17, p.130

[32] Supra note 1, p.4

[33] Robin Simpson, Mobile payments and consumer protection, accessed at march 2022,https://www.consumersinternational.org/media/1845/mobile-payments-and-consumer-protection.pdf, January 2014,consumer international, p.6

[34] ibid

[35] ibid

2.4 Standards for consumer protection of electronic payment system

There is a need for comprehensive financial consumer protection, particularly data protection, given the new and developing risks in our increasingly digital environment. The digital environment should be taken into consideration while developing and implementing financial consumer protection laws and procedures by regulatory organizations and policy makers.

Concerns about electronic payments and consumer protection include: 1) information on the terms, conditions and costs of transaction 2) privacy 3) security 4) confirmation process 5) varying levels of protection among payment providers and payment vehicle 6) fraudulent, misleading, deception and other unfair commercial practices 7) dispute resolution and redress.[36]

2.4.1Information on the terms, conditions and costs of transaction

Consumers may not always find it simple to get, read, maintain, and keep the terms and conditions of transactions, as well as the associated payment data and procedures. Due to mobile devices' small screens, limited computing power, and short battery life, disclosure issues may get worse in the context of mobile payments.[37]

Furthermore, mobile device-based transactions and associated payments are frequently completed in a "on the go" environment where customers make snap judgments about what to buy while transit. Customers' capacity to sufficiently access and/or review the terms of payment before making a payment may be restricted in such a situation.[38]Important information about payments is occasionally also provided in the form of footnotes or involves opening a number of additional windows.[39]

[36] OECD, **report on consumer protection in online and mobile payments** , OECD digital economy papers No 204 , p.34

[37] ibid

[38] Supra note 15, p.6

[39] ibid

Therefore, terms, conditions, and payment options should be included in the information in order to address such issues. Furthermore mobile and online payments may not always be easy for consumers to access and read. So, key payment and related transaction information should be provided to consumers early in a transaction process in a clear, conspicuous and easily accessible manner.

2.4.2 Privacy

The mobile and online payment environment raised a number of challenges with privacy implications. Due to the convergence of the industries, consumer protection policies are not specific to the needs of mobile payment. Regulators have been confronted with the question of how to regulate in such a manner that balances consumer rights to privacy with the objective of law enforcement officials who wish to combat money laundering. [40]

Transactions and personal data are transmitted through mobile phone networks, handled more often by third parties such as agents and accessed remotely by consumers and financial institution employees, here the risk of in appropriate access and usage rises.[41]

In this context, simple and transparent mechanisms are needed through which users can authorize an entity to access this kind of information. In addition the law should answer and define who can get access to a mobile money trail and how, when or under what conditions such access may be obtained. This will help to keep consumer information private and the regulators to keep consumer funds safe against financial crimes.[42]

Design and enforcement of data privacy and security rules also require some level of coordination between supervisory and regulatory authorities, as mobile payment cut across different sectors such as banking and telecommunications.[43]

[40] Supra note 4, p.34

[41] ibid

[42] ibid

[43] Ibid, p.35

2.4.3 Security

Besides the technological aspect, consumers' lack of education and experience with formal financial services and technology may raise data security risks.[44]According to EU General Data Protection Regulation (GDPR) its application is determined by notions of "processing "and "personal data ". This regulation imposes a duty on the controller to implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with regulations.[45]

The EU regulation also imposes duties to ensure a level of security appropriate with the risk associated with the processing such as unlawful access to personal data. Here the controller can signify compliance by virtue of adoption of internal policies and implementation of measures which meet the principle of data protection.[46]

Like Other financial services, mobile money raises the issue of security. Data in mobile money transaction may include payer and payee's ID, geographic location, time of day, purchased items, and the value of the transaction. Mobile money providers should have internal controls to minimize unauthorized access to consumer information, as well as the loss of consumer data.[47] In addition Regulators and mobile money providers need to work together to understand security concerns and maintain the integrity of consumer data.

2.4.4 Confirmation process

The 2008 guidance on mobile commerce notes the difficulties that consumers may sometimes have in fully accessing contractual information prior to making a decision. Consumers purchasing products via e-commerce may not realize when they are confirming a transaction.[48]

[44] Supra note 4, p34

[45] Henry Ndejapo, **Consumer protection in online payment methods**, thesis, University of Pretoria , October 2019, p.45

[46] ibid

[47] Ibid, p.36

[48] Supra note 14, p.13

Consumers using mobile devices to make "on the go" purchase through mobile applications ("apps") might not realize that by simply clicking on an icon, they have agreed to a purchase and that payment is due. As a result, consumers might end up being billed for products that they did not intend to buy. Consumers may also inadvertently supply wrong payment information and May, without their knowledge, wind up having their transaction cancelled or rejected.[49]

In order to know when a transaction has been concluded and that payment is due, consumers in electronic payment system should be[50]

1. Provided with an opportunity to confirm their payment information, or cancel an entire transaction, prior to concluding it.
2. Clearly notified when a transaction for which payment information has been provided, is not fully processed.

2.4.5 Varying levels of protection among payment providers and payment vehicle

In most OECD countries, consumers enjoy strong legal protection, as well as supplementary payment-related protection provided by financial intermediaries, when payments are made using payment cards. They may also enjoy some legal protection for bank debits. Such protection applies regardless of the device being use to make payments. [51]

The protections cover problems relating to unauthorized charges which may result from processing errors or from fraudulent transactions where a payment card is lost or stolen. It may also include problems relating to product conformity or delivery.[52] In a number of OECD countries, there is little or no statutory protection associated with the use of stored value money in prepaid and gift cards, or payments made via mobile phone bills.[53]

[49] ibid

[50] Ibid , p.14

[51] Ibid

[52] ibid

[53] Ibid, p.16

Thus the OECD consumer policy guidance recommends that consumers should adequately be informed about their rights and obligation in payment transaction. In addition governments and payment providers should work together to develop minimum standards of consumer protection for mobile and online payments transactions, regardless of the payment mechanisms used. [54]

2.4.6 Fraudulent, misleading, deceptive and other unfair commercial practice

The 2003 OECD cross-border fraud guidelines encourage governments to put frameworks in place that would help limit, prevent and deter fraudulent and deceptive commercial practices involving business and individuals.[55]

In addition governments are called to develop mechanisms for co-operation and information sharing between and among their own consumer protection enforcement agencies and their other law enforcement authorities for the purpose of combating fraudulent and deceptive commercial practices.

The 2007 guidance on electronic authentication provides that by providing a level of assurance regarding the identity claimed by parties engaged in an online relationship, authentication reduces uncertainty inherent in transactions at a distance. However, these remain areas of concern for consumers. [56]

In some instances , information provided to consumers on prices and other related issues is misleading, inconsistent or contradictory thus, the OECD consumer policy guidance on mobile and online payment recommend that businesses that provide information on price and other payment related issues should be consistent throughout the payment transaction.[57]

Consumers are sometimes charged for products that they thought were free, did not authorize or did not knowingly purchase. In order to protect consumers from such kind of unexpected additional charges consumers should be provided with information on the steps to be taken to discontinue purchasing the good and services when products are provided to consumers on

[54] Ibid, p.17

[55] Supra note 14, p.17

[56] Ibid, p.18

[57] ibid

favorable terms for a limited period of time .In addition consumers consent should be obtained for continuing a commercial relationship beyond a trial period, before consumers pay or incur any additional financial charges.[58]

Unauthorized purchases and charges, often through identity theft, continue to be a significant problem for consumers in the case of commercial transaction that are not proximity based. In order to help consumers to strengthen confidence in such kind of commercial transaction, the OECD consumer policy guidance on mobile and online payment provide payment providers, Businesses and other stakeholders to work together to develop effective practices and regulatory tools to help prevent payment fraud . In addition the aforementioned stake holders expected to develop tools that help consumers detect and protect themselves against deceptive, misleading and fraudulent practices.[59]

2.4.7Dispute resolution and redress

Electronic payment system channels are often seen as cumbersome for most mobile payment users and are not effective in dealing with the difficulties often experienced by mobile payment users. In order to solve those problems which emanate from electronic payment system, financial consumer protection redress mechanism should be accessible, affordable, independent, fair, accountable, timely and efficient.[60] In addition the redress mechanism should set in place complaints policy and procedures, alternative dispute resolutions or external recourse and timeframe provided for dispute resolution.[61]

When problems regarding the payment itself arise, consumers need to know who to contact in order to solve issues in a cost effective manner. One of the challenges is to design processes which are viable when low value products are involved. Another is to have mechanisms in place to deal effectively with transactions involving cross-border trade.[62]

[58] Ibid , p.19

[59] Supra note 14, p.21

[60]Supra note 12, p.32

[61] ibid

[62] ibid

In resolving online shopping disputes traditional mechanisms such as litigation can be time consuming and expensive for consumers. Thus, interest has grown in designing efficient mechanisms which involve online dispute resolution (ODR) schemes. This scheme uses online technologies to facilitate the resolution of disputes between parties. While recognizing the benefits of ODR may bring to consumers, there are also challenges in applying these schemes which includes lack of direct interpersonal contact that may limit consumer ability to explain their problem to a merchant.[63]

In addition the OECD consumer guidance on mobile and online payments stipulates that governments, payment providers, platform operators and other stake holders should work together to clarify the options that are available to consumers to address payment related disputes. There should also be clear information about which party should be contacted to address payment related problems and how that party should be contacted.[64]

The cost, time and effort required to resolve such disputes could discourage consumers from seeking redress, especially for low value transaction. Thus, there is a need for the development of effective online dispute resolution system which facilitates resolving claims over payments involving low value transactions.[65]

2.5 United Nations guidelines for consumer protection

The united nation General assembly in resolution No. 70/186 set a guideline for effective consumer's protection.[66] Furthermore the guideline assists to promote international enforcement cooperation between member states with respect to consumer protection. The main objective of the guideline includes assisting countries in achieving or maintaining adequate consumer protection, to curb abusive business practices, to have high level of ethical conduct for those who engage in production and distribution of goods and services to consumers.[67]

[63] Ibid, p.27

[64] Supra note 14, p.22

[65] ibid

[66] UNCTAD ,**United Nations Guidelines for consumer protection**, https://unctad.org/system/files/official-document/ditccplpmisc2016d1_en.pdf, accessed UNITED NATIONS, New York and Geneva, 2016

[67] Ibid, p.6

The scope of the guideline application limited the term consumer to refer only natural persons acting primarily for personal, family or house hold purposes. The guideline basically states that in order to have a good business practices in both online and offline commercial activities with consumers the following basic principles should be followed.[68]

A). A fair and equitable treatment of consumers should be made by business practices.

B). Businesses should follow the principle of disclosure and transparency. Here businesses obliged to provide accurate and not misleading information regarding the goods and services, terms and conditions of the transaction. There must be also an easy access to this information regardless of the means of technology.

C). consumers should not be subject to illegal, unethical, discriminatory or deceptive practices.

D).The other principle is businesses should develop mechanisms and programs in order to assist consumers. These mechanisms help consumers to understand the risks they take in the transaction.

E).The privacy of consumers should also be protected by businesses. In this regard a combination of appropriate control, transparency and consent mechanisms in collection and use of consumer's personal data is needed.

F).Finally there must be also a complaint handling and dispute resolution mechanisms with unnecessary cost or burden to consumers. These mechanisms should also include fair, transparent, speedy and effective mechanisms of dispute resolution.

The guideline also applies to imports and home produced goods and services. These procedures on the other hand in protecting the rights of consumers should not become barriers to international trade.[69]

[68]Ibid, p.7

[69] Ibid, p.10

2.6. Experience of Kenya and Tanzania

In Kenya 40% of the adult population uses mobile money. In 2013, 40% of Kenya's GDP flowed through Mobile money.[70] The service basically includes money deposit and withdrawal, remittance delivery, bill payment, and microcredit provision.[71]

The central bank of Kenya regulates and inspects the mobile payment operators in its functionality. The central bank also allows bank and mobile operators to offer the cross border mobile money services.

The Kenya National payment Act No.34 of 2011 embrace consumer protection services of disclosure mechanisms, redress to consumers complaints , transparent terms and conditions for services and must ensure privacy and confidentiality of consumer data.[72]

In Tanzania also 43% of the population actively uses the mobile money service.[73]These result emerged from a conducive regulatory environment. Tanzania used the 'test and learn' approach which focused on the development of the service and monitor its development.[74]In 2007 Tanzania issued guidelines for electronic payment schemes.

Tanzania also introduces cross-Border mobile transfer. In this circumstance the law requires a licensed payment provider to open and maintain a trust account.[75]Tanzania enacted a National Payment system act No.4 of 2015 to make provision for regulation and supervisions of payment system, payment instrument and payment service provider.

The Act also provides consumers protection provisions which include complain handling and dispute resolution mechanisms, terms and conditions that are transparent, fair, and legible in comprehensive language. The legal and regulatory challenges still exist in Tanzania despite the enactment of legal frameworks to govern mobile transaction.

[70] Masanja martine Ramadhan, Harmonization of consumer protection laws in mobile money transaction across East Africa community. A comparative study of Kenya and Tanzania, thesis,2019, P.23
[71] ibid
[72] Ibid, p.56
[73] Ibid, p.31
[74] ibid
[75] Ibid, p.46

However in both Kenya and Tanzania the insufficient regulation of cross-border mobile transactions has resulted to cyber crime and fraud.[76] In addition the multiplicity of the complaint settlement bodies which includes money issuers, Banks and fair competition commission fail consumers to get redress. Here there is no combination of complaint handling mechanism which poses as a challenge to consumers.

In addition the National payment System laws of both Tanzania and Kenya provide for measures against cyber attacks and illegal entry to the data of consumers.[77] But still many consumers are complaining which shows that the laws in place are not sufficient in protecting mobile transactions.

In case if mobile phone is stolen and used by fraudsters who are able to figure out the user PIN, the consumers should report as soon as possible so that the mobile money transaction can be blocked. However the research in Kenya showed that the law does not provide effective and convenient means for consumers to notify the loss, misuse, theft or breach of security code.[78]

Therefore, researches in Kenya and Tanzania suggested that the legal and regulatory framework needs to be strengthened in order to increase the confidence of consumers and ensure safe and sound national payment system.

2.7. Legal and regulatory challenges of consumer protection in electronic payment system

Introduction

The rationale of regulating financial market basically emerges from the risk of market failure.[79] When a bank fails to meet its obligation to depositors or other creditors, it can cause problems for the wider economy.[80]The main objective of financial regulation includes ensuring financial stability, soundness and protecting consumers and supervising market conduct.[81]

[76] Ibid, p.58
[77] Ibid, p.59
[78] Ibid, p.61
[79] Supra note 8, p.32

[80]Asena Degirmenci, **what is financial regulation and why it is important**? , accessed at February 2022 https://www.leasinglife.com/news/industry-news/what-is-financial-regulation/, May 10, 2019, p.1

[81] Supra note 7, p.20

There are two facets of financial regulation: prudential regulation and consumer protection.[82]Prudential regulation focuses on ensuring that firms have the funding necessary to trade safely and have the appropriate risk control in place and are properly governed while consumer protection focuses on enduring that firms treat consumers fairly from sales process to how complaints are managed.[83]

One of the basic challenges of regulators in financial market related with electronic payment systems. There are three types of consumer's challenges for policy makers and other stake holder in online and mobile payment markets[84]. The first challenge relates to regulatory framework, which involve both legal rules and their relationships to private sector measures. Here both financial and non financial institutions involve in e-commerce payment transaction with consumers. The rules governing their operations, which cover telecommunications, competition, and financial services regulation as well as consumer protection may differ.

The second set of challenges includes general consumer issues, such as unauthorized payment charges, non delivery, late delivery and non conformity of products, as well as dispute resolution and redress.

The third set of challenges concerns technical payment issues that are related to transactions. These include security related issues, such as digital identity management.

The future of a specific electronic payment system depends upon how it overcomes the practical and analytical challenges faced by various means of online payments. These challenges include issues of law and regulation. This topic will highlight some of the basic legal and regulatory challenges consumers encountered in using electronic payment system.

2.7.1. Legal challenges

Consumers, merchants and other parties who involves in transaction may not fully understand what legal and /or involuntary framework applies to a particular transaction, what responsibilities

[82] ibid

[83] ibid

[84] Supra note 39, p.16

are in case of fraud or security problems, or what types of dispute resolution mechanisms or redress rights may be available to consumers in the event of the problems.[85]

There are a number of parties involved in the process when consumers make mobile payment for transaction. Here consumers may have difficulties in determining their rights especially in the payment mechanism and on the device being used.

It is also not easy to determine the party responsible for addressing the problems that can arise in the transaction process, the procedures for seeking redress and the type of remedies that can be obtained.[86]

Due to a rapid change of technology which has given rise to unforeseen new products and services the laws that govern consumer protection today may cause problems when new technologies become available.[87]Thus, there is a need to undertake necessary adjustments and amendments to balance the benefits from the developments and the risks it poses.

The World Bank Good Practices for financial consumer protection recommends that the law provides clear consumer protection rules regarding financial products and services. There are two sets of legislation governing financial consumer protection. The first one contains provisions on consumer protection covering the operations of financial service providers and their clients. On the other hand, the second one focuses on consumer protection and fair competition legislation which defines the rights of consumers of various goods and services.[88]

A number of countries recently added new legal acts dealing specifically with consumer protection with in financial services in a comprehensive manner. [89]

---

[85] ibid

[86] European parliament, **consumers protection aspect of mobile payment**, accessed at February 2022, https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/564354/EPRS_BRI(2015)564354_EN.pdf, June 2015, p.4

[87] Supra note 4, p.20

[88] World bank, **Global survey on Consumer Protection and Financial Literacy ; Oversight framework and practices in 114 Economies**, 2014, accessed at November 2022 , https://documents.worldbank.org/en/publication/documents-reports/documentdetail/815911468154453508/results-brief-regulatory-practices-in-114-economies, p.6

[89] ibid

2.7.2 Regulatory challenge

The regulatory environment governing electronic payments is continuously evolving. Various regulatory instruments aimed to harmonize, secure and enhance consumer trust in online payments have been developed in recent years.

There are questions as to whether the new electronic payment schemes are covered by the legal and regulatory regimes applicable to traditional payment systems. [90]Thus, there is a need for a major review to determine how existing rules which applies to traditional payment system should be adopted to the new payment system or how new rules developed to tackle emerging issues.[91]

Some countries like South Korea have specific legislation that applies to electronic payment system while others apply to general consumer protection, telecommunication or financial regulation.[92]

The need and level of consumer protection in electronic payment system may vary from country to country depending on the payment organization involved (bank and non bank organization), the medium used to make payment , the tool being used to process a payment , the nature of the transaction and the nature of the problem.[93] Here regulators are expected to come up with adequate regulatory frame work to regulate the new technology and make sure that it does not affect consumers and the stability of the financial system.[94]

The financial and non financial institutions may have different objectives in regulating the payment system. The objective of regulating financial institution basically focuses on ensuring that the electronic payment system does not cause systemic risks in the long run while the objective of regulating non financial institutions like telecommunications is to ensure that consumers are protected from operators reducing output to increase prices on low quality services.[95]The different objective of these institutions makes regulation more difficult as there is

[90] Supra note 39, p.17

[91] ibid

[92] ibid

[9393] Ibid, p.16

[94] Supra note 8, p.31

[95] Supra note 4, p.19

a need to determine which objective to pursue and how to achieve them as several institutions provide multiple services.[96]

The other challenge is a regulatory vacuum created due to the interconnectedness of telecommunication and finance. Here if the government has not issued regulation on new services then the new service may become controversial as to under which regulatory frame work it fall.[97]When there are multiple regulators companies can select the ones that advance their interest the most. This could mean they may select a more lenient regulator or take advantage of the rules that most benefit them. [98]

The basic regulatory challenges in electronic payment system include data privacy, money laundering and cyber attacks. Here regulatory bodies concerned with data privacy can sanction companies for not following proper risk assessment and meeting standards around consumer data.[99]

On the other hand governments take money laundering seriously. They recognize that these new payment technologies could be used to avoid duties. As such, each territory has its own anti-money laundry laws. Traditional banks and financial technology start ups are also big targets for hackers and other cyber criminals.[100]

[96] ibid

[97] Ibid, p.20

[98] ibid

[99]Nazaviy H., **Fintech Regulation: Legal issues and Regulatory compliance** , accessed at November 2022, https://geniusee.com/single-blog/fintech-regulation-legal-and-regulatory-aspects , July 2022, Guniusee, p.1.

[100] ibid

Chapter Three

Consumer protection of Electronic payment system in Ethiopia

3.1Introduction

Consumers gain from the expansion of mobile devices, the internet, and other technical advancements. The utilization of these cutting-edge technologies in financial services and goods alters how we borrow money, turn a profit, and handle our finances. Previous studies have found that younger, more educated consumers with higher incomes were more likely to use electronic payment systems.[101]

Electronics payment system is a recent phenomenon in Ethiopia. Thus, the issue of consumer protection in relation with such payment systems is also a new challenge for regulatory institutions and law makers. The Ethiopian civil code enacted in 1960 recognizes the issue of consumer protection especially in connection with contract and tort law[102]. After the liberalization of Ethiopian Economy in 1991, which recognized the issue of consumer protection was enacted as Trade practice Proclamation No. 329/2003. This Proclamation was later repealed and replaced by Proclamation No. 685/2010. Then this also replaced by the current proclamation of Trade competition and consumer protection No. 813/13(here in after TCCPP).

One of the TCCPP's goals, according to its preamble, is to safeguard consumers against deceptive and unfair business practices. However, Ethiopia was not familiar with the electronic payment system at the time this proclamation was enacted, and the technology for utilizing it is advancing quickly. It is therefore a question of whether consumers have sufficient legal protection against disputes arising from the use of electronic payments and whether our

[101] Joanna Stavins**, Effect of Consumer characteristics on the use of payment instrument**, 2001, accessed at march 2013 file:///C:/Users/user/Downloads/neer301b%20(5).pdf , p.23

[102] The civil code of the Empire of Ethiopian proclamation No.165/1960, **Negarit Gazeta extra ordinary issue**,, 19th Year, No.2

regulatory bodies are capable of overseeing these kinds of innovative electronic payment systems.

The NBE on the other hand issued multiple directives which address payment systems. These directives include mobile banking and agent banking, payment system operators, licensing and authorization of payment instrument issuers. The National Payment System Proclamation and the National Bank of Ethiopia establishment Proclamation are the main legal frame works which deal with payment system in general and the consumer protection of EPS consumers in particular.

This chapter aims to discuss the effectiveness of these regulations in safeguarding consumers and the various regulatory authorities' capacity to do so when it comes to EPS users.

3.2 General overview of electronic payment system in Ethiopia

Unlike the traditional banking system which needs the physical appearance of only the banker and consumer, the digital financial service requires different stakeholders and needs the cooperation of plural actors.[103]It needs the cooperation of banks, non-bank electronic payment providers, mobile network operators and other agents. In addition, each stakeholder is expected to operate in good faith and in accordance with the law. [104]

According to NPS Proclamation No. 718/2011 the Ethiopian payment system also involves different payment service providers which include operators, participants, issuers of payment instruments and any third party acting on behalf of them either as an agent or by way of outsourcing agreements.[105]

It's time to investigate these service providers' roles in the Ethiopian payment system. Here a payment system means a set of instruments, procedures, and rules for the transfer of funds

[103]Fekadu peteros, **Overview of Ethiopia's New payment issuer Regulation**, Journal of African Law, June 2020, p.7

[104] ibid

[105]The National payment system proclamation No. 718/2011, art 2(16), **Federal Negarit Gazeta**, 17th Year, No.84 (here in after NPSP)

between or among participants; the system includes the participants and the person operating the arrangement.[106]This includes

1. Payment instrument Issuer: -here it is a person licensed by the National bank to issue payment instruments against receipt of funds in Ethiopian birr.[107]
2. Payment operators: - According to article 2.34 of the operating directive, a payment service operator means the National Bank, a financial institution or any other person authorized by the national bank to own, operate and administer a payment system. The operator can be any person other than a financial institution who intends to operate a system that routes payment transactions, authorization and settlement request from merchants.[108] It also includes those who intend to engage in the provision of payment processing, personalization of payment cards, merchant acquiring, payment aggregation and payment application. These persons can get a license as per the directive.[109]
3. National Switch Operator:-here switch means a payment platform or network that enables payment transaction to be routed from one participant to another, whether within the same scheme or between different schemes.[110]In Ethiopia, there is a single national switch operator and it basically processes inter-bank direct debit and credit transfers.[111]There is also a switch operator which is connected to the national switch for the purpose of routing, clearing and settlement of inter-institutional payments.[112]
4. Participant: - a party who participates in a payment, clearing or settlement system directly or indirectly by opening or maintaining a settlement account at the National Bank.[113]Here a settlement system mean a system for the discharge of payment and settlement obligations

[106]The licensing and authorization of payment system operators directive No. ONPS/02/2020, art 2.33

[107] The licensing and authorization of payment instrument issuer directive No. ONPS/01/2020. Art 1(8)

[108] Supra note 95, art 4.1

[109] Ibid, art. 4.2

[110] Ibid, art. 2.43

[111] Ibid, art. 9

[112] Ibid, art. 10.1

[113] Supra note 94, art.2(19)

established and operated by the national bank or any other settlement system authorized by the National bank.[114]

5. Agents:-An agent is the one who is engaged in commercial / business activity and has been contracted by financial institutions to provide services of the financial institutions on its behalf as per the directive. These agents can also involve in agent banking which involves conducting a banking business on behalf of financial institutions by using various service delivery channels as permitted under mobile money and agent directive.[115]
6. Consumers: - A consumer is an individual or entity who uses financial institution services by using different electronic payment system[116]. Here a consumer can be a natural or juridical person.[117]On the other hand the TCCPP limits the scope of consumer only to natural persons who buy goods and services for personal and family consumption.

The engagement of these actors will therefore be covered in the following topics from the standpoint of consumer protection. In Ethiopia, the NBE is the main regulatory organ to give license, supervise and regulate the aforementioned actors who involve in the payment system.[118]

3.3 Regulation of electronic payment system in Ethiopia

For several reasons, authorities regulate payment systems and payment service providers. These reasons include maintaining the integrity of the monetary system, safeguard the financial stability by ensuring final settlement of money transfer and protect consumers with regard to non-currency money that entail credit risks.[119]

In many jurisdictions, the regulatory responsibility for payment related activities are broad and have two distinct roles-prudential supervision and oversight.[120] These regulatory mechanisms are

[114] Ibid, art 2(25)

[115]Regulation of Mobile and agent banking services directive No.FIS. 01/2012, art 2.1 and 2.2

[116] Ibid, art. 2.5

[117] National Bank of Ethiopia Establishment (as amended) proclamation No. 591/2008**, Federal Negarit Gazetta**, 14th year No. 50, art.2(11)

[118] Ibid, art.5

[119]Tanaikhiaonarong and Terry Goh, **Fintech and payments Regulation : Analytical Framework, accessed at https://get.adobe.com/uk/reader/**April 2023, IMF working papers , may 29/2020

[120] ibid

established by central bank laws and payment service laws. The prudential supervision focuses on payment service providers which mainly targets in achieving safe, secure and stable financial institutions and in delivering payment service to consumers while an oversight monitoring mechanism is implemented in payment systems with the purpose of achieving a sound and safe functioning of payment systems, payment instruments and infrastructures.[121]

These payment regulatory frameworks in many jurisdictions include identifying activities as payment service, licensing entities and designating systems, analyzing and managing risks and finally promoting legal certainty which includes a body of law that determines the rights and obligations of parties in the system.[122]

In Ethiopia, the NBE is the main regulatory organ which has the power to regulate the payment system in general and electronic payment system in particular.[123] The NBE has the power and duties to take steps to establish, modernize, conduct, monitor, regulate and supervise payment, clearing and settlement systems.[124]

In addition due to the involvement of technology in using payment system platform the financial sector in general and the EPS in particular depends on the service of Telecom Company in delivering its service to consumers. Thus, telecommunications laws and regulations are expected to align with the financial laws in general and electronic payment system in particular. Here, therefore, it is important to set boundaries between the regulations of telecommunications from that of financial services. [125]

The other organ which has its own impact on delivering electronic payment is the Information Network security authority (INSA). The authority has a mandate to regulate cyber security issues in Ethiopia.[126] It has also power to ensure that information and computer-based key

[121] ibid

[122] ibid

[123] Supra note 107, article 5(15)

[124] Ibid

[125] Supra note 8, p.36

[126] Information Network Security Agency Re-establishment Proclamation No, 808/2013**, Negarit Gazetta**, Year 20, No.6, Article 6

infrastructures are secured. Here any payment service provider in issuing a new payment application product is expected to get the approval of the NBE[127]. The NBE, on the other hand, before it approves the new payment application examines the new product and in doing so the NBE contacts INSA to ensure and evaluate the strength of the new app from the perspective of security.[128] Thus, we can understand that there is a coordinated effort between the NBE and INSA in approving the new payment application.

Therefore, INSA has indirect involvement in regulating these electronic payment systems and in examining and approving the new payment applications from the perspective of security.[129]

3.4 Institutional framework for regulation of electronic payment system

3.4.1 National Bank of Ethiopia

The NBE in Ethiopia is authorized to grant licenses and supervise electronic payment service providers. This includes payment issuers, operators and agents.[130]The NBE can take such steps to establish, modernize, conduct, monitor, regulate and supervise payment, clearing and settlement system.[131]

The regulatory framework of the NBE appears to be focused on prudential regulatory schemes and supervisory policies as a result of the rapid technological improvement in EPS. Recently, the NBE released directives for the licensing and authorization of payment operators and issuers of payment instruments. These directives allowed payment issuers with the approval of the NBE to issue electronic money instruments. The NBE also issued a use of Agents directive No.FIS/02/2020. Here, the directive put minimal requirements for risk management and consumer protection.

[127] Supra note 95, article 4(2)(a)(2)

[128] Supra note 116

[129] An Interview with Ato Ermias Kanja, NBE payment system oversight development follow up officer, held on April 11,2023 , Addis Ababa.

[130] Supra note 94, article 5(15)

[131] Ibid, article 5(3)

A new advanced version of payment instrument mostly presents a new regulatory problem, particularly with regard to security, privacy of data and related issues. Therefore, the primary duty of the regulator will be to comprehend the new product in order to make any necessary regulatory alterations to it. The NBE uses INSA experts to understand the new payment product.[132]Then it will take action in adjusting its regulatory framework if the new payment instruments need an adjustment in relation to security, data privacy and other similar issues.

Regarding EPS regulation, the NBE established distinct guidelines to safeguard consumers. The application process is the first step in the prudent regulatory framework's operation. After taking into account the operating system security protocols and the interest of consumers the NBE may approve an application to operate a system[133]. Here the directive stipulates that if the intended payment system to be operated or its related service poses risk to users (consumers) the NBE may reject the application for licensing.[134]

EP system operators are required to submit a report to the NBE on a monthly basis[135]. The report covers consumer protection issues such as the amount of fraud, cyber-attacks, and data loss that has occurred.[136]These enable the NBE to regulate the development of potential treats to the payment system.

However, Ethiopia recently modified the NPS Proclamation to permit foreign investors to operate digital financial services businesses, including the issuing of payment instruments and the operation of payment systems, provided they first get an NBE license.[137]Cross-border payments are also included[138]. Therefore, in order to address the issues brought up by these significant modifications to the payment system, the regulatory framework of the NBE needs to be adjusted.

[132] Supra note 116

[133]Supera note 95, article 6(4)(c)

[134] Ibid , article 4(20)(F)

[135] Supra note 96, article 17

[136] Supra note 95, article 17(2)(9)

[137] Ibid, article 6(6)(7)(8)

[138] Ibid, article 33

The NBE also takes different kind of administrative measures against any operator, participant or issuer of payment instrument when it determines that an infringement was committed on the NPS Proclamation or regulation or directives issued pursuant to the Proclamation. These measures include a written warning, imposition of restrictions or fines, suspension or revocation of the authorization of the perpetrator .[139]

According to the Ethiopian national digital payment strategy (2021-2024) even if the aforementioned regulatory mechanisms are set by the NBE there is a need for an additional regulatory framework as the digital financial services are becoming increasingly complex. Therefore, it would be imperative to look into sustainable and responsible approaches to boost the regulators' capacity. Moreover, extra competencies, such as risk management, are also required.[140].

In addition, even if there is an effort taken to improve the oversight and regulatory mechanisms for payment systems and services, the national digital payment strategy also recommends that there is a room for oversight improvement which includes capacity building of payment system staffs, development of procedures for the oversight unit and development of off-sight reporting and on sight inspection process.[141]

3.4.2 Telecommunications

More organizations need to collaborate in order to establish a more efficient regulatory framework, even though the NBE is the main regulatory authority in charge of overseeing EPS. Ethio-Telecommunications is responsible for providing a robust and secure infrastructure to connect electronic payment service providers and their clients. Thus, it stands to reason that the rules and legislation regulating telecommunications should be in line with those governing finance.[142]

[139] Supra note 106, article 34

[140] National Bank of Ethiopia, **National Digital payment strategy(2021-2024**), p.54

[141] Ibid

[142] Supra note 8, p.36

In other jurisdictions, however, the convergence of telecommunications and finance raises a regulatory challenge. The main issue with these kinds of regulatory schemes is that each sector has its own unique set of rules, which makes it difficult for regulators to establish a consolidated consumer protection law.[143].

ETHIO-telecom recently broadened its business horizon and joined the digital financing market. In May 2021, it introduced mobile payment service under the brand name "TELE-birr". ETHIO-telecom claims that its primary goal is to offer financial services to residents in rural areas and low-income communities who do not have access to banking facilities.[144]Thus, it appears that ETHIO-Telecom has assumed the role of both payment instrument issuer and the one in charge of offering a safe connection to all EPS participants. The regulation becomes more difficult in this case due to the convergence of these two roles, as already mentioned.

The Ethiopian Communication Authorities also mandated to safeguard the interests of consumers of communication services and to ensure electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondences in any electronic medium.[145]When conducting online business, electronic commerce employs electronic payment methods. Furthermore the Authority in protecting consumers uses its own regulatory schemes and for this reason it issued a directive.[146]

In the case between ***Mr.Kibrom Abraham vs. Mr.Kedir Ali et al.*** the Federal First Instance Court found out the commission of deceitful act, which obliges the defendants to pay a certain amount of money to the plaintiff. The plaintiff claimed the payment of 229,000 Ethiopian Birr, which was stolen from his Bank account at CBE, using mobile transfer. As the plaintiff stated in his statement of claim, on March 6, 2022 at 10:00 AM his SIM card suddenly stopped working and on the next day his SIM card was replaced by another SIM card up on his application to the 4th defendant (ETHIO-telecom). However, on March 6, while the SIM card was unworkable, birr

[143] Supra note 4, p.19

[144]https://www.ethiotelecom.et/ethio-telecom-launches-telebirr-digital-financial-services/2/#:~:text=Accordingly%2C%20Mobile%20Money%20business%20under,people%20who%20do%20not%20have, august 05, 2021, accessed at march 07/2022

[145] Communication service proclamation No. 1148/2019, **Negarit Gazzeta**, 25 year. No.82, article 6(14) and 6(26)

[146] Telecommunication consumer rights and protection directive No. 832/2021

174,000 was transferred to the 1st defendant and birr 55,000 was transferred to the 2nd defendant by unknown person from the plaintiff's bank account. And then, the plaintiff claimed the repayment of the money as the 1st and 2nd defendants are unlawfully enriched. In addition, the plaintiff claimed, that the 3rd defendant (CBE) breached the duty of protecting the consumer`s password and the 4th defendant gave my SIM card to the unknown person, who used my numbers to transfer money from my Bank account using mobile banking.

The first defendant defended the claim by stating that it is because of other business transaction the money transferred from other third party in to his account. The second defendant never defended himself as the case was proceeded *ex-parte against him*. The third defendant said that, the mobile banking password has already been given to the plaintiff and it's the plaintiff's duty not to disclose the password to third parties. The fourth defendant stated that, the transfer of money can only be done by the plaintiff and the 3rd defendant agreement. Since, the 4th defendant doesn't have any relation with transfer of money, we are not liable for the money stolen from the plaintiff, said the fourth defendant.

The court having examined the arguments and evidences provided by the parties, ruled that the first and second defendants are liable to pay the money claimed by the plaintiff as it was proven that the stated sum of money was transferred to their accounts and they were unlawfully enriched by it; whereas they didn't prove whether the money was transferred through other transactions. The 3rd defendant is not liable to the suit as the plaintiff didn't prove whether the 3rd defendant breached the duty of protecting consumer's password. The 4th defendant also became liable as it was proved that the employee of the 4th defendant blocked the SIM card of the plaintiff and gave new SIM card of the same numbers to the unknown person, who used it to transfer the stated amount of money. Finally, the court decided that the 1st, 2nd and 4th defendants are jointly and severally liable to pay the claimed sum of money to the plaintiff.[147]

This shows that there must be a co-ordinate effort between the NBE and ETHIO- telecom in order to protect EPS consumers. As we can understand from the case the fraudulent act can be made by an employee of the telecom service providers thus even with due diligence of the

[147] Mr.Kibrom Abraham vs. Mr.Kedir Ali et al**.** the Federal First Instance Court File number **89369**

consumer such kind of fraudulent act can be committed. Here it must be clear that the NBE does not have the mandate to regulate the activities of Ethio-telecom. On the other hand to use mobile money and internet banking, SIM card and internet is necessary. These services in Ethiopia currently are provided by ETHIO-Telecom and Safari Com which is regulated by Ethiopian Communications Authority.

The Authority is tasked for safeguarding consumers of telecommunication services, including their rights to safety, privacy, and other considerations. Based on the aforementioned circumstances, we can conclude that the regulatory measures of the NBE are insufficient to protect EPS consumers, as fraudulent acts can transcend the NBE's authority through the usage of mobile banking users' SIM cards.

The other important point we can infer from the case is that those employers who provide services for consumers are jointly and severally liable for their employees fraudulent acts committed against consumers. Therefore, there must be a coordinated effort between the NBE, Ethiopian Telecommunication Authority and other stake holders in order to protect consumers in a better way.

3.5 The current legal framework for consumer protection of EPS.

Regarding payment methods, the Ethiopian Government issued various laws. However, Ethiopia lacks a cohesive legal framework that governs EPS consumer protection. Thus, we find the issue of consumer protection in relation to EPS in different Proclamations and Directives. According to the amended NPS Proclamation, the National Bank may also issue a Directive to adopt relevant international principles and standards on payment systems to enhance the safety, efficiency and reliability of the national payment system[148]. This Directive is not issued yet.

The main legal framework in connection with EPS consumer protection includes the Civil Code of Ethiopia which deals with contract and tort law, the FDRE Criminal Code, the National Payment System Proclamation with its amendment, the Trade Competition and Consumer Protection Proclamation, payment instrument issuers Directive, Financial Consumer Protection Directive and national digital payment strategy (2021-2024).

[148] Supra note 106, article 35

The regulatory body should provide precise regulations and recommendations in the area of consumer protection, as highlighted by the OECD and UN standards for consumer protection and the experience of other countries. The global standard addresses data privacy, equitable consumer treatment, openness and transparency, and efficient dispute resolution procedures.[149]

The OECD, an international organization, which with its partners represents about 80 % of the world trade and investment, also launches guidelines for consumer protection of online payments. Ethiopia recently opened its financial sectors including the Bank sector to foreigners. The requirements covered in the policy guidance for consumer protection were covered in chapter two.

In order to safeguard EPS consumers, this topic primarily focuses on assessing the disparate consumer protection legislation frameworks and comparing them to worldwide standards.

3.5.1 Consumer protection in contract and Tort law of Ethiopia

The parties must voluntarily express their approval in order to be bound by the terms of the agreement. Under Ethiopian law, silence does not amount to acceptance in the absence of pre-existing business relationship.[150]This clause safeguards consumers during transaction.

Consumers are additionally protected by contract law provisions pertaining to fraud, duress, and mistake. Thus, consumers who are parties to a contract if they are forced or subjected to duress or make fundamental mistakes in concluding contracts the law provides for the invalidation of the contracts. [151]According to Ethiopian contract law, consumers are so protected as contracting parties. Hence, in the event that the contract is deemed void, a consumer who uses EPS to fulfill his contractual obligations is entitled to reimbursement of his money.[152]

Additionally, Ethiopian contract law offers several warranties which include the seller to guarantee the buyer that the goods and products are in accordance with the agreement and are free from defects.[153]

---

[149] Supra note 37

[150]Supra note 102, article. 1682

[151] Ibid, art.1706 and 1707(1)

[152] Ibid, art. 1815

[153] Ibid, art. 2287

These warranties become due when the seller provides the buyer with only a portion of the item that was purchased, or goods of a different type than what was specified in the contract.[154]

The consumer shall also inspect the items at the first moment preferably at the time the thing sold is delivered to him.[155]If the consumer discovers defects in these conditions, they have the right to request a replacement or the delivery of the missing component or quality.[156]

A specific (forced) performance is one of the additional remedies for non performance. This remedy may be requested in the event that the contract may be carried out without impairing the defaulting party's personal freedom and the consumer has a particular interest in seeing the transaction through to completion.[157]

Consumers may also request a contract cancellation in the event that the other contracting party is not performing within the terms of the agreement.[158]

In addition to the aforementioned remedies, consumers, as contracting parties, may also demand payment of damages in the event of nonperformance.[159]

Therefore, in the event that the other party breaches the contract, buyers who utilize electronic payment systems to fulfill their payment obligations may demand the aforementioned remedies.

However, there might not be a direct contractual link between consumers and manufacturers because of lengthy distribution channels. Manufacturers are generally responsible for ensuring that their products are safe for consumers, but if they make mistakes, whether intentionally or by negligence, they will be held liable. In such a situation, buyers are expected to demonstrate how manufacturers violated product liability laws and how this resulted in real costs and losses.[160]In

[154] ibid

[155] Ibid, art. 2295

[156] Ibid, art.2332

[157] Ibid, art.1776

[158]ibid, art.1784,2336 and 1789

[159]Ibid, art. 1790

[160]Dessalegn Adera , **The legal and institutional framework for consumer protection in Ethiopia**, Thesis, Addis Ababa university, School of Law, June 2011, p.13

this kind of circumstances strict liability or culpability may be the basis for this type of obligation. [161]

However, in cases where a defective product results in injury, the producer may be held strictly liable. In this case, the manufacturer's liability is independent of the consumer's capacity to demonstrate fault and is not contingent on warranty being there.[162]

Under the Ethiopian law, defective products are also dealt with in article 2085 of the Civil Code. According to this provision, manufacturers are liable for their product if it caused damage to consumers. The only exception to this liability is the defect which has caused the damage could have been discovered by customary examination of the goods or the damage is caused by the buyer.[163]

If a consumer pays via electronic payment system and the manufacturer is held extra contractually accountable, the manufacturer must reimburse the consumer.[164]In this sense, the victim should receive compensation that is equivalent to the harm s/he suffered. We can therefore draw the conclusion that the Ethiopian Civil Code's provisions on contractual and extra contractual liability can both be viewed as tools for consumer protection law.

3.5.2 Consumer protection and Criminal law

The significance of consumer protection is also acknowledged by Ethiopian criminal law. Accordingly, producing and distributing hazardous products can result in criminal liability, whether done so knowingly or negligently[165]. These criminal acts include manufacturing food staff or products which contain injurious or damaged ingredients[166]. Additionally, storing, offering for sale, importing, exporting, or distributing such harmful materials carries a sentence of simple imprisonment of at least six months[167].

[161] Ibid

[162] Ibid, p.15

[163] Supra note 138, art.2085(1) and 2086(2)

[164] Ibid , art.2091

[165] The criminal code of the Federal Democratic Republic of Ethiopia Proclamation No.414/2004, art.527

[166] Ibid, art 527(1)

[167] Ibid, art 527(2)

In addition if a crime is committed negligently in the above circumstances, the punishment is a fine or simple imprisonment lasting no more than six months.[168]Furthermore, consumers are protected under the Criminal Code in cases where property rights are violated. In this regard crimes involving fraud with misrepresentation of facts or situations or concealing facts which the criminal had a duty to reveal is punishable with simple imprisonment or depending on the gravity of the case, with rigorous imprisonment not exceeding five years and fine[169]. In addition, provisions in relation to fraudulent act including manipulation of stock exchange transaction, acts relating to insurance and forgery may be used to protect consumers[170].

On the other hand, criminal law has its own limitations when it comes to defending the rights of consumers. Among the explanations are that it must be proven beyond a reasonable doubt. Furthermore, the victim is not compensated by the criminal action.[171]

3.5.3 The National Payment System Proclamation

Ethiopia recently modified its financial sector rules and implemented a number of financial reforms. Recently, the National Payment Proclamation underwent various modifications and amendments. Opening the banking sector's market to foreign investment is one of the fundamental changes made.[172]With the NBE's approval, foreign nationals are permitted to invest as issuers of payment instruments or operators of payment systems.[173]

Furthermore, as we previously noted, the amended proclamation recognizes cross-border payments as well. In contrast to the previous amendment, the current one also classifies payment system operators and issuers of payment instruments as financial institutions.[174]

---

[168] Ibid, art 527(3)

[169] Ibid , art 682

[170] Ibid , art 694,698 and 699

[171] Supra note 151

[172] Supra note 106, article 6(7)

[173] National payment system (amendment) proclamation No.1282/2022, Negarit Gazzetta Communication service proclamation No. 1148/2019, **Negarit Gazzeta**, 25 year. No.82, article 6(7)(8)

[174] Ibid, article 2(12)

The amendment of the NPS Proclamation's was required to improve the regulatory framework in order to accommodate new NPS innovations, improvements, and advancements. In addition, according to the NPS proclamation's preamble, it also aims to ensure the safety, security, and efficiency of the national payment system.

The NBE under the NPS Proclamation empowered to authorize persons to set up, run, and issue payment instruments for the payment system.[175]Here according to article 2(21) of the NPS proclamation 'person 'means any natural or juridical person. These payment service providers are also considered as financial institutions in the amended proclamation.[176]

The NBE regulates and supervises service providers and for this reason the NBE issues directives which regulate the license and authorization of the payment instrument issuer and payment operator. Ensuring effective consumer protection is one of the goals stated in the preamble of these directives. The NBE also addresses consumer protection issues through the NPS Proclamation.

Here, we'll talk about the legislative frameworks designed to protect consumers and contrast them with global norms intended to safeguard users of electronic payments.

3.5.3.1 Terms and Conditions of the Contract

Creating clear and standard terms and conditions is one of the responsibilities of payment service providers to safeguard consumers. Additionally, these terms and conditions ought to apply to all of its consumers in a similar manner and make it available for their review and possible agreement.[177]Consumers can obtain information and transparency regarding the payment product through the terms and conditions. This helps to build confidence on consumers in using the payment instrument.

Among the concerns mentioned here is that reading and accessing these terms and conditions might not be simple. Additionally, consumers rush into agreeing to terms and conditions with the

[175] Supra note 94, article 4(2)

[176] Supra note 106, article 2(12)

[177] Supra note 94, article 19

payment issuer, leaving them with little opportunity to access and consider them.[178]In payment instruments like 'Tele-birr' consumers can download the payment application from play store. Consumers' ability to review payment terms is so limited because it is challenging to review the terms and conditions as we discover them on electronic devices. Here it seems it has the form of adhesive contract. However, in accordance with Ethiopian contract law, a deal is considered finalized if both parties have indicated that they agree to every aspect of the negotiation.[179]To address this issue, the NBE should guarantee that consumers receive the terms and conditions promptly and in an easily readable format.[180]So that consumers will have the opportunity to review the terms and conditions of the contract as per the provision of the NPSP. Also, it should be provided in simple language that the majority of people can understand in order to create a clear terms and condition.[181]

All alterations to these terms and standards must first have NBE approval. Additionally, the NBE has the authority to establish fundamental terms and conditions by directives that will apply to parties entering into contracts for stored value facilities and electronic financial transfers.[182]In accordance with this provision the NBE has issued the licensing and authorization of payment instrument issuer directive No. ONPS /01/2010. In this directive the payment issuer is obliged to enter into an agreement with the user and these terms on the other hand are expected to include at least disclosing price for products and services, stating the confidentiality of all users information, notifying easily the rights and responsibilities of users, informing the roles and responsibility of parties and other requirements which is stated in the directive.[183]

3.5.3.2 Data Protection and Privacy

Data protection and privacy constitute the other set of standards designed to safeguard consumers. Ethiopia currently lacks a robust privacy and data protection legislation. Even though several laws cover different aspects of data privacy, there is no comprehensive structure

[178] Supra note 35

[179] Supra note138, article 1695(1)

[180] Supra note 37, p.7

[181] Ibid, p.8

[182] Supra note 94, article 19(2)(3)

[183] Supra note 96, article 12(2)

controlling the use and exchange of consumer data. So, it appears that financial institutions and other parties routinely share this kind of information informally.[184]

The issue of privacy regulated under the NPSP. According to article 35(2) (e) of the NPSP payment service providers are obliged not to disclose any confidential information of their consumers. But there are exceptions to this rule if it is ordered by the court, law or legally authorized person or the National Bank[185]. It appears that the NPSP only covered the aforementioned employees' criminal responsibility in the event that consumer information was disclosed to outside parties[186]. Here it is not clear how the NBE regulates such misuse or data breach of consumer's information. Thus, it seems there is a need to have further guidance on data protection requirements for payment service providers.

The fact that numerous organizations might have access to consumer's mobile and online payment information is another concern regarding privacy. According to the study conducted by the FDRE Ministry of Justice on the title ''A study designed to propose solutions to, by identifying the causes and methods of committing crimes of fraud on banks''[187]there are different kinds of crimes on banks. Among those card fraud and money transfer fraud are mainly related with E-commerce.

Card Fraud is a kind of bank fraud takes place at an ATM machine. Fraudsters withdraw money using the information in the magnetic strip on the actual card. Sometimes fraudsters use small cameras to capture card information and pass codes and withdraw money.[188]

Money transfer fraud occurs when the detailed information of users is changed or altered to benefit other individuals. Money transfer service means the transaction of financial resources or money from one account to another account, especially to a user's account , Remittance by email,

[184] World Bank Group**, Federal democratic republic of Ethiopia, Diagnostic review of financial customer protection, Key findings and recommendations**, April 2017, p.18

[185] Supra note 94, article 35(2)(e)

[186] Ibid, article 35

[187]**በባንኮችላይየሚፈጸሙየማጭበርበርወንጀሎችመንስኤዎችውናየአፈጻጸምዘይኤዎችውንበመለየትየመፍትሔኃሳቦችን ለማቅረብ የተዘጋጀጥናት** (ማንቦት/2014 ዓ.ም የኢፌድሪ ፍትሕ ሚኒስቴር)

[188] ibid

or on a mobile phone; they can be done through other electronic means or by contacting the payee directly.[189]

In the case between ***Mr. SisayMoges vs. Ethiopian Telecommunication Corporation et al.***[190]the court confirmed the existence of fraudulent act. The case was presented before the Federal First Instance Court, where the plaintiff claimed the re-payment of 400,000 Ethiopian Birr, which was stolen from his bank account opened in the Commercial Bank of Ethiopia. The plaintiff stated in his claim, that the SIM card he has been using for telecom services was blocked for a certain period of time and at the same time 200,000 Ethiopian Birr was transferred using Mobile Banking from his account to the unknown person, whose name was later found to be Mr. Asres Tiruneh, and finally joined the case as a third party defendant. Again another 200,000 Ethiopian Birr was transferred to the same person with the same technique. Both those mobile transfers were made deprived of the plaintiff's awareness. The first defendant, Ethio-Telecom was sued vicariously for the blockade of the plaintiff's SIM card, as its employee did it, whereas the second defendant, Commercial Bank of Ethiopia was sued for not protecting the plaintiff's bank account, while it has legal and contractual duty of care to protect customer's deposits.

The defendants were totally denied the plaintiff's claim. The first defendant argued that it doesn't have any access to the plaintiff's password used for the mobile banking transfer. It is only the plaintiff and the second defendant that have access to the password, it added. The second defendant also argued that, it is the plaintiff's negligence, as he recklessly made other persons to know his secretive password. Again, the plaintiff doesn't prove whether the bank did any fault regarding the bank transfer.

Finally, the Court ruled out that the first defendant is liable for the systematic blockade of the plaintiff's SIM card that subsequences the withdrawal of money from the plaintiff's bank account. The second defendant (commercial Bank of Ethiopia) also became liable for breaching its duty of care and protection of plaintiff's money deposits. Hence, both defendants are jointly and severally became liable for the payment of 400,000 Ethiopian Birr to the plaintiff.

[189] ibid

[190] Sisay Moges Vs Ethio telecom et al. , Federal First Instance Court File No. 89369

The case shows that organizations providing mobile services, such as ETHIO-Telecom, can be able to access the data of their consumers who utilize mobile money. Here it seems the regulatory scheme to protect the privacy of mobile consumers given to the Ethiopian Communication Authority.[191]In addition, the recent Personal Data Protection Proclamation empowered the Ethiopian Communication Authority to ensure the enforcement of the Proclamation and monitor the utilization of personal data.[192] To ensure that consumer information is properly gathered, stored, and protected, all telecommunications service providers are required to create a policy protecting consumer privacy. [193]

Therefore, in order to safeguard the privacy of consumers using their mobile for payment transactions, various regulatory bodies must cooperate in a coordinated manner.

3.5.3.3Fair Treatment of Mistaken and Unauthorized Payment

Another issue raised here is a fair treatment of consumers in the case of mistaken and unauthorized payment transaction. Under these circumstances, the PSPS was obligated to inform consumers of their limitations and the circumstances under which they were liable for damages resulting from unlawful and wrong transactions.[194]Here the good practices in this regard generally limited the losses from unauthorized transaction to an amount specified by law. In these regard the NPSP does not have a provision which deals with mistaken and unauthorized transaction. Thus it should have a provision which answers the issues of reimbursement or other remedies for such kind of transaction.[195]On the other hand the financial consumer protection directive deals with unauthorized and mistaken transaction.[196]The Financial service providers shall disclose to financial consumers that they are being compensated fully for losses from unauthorized transaction except in cases of consumer's fraud or gross negligence.[197]

[191] Supra note 134, article 15

[192] **Personal Data Protection Proclamation** No. 1321/2024,Negarit Gazette, 30th Year, No.35, July 24th 2024, article 5

[193] ibid

[194] Supra note 173, p.46

[195] Ibid , p.47

[196] FINANCIAL CONSUMER PROTECTION DIRECTIVE NO. FCP/01/2020, article 5.1.7

[197] Ibid, article 5.1.7.3

In the case of w/o WorkneshBekele v. Ethio- Telecom et al, the claimant, W/o Worknesh, alleged that she was provided with phone line number 0911382422 by the first defendant, which she used for various purposes including mobile banking services until 24/11/2014EC. Subsequently, the second defendant closed the phone line and reassigned it to another individual who fraudulently withdrew 334,765.00 birr from the claimant's account and transferred it to a certain Ato Mulatu Debalke's account number. In her claim, W/o Worknesh requested the court to determine the responsible party among the defendants according to Article 35 of the CPC and order the repayment of the misappropriated funds. After reviewing the evidence presented, the court concluded that the first defendant had breached the contract by closing the phone line without the claimant's consent. Additionally, the second defendant had failed to exercise due diligence when the claimant informed them of the suspicious activity before the transfer occurred. As a result, the court held both defendants jointly liable to repay the sum of 334,765.00 birr to W/o Worknesh.[198]

This shows that even if the service providers have information before unauthorized transaction have been made they are not willing to reimburse and consumers are obliged to bring the case before courts. Thus the NBE as a regulatory body should take measures on those service providers who are not willing to reimburse as per the financial consumer protection Directive.

3.5.3.4Dispute Settlement Mechanism

In case of any payment transaction a dispute may arise especially in electronics commercial activities. Therefore, there is a need to provide consumers with remedies for disputes arising out of transactions for goods and services. Thus, there should be a guideline which protects consumers by establishing a dispute resolution and redress mechanism.

These mechanisms include establishing fair, effective and transparent self regulatory mechanisms, policies and procedures to address consumer complaints and resolve consumer disputes arising from electronics commercial activities.[199]In addition these mechanisms are expected to show which organ should be conducted and how that organ should also be conducted

[198] W/o WorkneshBekele v. ethio telecom et al, Federal First Instant court File No. 95618
[199] Supra note 37, p.21

in case of dispute. Furthermore these mechanisms should be adequate, low cost and easy to use. There must also be unreasonable delay if the consumers are entitled for reimbursement. [200]

The NPSP in these regard specifies that operators, participants and issuers of payment instruments must have internal complaints handling procedures which need to be communicated to consumers that use electronic payment services.[201]The Proclamation also gives the power to NBE to issue more detailed requirements in relation to such procedures.

According to the NPSP the payment service providers also obliged to advice users on the procedures for lodging complaints[202]. But the provision of the NPSP does not stipulate in a clear manner what kind of internal complaint handling procedures required. The NBE empowered to issue such detailed procedures for investigating and handling complaints of consumers in using electronic payment system[203]. In accordance with this provision the NBE issued Financial Consumer Protection Directive No. FCP/01/2020. The preamble of the Directive stipulates that one of the reasons to issue this Directive is the power given to the NBE to prescribe a detailed complaint handling mechanism.

The Directive stipulates in a detailed manner the obligation of service providers to apply policies and procedures for a fair, accessible, transparent, free and efficient internal complaint handling mechanism. The service providers shall also establish internal complaint handling unit at the head office and relevant information shall be communicated to the consumer at the time of concluding a contract.[204] The Directive also allows the consumer to make any complain in any language by using a variety of communication channels such as telephone and electronic messages. The service providers shall also respond to the complaints in the same medium of communication.[205]

If the consumer is not satisfied with the decisions given by the service provider or has not received response from the service provider, the consumer may submit the complaint to the

[200] Ibid, p.22

[201] Supra note 94, article 20(1)

[202] ibid

[203] Ibid, article 20(2)

[204] Supra note 182, article 5.5.2

[205] Ibid, article 5.5.2.4

National Bank.[206]However, the procedure in the Directive does not mention the role of courts if consumers are dissatisfied by the final decision of the NBE. In this circumstance the Directive stipulates that the decision passed by the NBE is binding on the service providers but optional to the consumer. Here it is not clear what optional mean for consumers.

Therefore one of the controversial issues in the dispute settlement mechanism of payment system is related with the power of courts in entertaining the civil matter arising from national payment system. Here the NPSP stipulates that disputes among parties involved in the national payment system concerning any civil matter arising under the proclamation expected to be resolved through mediation and if the disputes cannot be resolved through mediation the matter will be settled by arbitration. In addition the arbitral award will be final and binding on the parties.[207]

On the other hand in the same provision it clearly stipulates the provisions of the civil procedure code in relation with appeals also apply for such kind of disputes. Therefore we need to address the role of courts to entertain such disputes. It seems the above NPSP provisions particularly focus on mediation and arbitration in case of disputes arise among parties in the NPSP and it does not say anything about the role of courts.

If we carefully examine the NPSP provisions, we can observe that mediation and arbitration are the only options available for resolving disputes between the parties to the NPSP. In this regard it is not clear who are considered as parties in the NPSP. Does it include consumers as party? Need to be addressed.

We are required to examine the cumulative reading of NPSP articles 2(16) and 31 in order to respond to these inquiries. Article 31 (1) of the NPSP mandates that any disputes between parties involved in the NPS regarding a civil case should be settled through mediation. Therefore, it is unclear that who is mentioned as a party involved in the NPSP. Thus, in order to determine who is listed as a party, we should have to review other provisions. According to article 2(16)(e) of the NPSP the national payment system is a system that constitutes payment service providers including operators, participants, issuers of payment instrument and any third party acting on

[206] Ibid , article 5.5.4
[207] Ibid, article 31(1)(2)(3)

behalf of them, either as an agent or by way of outsourcing agreements, whether entirely or partially operating in the country.

In article 2(19) of the NPSP, "participant" is also defined as a party that creates and maintains a settlement account at the national bank or any other settlement organization as a direct participant in a payment, clearing, or settlement system. It is clear that the term "participant" does not include consumers in this case because not every consumer who utilizes an electronic payment system is required to open and maintain a settlement account with a national bank. As a result, consumers are typically excluded from involvement in the NPS.

Therefore we can conclude that any consumer who has a dispute arising from the electronic payment system can take the case to courts as consumers are not included in article 31(1) of the NPSP which limited those disputes to be resolved only through mediation and arbitration.

The researcher is also aware of the fact that a large number of cases are brought before courts by consumers especially in connection with fraud committed by third parties using EPS. This demonstrates that courts have the power to entertain disputable issues which arise from using electronic payments.

Last but not least, the NPS amendment Proclamation introduces Cross-border payment.[208] In this regard it is not clear how the current complaint handling mechanism framework can be effective due to the unique feature of cross-border transaction. Therefore it seems the NBE needs to adopt relevant payment systems principles and standards as it is allowed in the amended NPSP.[209]In addition the NBE may also collaborate with regional and international regulatory authorities[210] in order to place effective complaint handling mechanisms in case of cross-border transaction.

3.5.4 Trade competition and consumer protection proclamation

The primary legislative framework established in Ethiopia to safeguard consumers is the Trade Competition and Consumer Protection Proclamation (TCCPP).The concern is, however, whether it has a sufficient legislative framework to safeguard consumers who use payment systems

[208] Supra note 163, article 33
[209] Ibid, article 35
[210] Ibid, article 34

generally, and electronic payment systems specifically? We must examine the range of its use in order to respond to this query. According to article 4 of the TCCPP it applies to any commercial activity or transaction in goods and services conducted or having effect with in Ethiopia.

Thus, it is clear from its scope of applicability that the TCCPP solely covers commercial activity involving products and services. [211] However, using an electronic payment system is not limited to using it for commercial purposes; it may also be used for any non-commercial activity that involves getting money, sending money, or making payments.

Furthermore, it is clear from the NPSP that EPS can be used as a payment mechanism and that anyone can be authorized to issue this type of payment instrument as long as the NBE is in charge of overseeing it.[212]

Therefore, we could contend that this is one of the TCCPP's limitations in terms of its applicability to all electronic payment types, particularly those involving non-commercial activity.

The TCCPP's definition of a consumer as a natural person who purchases goods and services for their own or their family's use is a further limitation on its application to electronic payment systems.[213]However, based on a cumulative reading of NPSP articles 2(21) and 4(2) (a), any entity that is permitted to issue payment instruments, such as EPS, may be either a natural or legal person. We can therefore draw the conclusion that, in contrast to the TCCPP, which restricts its applicability to natural persons only, the NPSP is applicable to both natural and juridical (legal) persons. Therefore, in the situation of EPS, we are unable to apply the TCCPP's consumer protection rules to financial and nonfinancial institutions that possess independent legal personality.

Furthermore, the TCCPP does not apply to natural persons who utilize EPS for transactions involving goods and services beyond their own and their families' personal use. For the reasons

[211] Supra note 94, article 2(20)

[212] Ibid, article 4(2)(a) (2)

[213]**Trade competition and Consumer protection proclamation** No. 813/2013, article 2(4), Negaritt Gazetta, 20th year, No.28, March ,2014

listed above, we can thus infer that the application of the TCCPP's consumer protection to EPS is limited.

The official from the trade competition and consumer protection authority on the other hand argue that the authority has the power to entertain those disputes arising from EPS as the authority is the main body empowered by law to protect any kind of consumers[214].

However, bank officials argue that disputes resulting from EPS are not covered by the TCCPP. Their justification for their position is that, with regard to financial institutions, the NBE is the primary regulator. Therefore, the NBE should address any concerns that consumers may have. In addition, the NBE has issued a number of Directives to safeguard consumers in these kinds of conflicts. Therefore they argue that as there is a special regulatory organ which regularly inspect and supervise those financial institutions, there is no need to apply TCCPP in case of EPS in order to protect consumers.[215]

Here therefore unless there is a contradictory provision between the TCCPP and the different legislations issued by the NBE in relation with the EPS, consumers can use and cite both legislations in order to exercise their rights. But if there is any kind of contradictions the NBE in case of EPS seems to have a special regulatory mandate as it issued different Directives in connection with consumer protection of EPS which we discuss earlier. In addition the scope of its applicability in case of the TCCPP also seems limited as we discussed earlier. Therefore, we can conclude that in case of contradiction the NBE is a primary regulatory body.

3.5.5 Payment instrument issuer directive

A payment instrument is anything, tangible or intangible, such checks, drafts, and cards, that allows someone to receive money, commodities, or services, or to make payments or transfer

[214] An Interview with Ato Getnet Ashenafi, Head of restrictive business practices, prevention desk of Trade competition and consumer protection Authority (now the authority merged with Ministry of trade and regional integration) held on April 10,2023, Addis Ababa

[215]An Interview with Ato Ermias Kanja, NBE payment system oversight development follow up officer, held on April 11,2023, Addis Ababa, with Netsanet Admasu , Manager foreclosure of CBE, held on April 11,2023 and with Girma Asres , digital banking application senior official of Abay bank, held on April 12,2023, Addis ababa

money in other ways[216] .On the other hand, anyone licensed or allowed by the NBE to issue payment instruments is referred to as a payment instrument issuer.[217]

One of the goals stated in the directive's preamble is to create the enabling and transparent regulatory standards required to protect the interests of issuers of payment instruments. Here in order to get licensing and authorization for PII by the NBE one should at least fulfill the following requirements which includes equitable and fair treatment, confidentiality and disclosure of information, transparency, customer support arrangement, rights and responsibilities of all involved parties and complaint handling and redress mechanisms.[218]

Payment instrument issuers (PII) are required by this regulation to make every effort to protect their consumers as much as possible when conducting business.[219]However, it makes no indication of what it means to declare that every effort has been made to protect consumers.

On the other hand the PII and consumers also expected to enter into an agreement which at least includes disclosing information, confidentiality of consumers information, notifying users rights and responsibility, making a clear and standard terms and conditions applicable to all users, put in place a mechanism for complaint handling and dispute settlement mechanism.[220]

3.5.6 Mobile and agent banking services

Financial institutions may use other people who are involved in business or commercial activity to provide their services. These individuals can offer the service in accordance with the legal guidelines on behalf of the financial institutions. These people were known as agents.[221]Banks as financial institutions can also use an agent banking in order to serve their consumers by using various service delivery channels permitted by law.[222]

[216] Supra note 96, article 20

[217] Penalty for non compliance with the directive of the National bank directive No. ONPS/08/2022, article 2(2)

[218] Supra note 96, article 4(6)(h)

[219] Ibid, article 12(1)

[220] Ibid, article 12(2)

[221] Supra note 104, article 2(1)

[222] Ibid, article 2(2)

Mobile banking is another tool that banks utilize to better serve their clients. Using mobile devices, banks can carry out their banking operations, such as fund transfers and cash in and cash out services, through the usage of mobile banking, one of their service delivery channels.[223]Consumers in this case can be any person or organization that makes use of the mobile and agent banking services provided via mobile devices.

The NBE also issued Regulation of Mobile and Agent Banking Service Directive No. FIS /01/2012 to govern these services. The preamble of this regulation makes it clear that this technology was required to increase the accessibility of financial services to a larger segment of the population. On the other hand, there is a need to establish minimal requirements for risk management and consumer protection while employing these service delivery channels.

Financial institutions are obligated to implement sufficient rules and processes to safeguard their consumers while utilizing these service delivery channels.[224]Consumer identification should be the minimum of these policies and procedures, along with the issuance of standard, uniform, and easily identifiable paper receipts for every transaction, maintaining the privacy and confidentiality of consumers' information, disclosing terms and conditions, being transparent, and providing a mechanism for consumer complaints and redress.[225]

Furthermore, financial institutions offering agent and mobile banking services are required to notify the NBE as soon as they suspect or confirm fraud and significant security breaches. The issue is that, in contrast to the worldwide consumer protection standards we covered in chapter two, these directives only set standards in general terms. The NBE in this regard issued financial consumer protection Directive which applies to all financial service providers.[226]

[223] Ibid, article 2(11)

[224] Ibid , article 12(1)

[225] Ibid, article 12(2)

[226] Supra note 182, article 2.16

3.5.7 National payment digital strategy

A contemporary and effective financial sector is also required to have a sustainable and financially inclusive economic development, given the rapid digital transformation the world is going through. In this instance, a digital payment can boost the economy.

In this sense, the NBE is the primary entity in charge of changing the nation's payment ecosystem. The centerpiece of this transformation plan to modernize Ethiopia's national payment system is the national payment digital strategy (NPDS) for 2021–2024.[227]

The basic pillars of the NPDS includes the development of a reliable, inclusive and interoperable infrastructure, adoption of inclusive digital payments, building a robust and consistent regulatory and oversight framework and finally to create an enabling environment for innovation.[228]

Reform is required as part of one of the NBE's strategic initiatives to fortify its regulatory and oversight structure. This reform is essentially necessary because users are also at risk from the digital transition.[229]Therefore, in order to protect consumers in the face of this rapid digital revolution, regulatory reform is required.

The goal of NDPS Action 27 in this regard is to improve financial consumer protection. This includes the requirement for a dispute resolution process that can preserve openness and confidence in the electronic payment system. It also recommend data protection in digital environment which includes to take measures to ensure the confidentiality and security of consumers data, the ability of supervisors to have access to all consumers transaction data for oversight purpose.

These are the recommendations made in the digital strategy to enhance consumer protection; however, there are other areas that also need to be improved to achieve this goal. As we cover in chapter two, strengthening consumer protection in the area of confirmation processes, particularly in the case of electronic payments, is advised by worldwide best practices in this respect. This is because such methods might be misleading or fraudulent.

[227] Supra note 13, p.8

[228] Ibid , p.4 and p.5

[229] Ibid, p.55

Therefore, in order to safeguard financial consumers generally and users of electronic payments specifically, these criteria for consumer protection should also be enhanced in light of the significant technological advancements.

CHAPTER FOUR

Conclusion and recommendation

Conclusion

A recent phenomenon shows that the advancement of technology affected everyone's life. The business and financial activities are also affected by these technologies. This leads to the birth of electronic commerce and consumers start to use these technologies in order to do business and make payments. In this circumstances in many financial institutions and other businesses making payment by using electronic payment platforms become a common trend.

On the other hand it is important to understand that these financial technologies especially in payment system also pose a threat in regard to security, privacy, unauthorized transaction, fraudulent acts and so on. In addition from their unique characteristics these electronic payment plat forms need a close regulatory frame work in order to protect consumers.

In Ethiopia the NBE is the main regulatory body to regulate financial institutions in general and electronic service providers in particular. The NBE is mandated to issue different Directives which can help to strengthen its regulatory capacity to protect consumers but many of these directives are not issued yet. This includes a Directive to adopt relevant international principles and standards on payment systems as per article 35 of the amended NPSP, a Directive as per article 19(3) of the NPSP in order to supervise the basic terms and conditions to be applicable for contracting parties, a Directive as per article 31(4) of NPSP for the resolution of disputes arising in relation with the NPS and others.

However, NBE is not the only regulatory organ to protect consumers. In case of consumer protection other regulatory bodies including Ethiopian communication authority which is mandated to safe guard consumers who uses electronic mediums also participated. In this regard consumers use electronic mediums such as smart phones in order to transfer money for different reasons. This shows that that the authority also mandated to protect EPS consumers. However the role of the communication authority is limited basically in providing a secure and reliable connection to consumers.

The other regulatory body authorized in Ethiopia in case of consumer protection is the former trade competition and consumer protection authority. But now its power except adjudication is transferred to the ministry of trade and regional integration (MOTRI) as per article 22(1) (o) of proclamation No. 1263/2021. Here it should be clear that proclamation No. 1263/2021 does not repeal the former Trade competition and Consumer protection proclamation No. 813/2013. It rather only transfer the powers and duties of the TCCP authority to MOTRI as per article 22(1) (q) of proclamation No. 1263/2021. The Ministry in this circumstance protects consumers who involved in commercial activities and transaction in goods and services for the purpose of personal and family consumption. Therefore we can conclude that the Ministry is not mandated to regulate those consumers who make electronic payments for non commercial activities.

The other limitation of the TCCPP is it limits its consumer protection provisions for transactions of personal and family consumption. Thus we can infer that the consumer protection provisions of TCCPP cannot be applied for consumers who use EPS beyond the purpose of personal and family consumptions.

The third limitation of TCCPP in order to apply it for EP users is it defines consumers as natural persons who buy goods and services for their personal and family consumption. This shows that we can not apply TCCPP provisions in case of financial and non financial institutions which have their own legal personality.

The convergence of telecommunication and finance industries in using EPS raise also a challenge. These sectors have their own specific regulations and objective to achieve. Therefore still now Ethiopia does not have a consolidated legal frame work in order to protect users of EPS. We can also find the issue of EPS consumer protection in different legislation issued by different authorities.

The other problem emerges from entities beyond the regulatory schemes of the NBE like telecommunication which has an access to the information of consumers who uses their devices for payment purpose. In this regard the mandate to protect the privacy of consumers given to communication authority. Thus, there is a need for a coordinated effort of different regulatory organs in order to protect the privacy of consumers who uses EPS devices.

Ethiopian recently made several financial reforms in its financial sector policies. The NPSP in this regard amended recently and made a reform in areas of opening the national payment system market to foreign investment. Thus foreign nationals now allowed investing in PII or payment system operator with the approval of the NBE. In addition cross boarder payment also recognized under this amended proclamation.

Even if we don't have a consolidated consumer protection law in order to protect consumers' different legislation is enacted by different regulatory organs. Different standards are also set in these different legislations. The NPSP in this regard incorporate different consumer protection provisions including terms and conditions which provide information and transparency in payment product. Here the problem is consumers may not enter into contractual agreement with service providers after reading this terms and conditions. The reason for this is it may not be easy to access and read this conditions as consumers made rapid decisions without reading these terms and conditions. In addition, consumers can enter an agreement with service providers by down loading the application from play store. Thus it is difficult to review this terms and conditions as we find them in devices. On the other hand in order to fill these gaps the prior approval of the NBE is needed before the application of this terms and conditions. Furthermore, the NBE is also empowered to prescribe the basic terms and conditions.

Another standard set to protect consumers is privacy and data protection. Ethiopia in this regard does not have a comprehensive regime dealing with privacy and data protection. According to NPSP, payment service providers obliged not to disclose any confidential information of their consumers as per article 35(2) (e) of the proclamation. But here it is not clear how the NBE in this regard regulate the misuse or data breach of consumers' information. In addition it does not define what kind of information constitutes to say confidential information.

A fair treatment of consumers in case of mistaken and unauthorized payment transaction is set as a standard to protect consumers in international principles. We find this standard in financial consumer protection Directive.

In case of an electronic payment transaction a dispute may also arise. Thus there is a need to have a dispute resolution and redress mechanism. These mechanisms should include a fair, effective and transparent self regulatory mechanisms and procedures. These mechanisms should

also be low cost, easy to use and adequate. The financial consumer protection Directive tries to address complaint handling mechanism. However it has also limitation in addressing complaint handling mechanism in relation with cross-border payment.

The other controversial issue in dispute resolution is the power of courts. Some argue that the NPSP does not clearly stipulate about the power of courts therefore such disputes arising from the NPSP should only be entertained by mediation and arbitration as per article 31 of the NPSP. On the contrary others argue that mediation and arbitration as a means of dispute resolution applied to parties in the NPSP. In this circumstances parties in the NPSP are listed in article 2(16) of the NPSP. Consumers are not included in this list. Therefore, they argue that consumers can take their case to the court if a dispute arises in payment issues. In practice also there are disputes arising from payment transactions and entertained by courts..

The payment instrument issuer is another payment service provider. The PII is regulated by its own Directive issued by the NBE. In the preamble of this Directive one of its objectives is to protect the interest of consumers. Here in order to get licensing and authorization one of the criteria is to fulfill the rights and responsibilities of all involved parties. It also requires complaint handling and redress mechanism. This Directive expects maximum consumer protection from PII. However the Directive also does not mention what constitute to say that there is a maximum effort to protect consumers.

Financial institutions in providing their services may also use agents who engage in commercial activities. These services can be mobile or agent banking services. The NBE issued mobile and agent service Directive in order to regulate this service providers. The service providers also obliged to protect consumers by setting adequate policies and procedures including security, confidentiality of information, disclosure of terms and conditions, consumer complaint and redress mechanisms. The problem is what level of standard required in those policies and procedures is ambiguous.

Finally Ethiopia in order to transform the payment ecosystem with this technology advancement announced a national digital strategy which will stay from 2021-2024. One of the components of this digital strategy is to strengthen consumer protection. Action 27 of the NDPS basically focused on consumer protection. However the recommendations to strengthen consumer

protection strategy basically focus on the need to have a strong dispute resolution mechanisms and data protection. Here it seems the recommendation lacks to incorporate and strengthen other basic consumer protection standards when compared to the international good practices.

Recommendations

- The convergence o f telecommunication service with financial institutions makes it difficult to regulate EPS. Thus, there must be a coordinated effort between different regulatory organs including the NBE, communication authority, Ministry of trade and regional integration and others in order to protect consumers. This can solve the regulatory challenges and problems in relation to EPS.
- The NBE in regulating EPS is mandated to issue different Directive that have relevant in protecting consumers and strengthening the regulatory schemes of the NBE. But these Directives including adopting international principles and standards on payment systems, to prescribe basic terms and conditions applicable for contracting parties has not issued yet. Therefore, issuing these directives will allow the NBE to protect consumers of EPS in a better manner.
- Most of the consumer protection standards are stated in a general terms. This makes it difficult for regulatory bodies to supervise and oversight the service providers. Thus these general standards should have more detailed minimum standards. In this regard international good practices like OECD and UN guidelines can be used in order to set minimum standards that are expected from payment service providers in order to protect consumers..
- The amendment proclamation of the NPSP incorporates cross-border payment. This new development and change also may affect consumers. The NBE in regulating such kind of transactions should issue a different legislative and regulatory approach as it has its own unique feature. It may also adopt international principles as per article 35 of the amended NPSP.
- In the case of data protection and privacy it is not clear how the NBE regulate such misuse and data breach. Here the main regulatory body in the service of electronic devices is Ethiopian communication authority. Thus there must be a coordinated effort between the NBE and the authority in order to protect consumers. In addition there is a need to have further guidance on data protection.
- The national payment digital strategy should also incorporate other basic consumer protection standards other than dispute resolution mechanism and data protection in order to strengthen the regulatory scheme.

Bibliography

Books

- Amitabh Saxena, **Electronic payment system 201**,Digital disruptions , November 2014
- Joy Malala , **consumer protection for mobile payments in Kenya**, An examination of the fragmented legislation and complexities it presents for mobile payments , KBA center for research on financial markets and policy working paper series, Kenyan Bankers association, 2013
- Lauren saunders, **Fintech and consumer protection**, National consumer Law center, March 2019
- Roger E.meiners and Franies L.Edwards, **Manging in the legal environment** , (3rd ed),west publishing company,USA,1996
- World Bank Group**, Federal democratic republic of Ethiopia, Diagnostic review of financial customer protection, Key findings and recommendations**, April 2017
- **Zon-yau lee, Hsiao-cheng yu, pej-jen kuo**, **Analysis and comparison of different Types of electronic payment systems** , institution of management of technology, Chiao-Tung University, Taiwan

Research papers

- Ashenafi Lemecha Moti , **Consumers and third parties protection under the national payment system proclamation No. 718/2011**, thesis , Addis Ababa University, February 2017
- Bikila Ababu**, Regulation of electronic banking in Ethiopia, The analysis of legal frame work**, Thesis, Addis Ababa University, June 2019

- Dessalegn Adera , **The legal and institutional framework for consumer protection in Ethiopia**, Thesis, Addis Ababa university, School of Law, June 2011

- Lempere Solomon, **Consumer protection in the Kenyan financial sector: A case for a twin peaks model of financial regulation, thesis,** university of the western cape, August 2019
- OECD, **Consumers policy guidance on mobile and online payments**, OECD digital economy papers, No.236
- Simret Zewdie**, Electronic Funds transfer and the case for consumer protection in Ethiopia** , University of Oslo, August 6,2013
- Tanai khiaonarong and Terry Goh, **Fintech and payments Regulation : Analytical Framework, accessed at https://get.adobe.com/uk/reader/** April 2023, IMF working papers , may 29/2020

Articles

- Fekadu peteros, **Overview of Ethiopia's New payment issuer Regulation**, Journal of African Law, June 2020
- Gardachew work, **Electronic-Banking in Ethiopia practices, Opportunities and challenges**, Journal of internet and commerce, August 2010, Vol. 15. No.2.(http://www.auvaydev.com/commerce/jibc)
- Zlatko Bezhovski**, the future of the mobile payment as electronic payment system**, European Journal of Business and management , Vol.8, 2016
- **በባንኮች ላይ የሚፈጸሙ የማጭበርበር ወንጀሎች መንስኤአቸውና የአፈጻጸም ዘይአቸውን በመለየት የመፍትሔ ኃሳቦችን ለማቅረብ የተዘጋጀ ጥናት** (ግንቦት/2014 ዓ.ም የኢፌድሪ ፍትሕ ሚኒስቴር)

Sources from the World Wide Web

- Aman jain, **Challenges online payments are facing and how to solve them**, accessed at, https://finance.yahoo.com/news/challenges-online-payments-facing-solve-152910966.html, October 7,2021
- Asena Degirmenci, **what is financial regulation and why it is important**? , accessed at February 2022 https://www.leasinglife.com/news/industry-news/what-is-financial-regulation/, May 10, 2019
- European parliament, **consumers protection aspect of mobile payment**, accessed at February 2022, https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/564354/EPRS_BRI(2015)564354_EN.pdf, June
- European parliament, **consumers protection aspect of mobile payment**, accessed at February 2022, https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/564354/EPRS_BRI(2015)564354_EN.pdf, June 2015
- Joanna Stavins**, Effect of Consumer characteristics on the use of payment instrument**, 2001, accessed at march 2013 file:///C:/Users/user/Downloads/neer301b%20(5).pdf
- Nazaviy H., **Fintech Regulation: Legal issues and Regulatory compliance** , accessed at November 2022, https://geniusee.com/single-blog/fintech-regulation-legal-and-regulatory-aspects , July 2022
- OECD, **report on consumer protection in online and mobile payments** , OECD digital economy papers No 204
- Robin Simpson, **Mobile payments and consumer protection**, accessed at march 2022, https://www.consumersinternational.org/media/1845/mobile-payments-and-consumer-protection.pdf, January 2014,consumer international
- World bank, **Global survey on Consumer Protection and Financial Literacy ; Oversight framework and practices in 114 Economies** , 2014, accessed at November 2022 , https://documents.worldbank.org/en/publication/documents-

reports/documentdetail/815911468154453508/results-brief-regulatory-practices-in-114-economies

Laws

- A proclamation to provide for the definition of the powers and duties of the Executive organs of the Federal Democratic Republic of Ethiopia **Proclamation** No.1263/2021**, Neggrait Gazzeta, 28th year No.4, January 2022**
- The civil code of the Empire of Ethiopian proclamation No.165/1960, **Negarit Gazeta extra ordinary issue**, 19th Year, No.2
- The criminal code of the Federal Democratic Republic of Ethiopia Proclamation No.414/2004, **Negarit Gazetta, 9th of may 2005.**
- FINANCIAL CONSUMER PROTECTION DIRECTIVE NO. FCP/01/2020
- Information Network Security Agency Re-establishment Proclamation No, 808/2013**, Negarit Gazetta**, Year 20, No.6
- The licensing and authorization of payment instrument issuer directive No. ONPS/01/2020
- The licensing and authorization of payment system operators directive No. ONPS/02/2020
- Licensing and supervision of banking business fraud monitoring directive No.SSB/59/2014
- National Bank of Ethiopia Establishment (as amended) proclamation No. 591/2008**, Federal Negarit Gazetta**, 14th year No. 50)
- The National payment system proclamation No. 718/2011, **Federal Negarit Gazeta**, 17th Year, No.84.
- National payment system (amendment) proclamation No.1282/2022,Negarit Gazetta Communication service proclamation No. 1148/2019, **Negarit Gazzeta**, 25 year. No.82
- Penalty for non compliance with the directive of the National bank directive No. ONPS/08/2022

- Personal Data Protection Proclamation No. 1321/2024,Negarit Gazette, 30th Year, No.35, July 24th 2024
- Regulation of Mobile and agent banking services directive No.FIS. 01/2012
- Telecommunication consumer rights and protection directive No. 832/2021
- **Trade competition and Consumer protection proclamation** No. 813/2013, Negaritt Gazetta, 20th year, No.28, March ,2014
- UNCTAD ,**United Nations Guidelines for consumer protection**, https://unctad.org/system/files/official-document/ditccplpmisc2016d1_en.pdf, UNITED NATIONS, New York and Geneva, 2016

Interviews

- An Interview with Ato Ermias Kanja, NBE payment system oversight development follow up officer, held on April 11,2023, Addis Ababa
- An interview with Girma Asres , digital banking application senior official of Abay bank, held on April 12,2023, Addis Ababa
- An interview with Netsanet Admasu , Manager foreclosure of CBE, held on April 11,2023, Addis Ababa

Cases

- Mr.Kibrom Abraham vs. Mr.Kedir Ali et al**.** the Federal First Instance Court File number **89369**
- Sisay Moges vs Ethio telecom, Federal first instance court File number 302643
- W/o WorkneshBekele v. Ethio telecom et al, Federal First Instant court File No. 95618

Annexes

Annex one

Interview guides prepared for the National bank Authority

Personal detail of the respondent (if he/she consented) ----------

Position in authority ----------

Type of Study; - A Master thesis in law (LLM thesis)

Title:- Consumer Protection Of Electronic Payment System In Ethiopia

The objective of this interview is to assess the view of the officials of the NBE with regard to the regulation of electronic payment instruments in general and consumer protection of electronic payment users in particular. It also try to know whether there is formal or informal cooperation between the National Bank and other stake holders with the purpose to protect consumers of electronic payment instruments and finally to suggest possible solutions in the findings.

So, you are kindly requested to respond to the interviews as your information will be helpful for effective accomplishment of the study and as it will be kept confidential and analyzed anonymously unless you consented for the disclosure of your identity and personal views.

Thank you, in advance, for your co-operation

1. Do you think the trade competition and consumer protection proclamation No.813/13 are applicable for electronic payment users?
2. Is there any co-ordinate effort between payment service providers and the NBE to protect users of electronic payment instruments?
3. Is there any different approach in regulating electronic payment systems which is made under financial and non-financial institutions?
4. Do you think Ethiopia have adequate legal frame work to ensure consumer protection for electronic payment systems?
5. Is there any allegation made by users of electronic payment instrument against banks or other financial institutions?
6. As electronic payment systems related with technology who do you think should be a regulator? Do you think NBE should be the sole regulator?
7. Do our consumer protection laws answer the following questions?
   7.1 Who can access an individual mobile money records? When and for what purpose? Is there any regulatory scheme about what standard of privacy should be protected?
   7.2 Is there a coordinated effort between telecommunication and banks in Ethiopia in order to protect data privacy in using internet banking?
   7.3 Is there a coordinated effort between banks and telecommunication in order to solve problems which emanate from electronic payment system?
8. Is there any legal protection given to unauthorized transaction? Is there any period of limitation for such kind of unauthorized transaction?
9. Do we have any redress mechanisms for such kind of unauthorized transaction? If your answer is yes what are the redress mechanisms?
10. Is the national bank examining the consumer's protection issue when an application is made for obtaining an authorization for operating system?

11. Is there adequate consumer protection guidance given to electronic payment instrument in the following issues?
    1. Information on the terms, conditions and costs of transaction.
    2. Privacy
    3. Security
    4. Confirmation process
    5. Children
    6. Protection against fraudulent and misleading commercial practice
    7. Dispute resolution and redress
12. Does the NBE Oversight the terms and conditions prepared by the payment instrument issuer?
13. Does the NBE issue a directive on complaint resolution which arises from electronic fund transfer and stored value facilities as per article 20(2) of the NPS proclamation?
14. Does the NBE issue directive as per article 19(3) in order to supervise the basic terms and conditions to be applicable for contracting parties?
15. Does the NBE issue directive as per article 31(4) for the resolutions of disputes arising in relation with the NPSP?
16. Does courts have jurisdiction in order to entertain the disputes arising from NPS? As per article 31 of the NPS does a party include customers?
17. Why not good faith does not apply in case of article 34 while it applies in case of article 33?

Annex Two

Interview guides prepared for the Ministry of trade and regional integration

Personal detail of the respondent (if he/she consented) ----------

Position in authority ----------

Type of Study; - A Master thesis in law (LLM thesis)

Title: - <u>Consumer Protection Of Electronic Payment System In Ethiopia</u>

The objective of this interview is to assess the view of the officials of the authority with regard to the application of the Trade Competition and Consumers Protection Proclamation No. 813/13 in

consumer protection of electronic payment system and to know whether there is formal or informal cooperation between the National Bank and the ministry to protect consumers of electronic payment instruments and finally to suggest possible solutions in the findings.

So, you are kindly requested to respond to the interviews as your information will be helpful for effective accomplishment of the study and as it will be kept confidential and analyzed anonymously unless you consented for the disclosure of your identity and personal views.

Thank you, in advance, for your co-operation

1. Do you think the trade completion and consumer protection proclamation No.813/13 are applicable for electronic payment users?
2. Is there any co-ordinate effort between banks and the authority to protect users of electronic payment instruments?
3. Is there any different approach in regulating electronic payment systems which is made under financial and non-financial institutions?
4. Do you think Ethiopia have adequate legal frame work to ensure consumer protection for electronic payment systems?
5. Is there any allegation made by users of electronic payment instrument against banks or other financial institutions?
6. Do you think the Ethiopia consumer protection law gives adequate protection for consumers who use EPI?
7. As electronic payment systems related with technology who do you think should be a regulator?
8. Do our consumer protection laws answer the following questions?

   a).Who can access an individual mobile money records? When and for what purpose?

   b).Is there a coordinated effort between telecommunication and banks in Ethiopia in order to protect data privacy in using internet banking?

   c).Is there a coordinated effort between banks and telecommunication in order to solve problems which emanate from electronic payment system?
9. Is there any legal protection given to unauthorized transaction? Is there any period of limitation for such kind of unauthorized transaction?

10. Do we have any redress mechanisms for such kind of unauthorized transaction? If your answer is yes what are the redress mechanisms?
11. Is the national bank examining the consumer's protection issue when an application is made for obtaining an authorization for operating system?
12. Is there adequate consumer protection guidance given to electronic payment instrument in the following issues

    a).Information on the terms, conditions and costs of transaction.

    b). Privacy

    c). Security

    d). Confirmation process

    e). Children

    f). Protection against fraudulent and misleading commercial practice

    g). Dispute resolution and redress

13. Is there any effort made by the authority to protect electronic payment system?