UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

TOWARDS A ROBUST CONSUMER PROTECTION DRIVEN REGULATORY FRAMEWORK FOR E-COMMERCE IN NIGERIA

BY

ADETUTU TALABI.

DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF THE MASTERS OF LAWS (LLM) DEGREE IN INTERNATIONAL TRADE AND INVESTMENT LAW IN AFRICA

SUPERVISOR: DR FEMI OLUYEJU

8TH OCTOBER 2021

DECLARATION

I, ADETUTU TALABI, do hereby declare that this is an original work done by myself and has never been submitted for any degree or examination in any University or higher institution of learning for publication as a whole or in part. All the sources used have been indicated and acknowledged as complete references.

ADETUTU TALABI

8TH OCTOBER 2021

ACKNOWLEDGMENT

My first and foremost gratitude goes to God Almighty, my help in ages past and hope for years to come.

I dedicate this mini dissertation to the memory of my late mother, Margaret Talabi, who made me fall in love with the subject of International Trade and Investment Law. Her wisdom, passion and thirst for academic knowledge had always inspired me – and continues to do so.

I am ever grateful to my father, Mr Doyin Talabi, the best father in the world. He taught me what no academic curriculum could ever teach; faith in God, character, integrity and hardwork. May God Grant him Long Life and may he reap the fruit of his Labour.

My sincere Appreciation to my siblings, Mrs Obanya, Mr Gbolahan Talabi and Mr Goke Talabi, for their care and love. I especially appreciate Mr Goke Talabi for constantly being an anchor and a strong supporter of my dreams-God's love will be your portion always.

Tons of appreciation to Ms Memory Dube, Mr Tapiwa Cheuka and Mr Albert Puja for taking out time to review my thesis. May the Lord continue to bless you all. I specially appreciate Ms Ronke Famuyiwa, for her unwavering support and mentorship throughout this programme. I also thank the entire TILA class of 2021 for their friendship and support all through the year. I look forward to seeing you all at the top. Last, but not least, I am grateful to my supervisor, Dr Femi Oluyeju for his academic insight and guidance throughout the LL.M programme.

LIST OF ABBREVIATIONS

ADR	Alternative Dispute Resolution
B2B	Business-to-Business
B2C	Business-to-Consumers
B2G	Business-to-Government
C2C	Consumer-to-Consumer
CBN	Central Bank of Nigeria
CGSO	Consumer Goods and Services Ombudsman
CPA	Consumer Protection Act
EDI	Electronic Data Interchange
ETCA	Electronic Communication and Transaction Act
FCCPA	Federal Competition and Consumer Protection Act
IT	Information Technology
NDPR	General Data Protection Regulation
ODR	Online Dispute Mechanism
OECD	Organization for Economic Co-operation
POPIA	Protection of Personal Information Act
UNCITRAL	United Nations Commission on International Trade Law
UNGCP	United Nations Guideline on Consumer Protection
WTO	World Trade Organization

ABSTRACT

This study focuses on consumer protection in Nigeria's e-commerce Landscape. This study critically examines the extant regulatory frameworks in Nigeria. It compares its framework with international instruments and South Africa's frameworks, a fellow leading e-commerce giant on the continent. This study draws out lessons that Nigeria can learn from South Africa's success in providing robust laws to protect online consumers. It concludes with practical recommendations on improving Nigeria's current regulatory frameworks to engender consumer confidence in e-commerce.

TABLE OF CONTENT

CHAPTER SIX: FINDINGS AND RECOMMENDATIONS

CHAPTER ONE

1.1 INTRODUCTION

The growth of Information Technology (IT) has changed the landscape of trade globally.[1]One of these changes has taken the form of electronic commerce (e-commerce).[2] Innovators in the United States of America (USA) first developed e-commerce in the early 1960s[3] under the Electronic Data Interchange (EDI)[4] software, marking the first generation of e-commerce.[5] The EDI software helped businesses exchange documents amongst themselves through computers and facilitated the transfer of funds electronically.[6] Large corporations, financial firms and other few enterprises were the primary users of the EDI software. However, through the early 1970s and 1980s, manufacturing, retail and other service businesses began to embrace the technology.[7] These institutions used EDI software because they were trying to reduce the use of paper. Unfortunately, the adoption of the EDI software was low due to its high cost[8]; users also experienced several technical problems[9].

The early 1990s marked the beginning of the second generation of e-commerce.[10] The use of e-commerce was expanded to serve business to consumer needs.[11] There was a rapid creation of business to consumer e-commerce websites such as E-bay, Alibaba and Amazon.[12] Many businesses also began to build websites to conduct business on the internet.[13] In addition, companies such as Dell started to sell their computers to their consumers through the internet.[14] Over the years, the productivity, efficiency and effectiveness of e-commerce have created more extensive access to

[1] B Joseph "The Roles of Information & Communications Technology (ICTs) and E-commerce as Agents of Nigeria's Economic Development: Review of Challenges and Prospects" (2019) 10 Wireless Engineering and Technology Journal 43 https://www.scirp.org/pdf/wet_2020041415315688.pdf (accessed 6 October 2021)

[2] E-commerce is a means of buying and selling goods or services through the internet.

[3] Y Tian & C. Stewart "History of E-commerce" in SA Becker (1st edition) *Electronic Commerce: Concept, Methodologies, Tools and Applications" (2008) 2.*

[4] A Manzoor *E-commerce: An Introduction* (2010)13.

[5] As above.

[6] D White & G Ariguzo "The First Decade of E-commerce" (2008) Journal of International Business Information 1 Systems 239

[7] A Manzoor (n2) 13.

[8] A Manzoor (n2) 13.

[9] VF Santos, GM Morais, LR Sabino and CA Goncalves "E-commerce: A Short History Follow up on Trends" (2017) 8 International Journal of Business Administration 131.

[10] A Manzoor (n3) 13.

[11] VF Santos, GM Morais, LR Sabino and CA Goncalves (n70) 132.

[12] D White & G Ariguzo (n71) 242.

[13] Y.Tian & C. Stewart "History of E-commerce" in Anne Becker (n2) 3.

[14] VF Santos, GM Morais, LR Sabino and CA Goncalves (n70) 132.

markets globally[15], especially for enterprises in the developed world. According to a report by the International Trade Centre, e-commerce alone generates at least US$15 trillion annually from business to business transactions and well over US$1trillion from business to consumer trade.[16]

As with other markets, at the heart of a successful trade regime is consumer protection.[17] Generally, consumer protection deals with shielding consumers from business malpractices. Due to the virtual nature of e-commerce, it is crucial that consumers feel safe when transacting on e-commerce platforms.[18] Therefore, the failure of legal regimes to protect consumers transacting on e-commerce platform will hamper the growth of this sector.[19]

E-commerce is impressively growing in Africa. This growth is attributed to the high penetration of the internet, mobile technology and a growing young population. The retail landscape in Africa is currently being disrupted by e-commerce platforms such as *Jumia, Konga, takealot, Kilimal and Souq.* Nigeria is one of the leading e-commerce markets on the continent. In 2019 alone, the number of visitors to online marketplaces grew to over 250 million.[20] In addition, the Corona Virus 2019 (COVID-19) pandemic further accelerated e-commerce in Nigeria as businesses had to shut down physical operations to curtail the spread of the deadly virus. Even with the effect of the COVID 19 on e-commerce in Nigeria, the sector has still not reached its full potential, particularly in business to consumer e-commerce platforms.[21]

Despite the traction that e-commerce is gaining in Nigeria, malpractices against consumers are rife.[22] Studies[23] show that consumers utilising e-commerce platforms in Nigeria are confronted with a host of challenges, including misrepresentation[24], fraud, false advertising, deceptive pricing, late

[15] International Trade Centre "*International E-commerce in Africa: The way forward" 2015 at 4* Microsoft Word - E-commerce_111215 (intracen.org) (accessed 15 April 2021).
[16] As above.
[17] C Stork, K Fourati, P Esselar & F Odufuwa *A situational Analysis of Digital Trade and the Digital Economy in Africa* (2020) 2.
[18]OECD *Consumer Protection and E-commerce*(2016)390 https://www.oecd-ilibrary.org/docserver/9789264251823- accessed 6th October 2021.
[19] R Khare & G Rajvanshi "E-commerce and Consumer Protection: A Critical Analysis of the Legal regulations" (2013) International Journal on Consumer Law and Practice at 62.
[20]S Vanella"E-commerce in Nigeria: Statistics and facts (13 November 2020) https://www.statista.com/topics/6786/e-commerce-in-nigeria/ accessed 1st May 2020.
[21] N Okpara *Ethics and the Prospects of E-commerce Platforms in doing Business in Nigeria* (2021) 2.
[22] EU Gladys "Legal Framework for the Protection of Online Products Consumers in Nigeria (2018) 21 Nigerian Law Journal 26.
[23]I ILobinso, 'Paving the Path to an Enhanced Consumer Protection for the Nigerian Online Market: Theories and Concepts' (2017) 8 Nnamdi Azikiwe University Journal 81, EU Gladys (n5) 26, N Okpara (n5) 3.
[24] Okpara (n5) 2.

delivery or non-delivery of goods. In addition, the virtual nature of e-commerce has created an avenue for manipulation by sellers[25] and have made consumers susceptible[26] to the issues identified above. Overall, consumers have been put in a weak position; this has made it imperative to investigate the existing legal and regulatory frameworks for consumer protection under e-commerce in Nigeria to underscore if they are adequate in curbing these malpractices. This becomes particularly important because if consumers do not feel safe, it will undermine their acceptance, which will have the undesired effect of undermining the growth of e-commerce.

In light of the above, this study examines the legal and regulatory frameworks for the protection of consumers under e-commerce in Nigeria to identify its extant deficiencies. South Africa has successfully created a robust framework for consumer protection under e-commerce, thus the study will examine South Africa's framework and draw lessons that Nigeria can learn. This study also examines international instruments covering the subject of consumer protection under e-commerce. Finally, this study concludes by proffering practical recommendations for the robust protection of consumers under e-commerce in Nigeria.

1.2 RESEARCH PROBLEM

One of the significant challenges in e-commerce is consumer protection. The virtual nature of e-commerce makes consumers susceptible to unfair trade practices such as misrepresentation, fraud, false advertising, deceptive pricing and noncompliance with manufacturing standards.[27] These challenges are prevalent in Nigeria's e-commerce landscape. The deficiencies in Nigeria's extant legal and regulatory framework have further exacerbated these challenges. A case in point is that the Federal Competition and Consumer Protection Act, the leading framework on consumer protection in Nigeria, surprisingly makes no reference to e-commerce and does not address the peculiarities of e-commerce. In addition, there is currently no legal framework that regulates civil and contractual breaches under e-commerce.[28]

Furthermore, litigation has not been a suitable mechanism in seeking redress because e-commerce transactions are virtual and borderless, and the transaction volume is usually small. Alternative

[25] Ilobinso (n5) 83
[26] As above
[27] A Abubakar & F Adebayo "An Analysis of the Electronic Transactions Bill in Nigeria: Issues and Prospects" (2015) 3 Mediterranean Journal of social sciences 2.
[28] Although there is a Cybercrime (Prohibition and Protection) Act of 2015, this only regulates criminal activities.

Dispute Resolution Mechanisms (ADR) such as Mediation, Negotiation or the use of Ombudsmen would have helped augment the inadequacies of litigation for e-commerce dispute resolution. Unfortunately, these mechanisms have been underutilised under the existing frameworks.

1.3 RESEARCH QUESTIONS

The overarching question which this study seeks to answer is what measure can Nigeria adopt to improve protection for consumers under e-commerce? In order to answer this question, the following questions need to be answered-

1. What is the conceptual framework of e-commerce and consumer protection?
2. What are the international instruments governing consumer protection in e-commerce?
3. What is the current legal and regulatory framework for consumer protection in e-commerce in Nigeria?
4. Do the extant regulatory and institutional frameworks for e-commerce in Nigeria offer consumers adequate protection compared to South Africa?
5. How can Nigeria improve on its current legal and regulatory framework on consumer protection in e-commerce?

1.4 THESIS STATEMENT

The development of e-commerce in Nigeria is of great importance as it provides an enormous benefit to consumers, traders and the economy. In order to facilitate the growth of e-commerce in the country, consumer confidence is critical; consumer protection drives consumer confidence. This study argues that the lack of adequate protection for consumers under the extant laws and regulations has exacerbated unfair trading practices and eroded consumers' confidence in online transactions. This has also had the economic impact of undermining the growth of the sector.

1.5 JUSTIFICATION

The impressive growth of the internet and mobile connectivity in Nigeria has made the country a leading nation in e-commerce on the continent. Also, the COVID 19 Pandemic accelerated the use of online platforms for trade[29].

About 1.5%[30] of Nigeria's Gross Domestic Product (GDP) can be attributed to internet-related technologies and activities[31]. One major cause of this low percentage is the absence of consumer confidence.[32] Adequate consumer protection measures will increase consumer confidence and thereby cause exponential growth in the economy.

1.6 AIM AND OBJECTIVE OF THE STUDY

The of aim of this research is to examine the regulatory framework of e-commerce in Nigeria, mainly as it affects consumer protection and then proffer solutions in dealing with the legal problem.

1.7 LITERATURE REVIEW

Consumer protection under e-commerce is a developing area of law in Nigeria. Thus this study relies heavily on published articles by renowned Nigerian academics.

According to Ilobinso (2017),[33] the development of e-commerce in Nigeria offers enormous benefits to consumers, businesses and the economy. One of such benefits is that it connects buyers (consumers) and traders to an enormous marketplace where goods and services are advertised and sold devoid of the geographical barriers that usually inhibit physical trade. This virtual nature of trade is seen as both a benefit and a challenge as it has increased risks in trading. Thus, it is imperative to have robust legal frameworks to ensure adequate protection for the consumer. However, in his study, Ilobinso (2017) failed to identify what safeguards should be implemented

[29] United Nations Division on Trade and Development "*COVID 19 & E-commerce: A Global Review"* (2021) 5 dtlstict2020d13_en.pdf (unctad.org) (accessed 2 April 2021).
[30] International Trade Centre "*International E-commerce in Africa: The way forward" 2015 at 6* Microsoft Word - E-commerce_111215 (intracen.org) (accessed 5 April 2021).
[31] As above.
[32] A Boasiko "E-commerce development in Ghana/West Africa & Cyber security challenges" UNCTAD expert meeting on cyberlaw & regulation for enhancing e-commerce" E-commerce Development in Ghana/West Africa & Cyber Security Challenges (unctad.org) (accessed 5 April 2021).
[33] ILobinso (n4) 81-91.

in the extant legal frameworks. This study will focus on providing legal safeguards that can be put in place to ensure robust legislation for the protection of consumers under e-commerce.

Eze (2018),[34] on the other hand, identified the Cybercrimes Prohibition Act of 2015 as the only law that regulates online activities in Nigeria. However, it only regulates criminal acts/offences. Besides criminal acts, legislation is also needed to tackle contractual breaches and other civil breaches concerning e-commerce transactions. Therefore, Eze (2018) recommends that the UNCITRAL Model Law on e-commerce be adopted into domestic legislation to provide contractual and civil safeguards for consumers. However, the study failed to recognize that the model law only provides a foundation for consumer protection. It does not address specific issues that consumers face. Therefore, this study will focus on identifying key provisions that should be present in Nigeria legal framework to ensure that it adequately protects consumers.

Apart from the gaps in the legal framework, Nurrudeen, Yusof and Abdullahi (2017)[35] identified institutional deficiencies inherent in e-commerce space in Nigeria. For example, the Federal Competition and Consumer Protection Commission (the principal regulatory body for consumer protection in Nigeria) has no mandate to regulate e-commerce activities in Nigeria. This then puts consumers in a very difficult position as there is no authority available to address complaints and grievances.

The courts are another institution responsible for the enforcement of the rights of consumers and the resolution of disputes. However, the current judicial system in Nigeria is not ideal for the resolution of e-commerce disputes. First, litigation in Nigeria is costly and time-consuming. Also, purchases made online are of relatively small value. Thus, it would be a waste of time to seek redress through litigation.

Furthermore, due to the borderless nature of e-commerce, the seller and consumer may be in separate jurisdictions. Therefore, in the event of a dispute, the physical presence of both the seller and consumer would be needed; this then becomes problematic. While Nuruddeen, Yusof and Abdullahi (2017) recommended the small claims court to solve this problem, it failed to recognize ADR as a means of resolving disputes; ADR is easily accessible, it is also cheaper and faster. Therefore, this study intends to examine the current institutional framework for e-commerce in

[34] Gladys (n5) 24-37.

[35] M Nuruddeen, Y Yusof, and A Abdullahi "An examination of Judicial Mechanism of Protecting the Rights of E-commerce in Nigeria" (2017) 2 Journal of Governance and Development 6.

Nigeria and the suitability of the Alternative Dispute Resolutions mechanism for resolving disputes under e-commerce.

1.8 RESEARCH METHODOLOGY

This research uses a desktop-based research methodology. This entails the use of primary and secondary source materials. The primary sources of material consulted include the Nigerian legislation, international treaties and South Africa's laws on consumer protection in e-commerce.

In the Nigerian context, the following primary sources are used. The constitution, the Cybercrimes (Prohibition and Prevention) Act 2015, the Federal Competition and Consumer Protection Act 2016, the Central Bank Protection Framework for Banks and Other Financial Institutions 2016, the Nigerian Data Protection Regulation 2019 and the Consumer Code of Practice Regulations 2008. This research will also consult secondary sources such as books, policy reviews and reports from international organizations, journal articles, dissertations, newspapers and magazines.

The nature of this research is analytical and comparative. The analytical research method is used to examine the extant regulatory framework in Nigeria and identify its gaps and challenges. The comparative method is used to benchmark Nigeria's laws on consumer protection with South Africa's framework and then elicit lessons for Nigeria. This research chose South Africa because South Africa has successfully provided a robust regulatory framework for protecting consumers under e-commerce. In addition, Nigeria and South Africa are both leading economies in Africa; they are the leading giants of e-commerce on the continent and are both developing countries

1.9 OVERVIEW OF CHAPTERS

CHAPTER ONE

This chapter focuses on the introduction, research questions, and the aims and objectives of the thesis. It also outlines the literature review, research methodology and gives an overview of the content of each chapter.

CHAPTER TWO.

This chapter outlines the conceptual framework of the concept of e-commerce and the rationale behind consumer protection. Also, it identifies the issues consumers face in e-commerce transactions, such as privacy breaches, formation of contracts, deceptive trade practices, cybercrimes, jurisdiction, choice of law and effective dispute resolution mechanisms.

CHAPTER THREE

This chapter examines the global, continental and regional frameworks governing e-commerce and then draws out the key provisions that countries must have to achieve a robust consumer-driven regulatory framework

CHAPTER FOUR

This chapter scrutinizes the legal and regulatory framework governing consumer protection in commerce in Nigeria to determine whether it offers adequate protection for consumers or not.

CHAPTER FIVE

This chapter undertakes a comparative analysis of Nigeria's legal framework against South Africa, an equally leading giant on e-commerce within the continent. It also draws out that Nigeria could learn to improve its framework

CHAPTER SIX

This chapter concludes the study and proffers practical recommendations to improve Nigeria's current legal and regulatory frameworks for consumer protection in e-commerce.

CHAPTER TWO

CONCEPTUAL FRAMEWORK OF E-COMMERCE AND CONSUMER PROTECTION

2.1 INTRODUCTION

As discussed in chapter one, electronic commerce (e-commerce) is a by-product[36] of the growth of Information Technology globally.[37] Therefore, there is a need for this study to introduce the conceptual framework of e-commerce and consumer protection before delving into legal and institutional frameworks. Thus, this chapter will: (i) discuss the general concepts of e-commerce, its categories, features, advantages and disadvantages. (ii) examine the concept of consumer protection, and the United Nations Guidelines on Consumer Protection (iii) identify the attendant issues plaguing online consumers; and (iv) conclude with the need for a legal and regulatory framework to protect consumers under e-commerce.

2.2 THE CONCEPT OF E-COMMERCE

E-commerce is simply defined as the purchase, sale and advertisement of goods and services through the internet or any other network that uses electronic or similar media for distance Information exchange.[38] This includes the World Wide Web and other technologies such as emails, mobile phones, and social media.[39] Three distinct features of e-commerce separates it from traditional trading. They are as follows:

The virtual nature of e-commerce: E-commerce takes place in a virtual environment where the vendor and purchaser do not physically engage with each other; instead, computers are used to obtain about the product and vendor and the price and delivery methods.[40]

Absence of physical boundaries: E-commerce transactions are conducted irrespective of space, time or geography. Thus, transactions take place 24 hours a day, seven days a week and 365 days

[36] S Jayabalan "E-commerce & Consumer Protection: The Importance of Legislative Measures" (2012) 15 Journal of the National University of Malaysia 1 https://ejournal.ukm.my/juum/article/view/7523/3045 (accessed 20 September 2021).
[37] Joseph (n31) 42.
[38] African Union Convention on Cyber Security and Personal Data Protection, Article 1.
[39] International Trade Centre (n6).
[40] J.Binding & K. Purnhagen "Regulations on E-commerce Protection Rules in China and Europe compared –same but different (2011) 2 Journal of Intellectual Property, Information Technology & Electronic Commerce Law 187

a year without limitations. Also, transactions can take place between citizens of various countries at the same time[41].

Several actors: There are an array of actors involved in e-commerce transactions.[42] These include computer programmers who build and monitor the websites and applications, the website owner, the vendors who advertise their commodities on these sites, warehouse managers who store physical commodities and the consumer who purchases these goods. Other players include customer services operators who attend to complaints, financial technology companies or traditional banks responsible for regulating and securing payments, as well as logistics businesses who take care of transporting commodities where necessary.

2.3 CATEGORIES OF E-COMMERCE

There are four significant categories of e-commerce which are as follows:

Business-to-business (B2B): This involves e-commerce between enterprises[43]. This form of e-commerce encapsulates a range of commercial activities such as financial services[44], purchasing, inventory management[45], sales, advertising[46], payment and delivery systems[47] and customer service[48]

Business-to-consumer (B2C): This takes place between companies and consumers.[49] Here, businesses and consumers transact through e-commerce platforms.[50] Although consumers place orders virtually, sometimes the transactions are completed physically, especially for goods. Also, e-commerce websites catering for the needs of consumers offer complete flexibility in areas such as order placements, shipping methods, payment methods and cancellation of orders[51] where possible. Examples of B2C E-commerce models are Amazon, Alibaba and Jumia. This study is focused on B2C e-commerce as it is one of the fastest-growing types of e-commerce.[52] The global

[41] Binding & Purnhagen (n7)187.
[42] Binding & Purnhagen (n7)187.
[43] International Trade Centre *International E-commerce in Africa: The way forward (2015) 4* Microsoft Word - commerce_111215 (intracen.org) (accessed 21 May 2021)
[44] SA *Becker Electronic Commerce: Concept, Methodologies, Tools and Application* (2008) xxiv.
[45] SA Becker (n8) xxiv
[46] As above.
[47] As above.
[48] As above.
[49] International Trade Centre *International E-commerce in Africa: The way forward (2015) 4* Microsoft Word - E-commerce_111215 (intracen.org) (accessed 1 May 2021).
[50] SA Becker (n8) xxiv.
[51] As above.
[52] International trade centre (n6) 4

market value of B2C e-commerce is $4.01 trillion[53] as of 2021, and it is projected to increase to $7.6 trillion[54] by 2028. E-commerce activities for services under B2C usually operate by subscriptions to online service providers. Typical examples are subscriptions to online News platforms, Magazines, Journals, television and music streaming.

Consumer-to-consumer (C2C): These are e-commerce between consumers.[55] In the C2C E-commerce model, three[56] actors are majorly involved: a consumer selling a product or service, a consumer who is the buyer, and the e-commerce platform owner that connects the seller and the buyer[57]. Over the years, several C2C platforms have emerged, such as OLX, Bid or Buy in South Africa and Jiji in Nigeria.

Government-to-business (G2B): These are e-commerce transactions between a company and the government[58]; such transactions are usually in the form of electronic procurement.

There are other emerging areas of E-commerce, such as mobile commerce and social-commerce. mobile commerce (m-commerce) are online transactions conducted using mobile phones[59] and networks, while social commerce (s-commerce) takes place over social networking platforms[60] such as facebook and instagram.

2.4 ADVANTAGES OF E-COMMERCE

E-commerce provides enormous advantages to businesses, the economy and consumers.[61] Consumers enjoy numerous benefits under e-commerce as they can compare products with ease and have access to various choices all at once.[62] As a result of the access to a variety of products at a glance, competition ensues, leading to lower prices of commodities.[63] E-commerce has provided a platform for small and medium-sized enterprises to snowball. In addition, they have access to global markets at little or no cost[64]. In addition, e-commerce provides enormous benefits

[53] Grand View Research "Market Analysis Report" (2021) https://www.grandviewresearch.com/industry-analysis/b2c-e-commerce-market (accessed 20 September 2021)
[54] As above.
[55] International Trade Centre (n6) 4.
[56] Manzoor (n3)14.
[57] As above.
[58] International Trade Centre (n6)4.
[59] As above.
[60] As above.
[61] Manzoor (n3) 15.
[62] As above
[63] R Goel *E Commerce* (*2007) 11*
[64] E Turban, J White side, E King, J Outland *Introduction to Electronic Commerce and Social Commerce* (2017) 14.

to society at large; the lowered costs of production result in lower prices for consumers, more taxes for the government, and it has also created numerous job opportunities for the populace.

2.5 DISADVANTAGES OF E-COMMERCE

Despite the benefits e-commerce provides, there are several disadvantages; they are as follows: E-commerce presents the opportunity for ease and convenience; however, there are hidden costs for this convenience.[65] For instance, the delivery cost of online products is usually high, sometimes these goods do not have warranties, and the delivery terms may be unacceptable.[66] Also, due to many users on the internet daily, there is still the challenge of network failures.[67]In addition, e-commerce may not be appropriate for all types of businesses. For example, luxury items such as expensive art, diamonds and antiques would need inspection before purchase.[68] Also, due to the anonymity the internet provides, consumers are susceptible to the following: unfair trade practices, violation of data privacy, no delivery or late delivery, misrepresentation and even crimes such as identity theft, credit/debit card fraud, cyber-stalking and phishing. Before this study addresses the issues consumers face in e-commerce, it is crucial to examine the concept of consumer protection, its rationale, and the United Nations Guidelines on Consumer Protection.

2.6 CONSUMER PROTECTION

Consumer protection, in simple terms, is the promulgation of laws and regulations to protect consumers from exploitation and unfair trade practices.[69]Over the years, it has become necessary for governments to protect their citizens against unscrupulous business practices, there are several reasons for the government's intervention in the issue of consumer protection. These reasons are as follows:

First, businesses are superior to consumers when it comes to transactions as they possess higher knowledge and experience.[70] Also, companies are known to control the terms of contracts through standardised contracts, giving the consumer little to no room to negotiate[71]; this then makes it easy

[65]Goel (n9) 11.
[66] Goel(n9) 11.
[67] As above.
[68] TJ Talloo *Business Organization and Management* (2008) 52.
[69] CS Sitnikov. (2013) *Consumers' Protection*. In: SO Idowu, NL Capaldi, AD Gupta (eds) *Encyclopedia of Corporate Social Responsibility* (2013) 455.
[70] N Chawla & B Kumar "E-commerce and Consumer Protection in India: The Emerging Trend" (2021) Journal of Business Ethics at 6 https://doi.org/10.1007/s10551-021-04884-3 (accessed 1 August 2021).
[71] S Yuthayotin *Access to Justice in Transnational B2C E-commerce* (2014) 29.

for businesses to impose unfair terms on consumers. Hence, there is a need for government intervention to ensure that standardised terms do not contain strict, exploitative and oppressive terms[72]; this is achieved through the introduction of laws and regulations.[73]

Second, consumers have behavioural biases when it comes to the purchase of goods and services.[74] Businesses then take advantage of these behavioural biases.[75]A famous example is auctions sales, where vendors are likely to obtain better prices than ordinary sales. In an auction, a consumer bids higher than usual due to the fear of another person purchasing the commodity. Another example is in the use of discounts by vendors. Sometimes these vendors mislead the public that it is selling at a discounted price when it is selling at the regular price. The government has recognised that businesses must not diminish the consumers' ability to make informed decisions for selfish gains. Thus, laws and regulations are usually in place to prevent commercial practices targeted at altering consumer behaviour.[76]This research agrees with the above reasons for government intervention in the economic marketplace; science and technology have introduced complexities into the marketplace over the years. Consequently, consumers have little or no bargaining powers; this thereby informs the need of the government to intervene by creating a level playing field for both parties.

Third, governments can use consumer protection as a tool for poverty eradication and socio-economic justice, especially in developing countries.[77] Consumer protection helps to remove leakages in expenditures of low-income families, and it ensures that they get the fairest prices for their purchases; this is because the poor are often given inferior goods at a high cost compared to the rest of society.[78] President John F Kennedy, a former US President, was an avid advocate for consumer protection. In 1962, he delivered a "*Special Message to the Congress of the United States on Protecting the Consumer Interest",* and he thereby made the following remarks:

> *"…increased efforts to make the best possible use of their incomes can contribute more to the well-being of most families than equivalent efforts to raise their incomes".*[79]

[72] S Yuthayotin (n10) 29
[73] As above.
[74] As above.
[75] As above.
[76] As above.
[77] UNCTAD *Manual on Consumer Protection* (2016) 3 https://unctad.org/system/files/official-document/webditcclp2016d1.pdf accessed 13 August 2021
[78] As above
[79] JF Kennedy "Special Message to the Congress of the United States on the Protection of Consumers Rights" (1962)2

In 1968, the United States Federal Trade Commission carried out research that showed that low-income families pay significantly higher than the rest of the public. In the United Kingdom, a study showed a 40-year pattern where low-income consumers paid more for commodities. As a result of the realisation that consumer protection can be used to achieve redistribution of wealth, most countries have introduced this theme into their consumer protection law. Consumer protection as a tool for alleviating poverty is also present in target 10 of the Sustainable Development Goals (SDG). The objective is to *"reduce to 3% the transaction costs of migrant remittances and eliminate remittance corridors with costs higher than 5%.*[80]*"*

Fourth, the promulgation of robust laws in consumer protection benefits businesses, citizens, and society; thus, the government must curate sound legislation on the subject. President Kennedy, in his famous 1962 speech, clearly articulated the importance of consumer protection in the following words:

"Consumers, by definition, include us all. They are the largest economic group in the economy, affecting and affected by almost every public and private economic decision. Two-thirds of all spending in the economy is by consumers. However, they are the only important group in the economy that is not effectively organised whose views are often not heard.

We cannot afford waste in consumption any more than we can afford inefficiency in business or government. If consumers are offered inferior products, if prices are exorbitant, if drugs are unsafe or worthless, if the consumer is unable to choose on an informed basis, then his dollar is wasted, his health and safety may be threatened, and the national interest suffers.[81]*"*

President Kennedy further enumerated the rights consumers are to enjoy, which are:

a) The right to safety- consumers have a right to protection against dangerous goods (goods dangerous to health or life).[82]

[80]United Nations *Transforming our world: The 2030 Agenda for Sustainable Development* https://sustainabledevelopment.un.org/content/documents/21252030%20Agenda%20for%20Sustainable%20Development%20web.pdf (accessed 20 August 2021)
[81] Kennedy (n10)5.
[82] As above.

b) The right to be informed – Businesses must give consumers accurate facts and information concerning products and services to make informed decisions. Also, they must be protected against fraudulent or misleading advertising and marketing.[83]

c) The right to choose – consumers have the right to be assured of access to various goods at competitive prices where possible. In businesses where there is no competition, there must be an assurance that the quality of goods is satisfactory and fair.[84]

d) The right to be heard – consumers have a right to be assured that the government will consider their interests in formulating policies. Also, when it comes to enforcement of rights, consumers will be treated fairly.[85]

The General Assembly of the United Nations adopted these rights in 1985 as the United Nations Guidelines on Consumer Protection. Therefore, it is crucial to examine these guidelines as they serve as a foundation for the protection of online consumers under e-commerce.

2.7 THE UNITED NATIONS GUIDELINES ON CONSUMER PROTECTION

The United Nations Guidelines on Consumer Protection enumerates specific guidelines that members may incorporate into their laws on consumer protection; it also outlines the relevant institutions responsible for regulating consumer protection within a state's territory. These guidelines are as follows:

National Policies[86]

Countries are to formulate National Policies on consumer protection. These policies must ensure that it promotes good business practices[87], high standards of information disclosure, [88]fair contractual terms[89], effective dispute resolution mechanisms[90] and the protection of consumers privacy.[91]

[83] As above.
[84] As above.
[85] As above.
[86] United Nations Guidelines on Consumer Protection, Guideline 14.
[87] United Nations Guidelines on Consumer Protection, Guideline 14 (a).
[88] United Nations Guideline on Consumer Protection, Guideline 14(c).
[89] United Nations Guidelines on Consumer Protection, Guideline 14(d).
[90] United Nations Guidelines on Consumer Protection, Guideline 14 (g).
[91] United Nations Guidelines on Consumer Protection, Guideline 14(h).

Physical safety[92]

Countrie**s** should ensure that businesses adopt appropriate safety standards to ensure that the products are safe for their intended or reasonably foreseeable use.[93] Also, Members states must ensure that companies provide consumers with information on the appropriate use of the products and the risks involved in using the product.[94]

Protection of the economic interests of consumers[95]

Countries are to ensure that consumers get the best benefits from their financial resources.[96] Also, consumers must be protected against practices that can harm their economic interests.[97]

National Standards[98]

Countries are to formulate national standards that companies must comply with when producing goods or delivering services; these standards ensure that the goods and services are safe for consumption and of optimum quality.[99] Such measures must be in line with the global standards where possible.[100]

Distribution of Essential Goods and Services[101]

Countries are to create policies that ensure the efficient distribution of essential goods and services to consumers[102]. Governments should also develop specific guidelines for distributing critical goods and services to disadvantaged individuals and consumers.[103]

[92] United Nations Guidelines on Consumer Protection, Guideline 16.
[93] As above.
[94] United Nations Guidelines on Consumer Protection, Guideline 17.
[95] United Nations Guidelines on Consumer Protection, Guideline 20.
[96] As above.
[97] As above.
[98] United Nations Guidelines on Consumer Protection, Guideline 33.
[99] As above.
[100] United Nations Guidelines on Consumer Protection, Guideline 34.
[101] United Nations Guidelines on Consumer Protection, Guideline 36.
[102] United Nations Guidelines on Consumer Protection, Guideline 36 (a).
[103] As above.

Dispute Resolution Mechanisms[104]

Countries are to establish dispute resolution mechanisms that are efficient, affordable and accessible to the public.[105] Also, governments must ensure that businesses set up informal redress mechanisms that can quickly handle customer complaints and grievances.[106]

Information and Education Programmes[107]

Countries are to create and implement education programmes to enlighten consumers on their rights and duties[108]. Governments can do this by including consumer education into school curriculums[109] and the use of mass media[110] to educate the general public. Countries are also encouraged to partner with civil society groups[111] and businesses[112]in providing training programmes on consumer education.

E-commerce[113]

Countries are to create policies that enhance consumer confidence in e-commerce[114]. In formulating these policies, governments must ensure that the level of protection afforded to consumers under e-commerce must be no less favourable than that afforded to traditional commerce.[115]

Financial Services[116]

Countries are to create policies[117] to protect the assets of consumers by ensuring financial service businesses must provide measures for control of deposits[118] and the provision of insurance schemes to safeguard the assets of consumers. Countries must also ensure that there are regulators to ensure

[104] United Nations Guidelines on Consumer Protection Guideline 37.
[105] As above.
[106] United Nations Guidelines on Consumer Protection, Guideline 38.
[107] United Nations Guidelines on Consumer Protection, Guideline 42.
[108] As above.
[109] United Nations Guidelines on Consumer Protection, Guideline 43.
[110] United Nations Guidelines on Consumer Protection, Guideline 45.
[111] As above.
[112] United Nations Guidelines on Consumer Protection, Guideline 46.
[113] United Nations Guidelines on Consumer Protection, Guideline 63.
[114] As above.
[115] As above.
[116] United Nations Guidelines on Consumer Protection, Guideline 66.
[117] United Nations Guidelines on Consumer Protection, Guideline 66 (a).
[118] United Nations Guidelines on Consumer Protection, Guideline 66(c).

compliance with government policies.[119] In addition, government, in partnership with financial service firms, must provide financial education programmes to ensure financial literacy.[120]

2.6.2 The Challenge of the United Nations Guidelines on Consumer Protection

The above guidelines provide valuable tools for governments to develop their laws and regulations on consumer protection. However, the major challenge with these guidelines is that it is regarded as soft law; thus, member states are not obliged to follow its principles in preparing their laws on consumer protection.

Also, while the above guidelines recognise the need to protect consumer protection under e-commerce, they failed to provide specific provisions for how governments can sufficiently protect consumers online. Therefore, it is essential to identify the peculiar challenges consumers face under this platform to know how best to protect online consumers.

2.8 PROBLEMS CONSUMERS FACE IN E-COMMERCE

E-commerce has undoubtedly provided enormous benefits to consumers and businesses alike. These benefits include increased access to global markets, enhanced variety of products and lower costs for consumers, greater competition leading to better efficiency, and new business opportunities[121]. However, there are several legal issues in e-commerce that affect consumers. It is essential to discuss these issues as they will serve as critical indicators to determine the robustness of legal and regulatory frameworks on e-commerce. These issues are explained below:

2.8.1 Privacy Breaches

Under e-commerce transactions, consumers must fill in information such as name, address, credit or debit card details, gender, birth date, ID, address, phone number and email addresses, personal income, credit card/ debit card details, and other necessary information for the transaction. The collection of this information is used to confirm the authenticity of the consumer. In addition, the use of this information will enable businesses to provide better commercial service to the consumer. Thus, because of the amount of private information the consumer is supplying, it becomes pertinent to protect them as they are personal and confidential. Unfortunately, privacy

[119] United Nations Guidelines on Consumer Protection, Guideline 66 (b).
[120] United Nations Guidelines on Consumer Protection, Guideline 66(d).
[121] R Khare & G Rajvanshi "E-commerce & Consumer Protection: A Critical Analysis of Legal Regulation (2013) International Journal on Consumer Law and Practice 62.

breaches have become one of the most significant issues facing e-commerce today, as privacy invasion has been a prevalent factor.

Many e-commerce sites directly ask users for personal information through forms. However, many sites also record data about their users' browsing habits in addition to such information. This e-commerce website software matches this data with personal and demographic information to create a profile of user preferences. Privacy invasion usually occurs for two purposes, first to enhance customer satisfaction and to increase profitability. Businesses use the data collected to offer customers customised services or use them for "*web lining*", this is a situation where users are shown different prices based on the information submitted. Here, the user's profile will determine the price offered; wealthy users are charged more, while those who are not will be charged less. E-commerce sites equally use certain technologies to collect information from consumers. An example of this is "*Cookies"*. Cookies extract information as a consumer browses through the internet[122]. The e-commerce site usually sends these cookies to the consumer's computer, saving them on the hard drive. Thus, when a consumer revisits the E-commerce site, the site gets a notification. In addition, these cookies monitor the consumer's activities on the website by studying the consumer's preferences and shopping patterns[123]. Although these cookies can be disabled, e-commerce websites have ensured that consumers cannot surf through a website unless these cookies are accepted[124].

E-commerce websites use cookies for two purposes. The first purpose is to "*remember the user"*. Cookies present a unique feature that saves the passwords and usernames of consumers on the website for those that prefer not to type their user name and password each time they open the website[125]. However, the implication of this is that these cookies monitor the activities of the consumer. On the other hand, the vendor can use this opportunity to create a customised experience for the consumer; the consumer will get specific adverts and commodities peculiar to him[126]. Second, advertising agencies use cookies to collect the shopping patterns and preferences of

[122] S Velagapudi & H Gupta, "Privacy, Security of Cookies in HTTP Transmission" (*2019)* 4th International Conference on Information Systems and Computer Networks (ISCON) at 22 https://ieeexplore-ieee org.uplib.idm.oclc.org/document/9036289 (accessed 24 August 2021).
[123] H Liu & X Liu, "The protection of the privacy right in electronic commerce" (2012) 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet) at 691 doi: 10.1109/CECNet.2012.6201744. https://ieeexplore-ieee-org.uplib.idm.oclc.org/document/6201744 (accessed 23 August 2021).
[124] D Cabel, B Bilstad & K Enright "Consumer Privacy" (2000) Berman Online Lecture and Discussion Series Harvard Law School at 1 https://cyber.harvard.edu/olds/ecommerce/privacytext.html (accessed 24 August 2021)
[125] Cabel, Bilstad & Enright (n12) 1.
[126] Liu & Liu (n13) 691.

consumers[127]. Also, they contract with various E-commerce websites, and these cookies are used to trace a consumer's activities on different websites. The information gathered is then collated into a central database[128].

Another data collection technology used by e-commerce websites are "*Web bugs*[129]" or "*pixel tags*"[130]. These are invisible images that are fixed into web pages and "*HTML formatted emails*[131]. These bugs are used to monitor behaviour on various sites[132]. Unlike cookies that can be accepted or rejected, these bugs are presented as "*gifs*[133]" *or "a file object"*[134]. These bugs are also hidden in junk emails, and they are used to find out how many users visited their websites or read their emails[135]. Privacy is a fundamental human right, and companies must respect this right. Unfortunately, online enterprises have used the personal data gathered unscrupulously[136]. Data collection is referred to as "the new oil"; thus, some businesses have sold this information for profit or have exchanged this information with other enterprises for data analytics to enhance business operations and make more profits[137]. As a result of the above issues, consumers are usually skeptical about using E-commerce platforms.

2.8.2 Formation of Electronic Contracts

The formation of contracts is one of the main issues in e-commerce[138]. It is easy to determine when a contract comes into existence in traditional commerce as the rules of common law and statutes stipulate what amounts to a valid contract[139]. However, in e-commerce, contracts are usually virtual and borderless. Thus, it makes it difficult to determine when a valid contract has been formed. Although emails are likened to commercial transactions performed through postal correspondences, it has been challenging to determine how to place contracts concluded via

[127] Cabel, Bilstad& Enright (n12) 1.
[128] As above.
[129] J Dobias "Privacy Effects of Web Bugs Amplified by Web 2.0" In: F Hübner, S Duquenoy, P Hansen, M Leenes, R Zhang (eds) *Privacy and Identity Management for Life Privacy and Identity (2010)* 244 https://doi.org/10.1007/978-3-642-20769-3_20 (accessed 24 August 2021).
[130] Cabel, Bilstad & Enright (n12) 1.
[131] As above.
[132] J Dobias "Privacy Effects of Web bugs Amplified by Web 2.0" in F Hubner et al (n14) 244.
[133] Cabel, Bilstad & Enright (n12) 1
[134] As above
[135] J Dobias "Privacy Effects of Web bugs Amplified by Web 2.0" in F Hubner et al (n14) 244
[136] Liu & Liu (n13) 692
[137] As above
[138] Akomolede(n15)5
[139] Akomolede (n15)5

website trading, the most popular electronic commerce platform[140]. Under this, vendors display products on the website. The consumer scrolls through the site and indicates interest in a particular commodity or service by clicking on the item. This research will highlight the contractual issues associated with website trading below:

a) Electronic offer

In traditional commerce, an offer is an undertaking made by one party to the other with the intention that such an offer becomes binding on the other party when he accepts[141]. Such an offer should be precise and clear; also, it can be made to one person or the entire world[142]. However, where there is no intention to be bound by that offer, such an undertaking would be considered an invitation to treat[143]. For example, the display of goods in a physical shop is usually viewed as an invitation to treat[144]. Thus when the consumer picks up the item, this is considered to be the offer. The cashier accepts the offer by collecting the money and issues a receipt as proof of the contract. However, in e-commerce, the display and actual sale of the goods are often combined[145]; it then becomes difficult to determine what constitutes an offer and which party makes the offer. Apart from displaying items, there is also the controversial issue of whether web advertisements amount to offers or invitations to treat[146]. Therefore, it is pertinent for laws and regulations to stipulate clearly what constitutes an offer under an internet transaction and which party makes the offer.

b) Terms and conditions

E-commerce sites display items, and consumers browse through them—the consumer clicks on the item to place an order for the product. Once the consumer does this, a page titled "terms and conditions" usually pops up[147]. Here, the consumer is required to agree or disagree with these terms and conditions. E-commerce sites present these terms and conditions in three ways; "*shrink wrap*[148]*", "click wrap",* [149]*and "browse wrap*[150]*"*. In shrinkwrap agreements, the consumer cannot see the content of the terms and conditions until he agrees; this is commonly used to purchase

[140] Ilobinso(n4)54
[141] C Turner *Contract Law* (2014) 6
[142] Turner (n16)6
[143] As above.
[144] Ilobinso (n4)54.
[145] Akomolede (n4)5.
[146] Ilobinso (n4) 58.
[147] A Davidson *The Law of Electronic Commerce* (2009) 67.
[148] NS Kim *Wrap Contracts: Foundations & Ramifications* (2013) 36.
[149] Kim (n16) 39.
[150] Kim (n16) 41.

software packages[151]. The implication is that the contract would bind the consumer before reading the terms and conditions[152]. The clickwrap and browsewrap agreements seem to present better advantages to the consumer. In clickwrap agreements, the consumer is presented with the list of terms and conditions and can read it[153] before clicking on the icon marked "agreed[154]" or "accept[155]"; thus, access to the product is contingent on the buyer reading and accepting the terms and conditions. The problem is that buyers are forced to agree with these standard agreements as they do not have a choice, and ignorance will not be taken as a defence. In *Steven J Caspi v Microsoft Network*[156], the terms and conditions were placed in a position that denied the plaintiff access to the Microsoft Network until he assented to the terms and conditions. The US court held that the contract was enforceable as the plaintiff had given his consent.

On the other hand, in browsewrap agreements, the buyer has the option to read and agree with the terms of the contract[157]. Thus, the buyer's consent to the terms and conditions is not contingent on gaining access to the product[158]. The danger here is that it would be difficult to determine whether there was a "meeting of the mind", and once there is doubt as to consensus, it becomes difficult to enforce such an agreement. For example, in *Specht v Netscape Communications Corp*[159], the plaintiff could download Netscape's Software without agreeing to the terms and conditions as it was optional. The court held that the plaintiff was not bound to the terms as users were not required to give unequivocal consent to the terms and conditions.

2.8.3 Deceptive Trade Practices

The unique features of e-commerce, such as low entry barriers[160] and anonymity,[161] present an opportunity to perpetuate deceptive and unfair trade practices[162]. For instance, in traditional trade, a lot of money is required to set up a physical shop, and consumers can locate the business where

[151] D Shilling *Lawyer's Desk Book* (2018) 10.
[152] Davidson(n17)67.
[153] J Homle *Internet Jurisdiction Law and Practice* (2021) 338.
[154] Homle (n18)338.
[155] As above.
[156] Steven J Caspi v Microsoft Network 323 NJ Super 118 (1999).
[157] Davidson (n17) 70.
[158] Davidson (n17)70.
[159] Specht v Netscape Communications Corp (2001) 150 F. Supp. 2d 585.
[160] B Xiao & I Bonbasat "Product Related Deception in E-commerce: A Theoretical Perspective" (2011) 35 MIS Quarterly 170.
[161] Xiao & Bonbasat (n18) 170.
[162] J Braucher " Delayed Disclosure in Consumer E-commerce as an Unfair and Deceptive practice" (2000) 46 at 1806.

things go wrong because they have a physical address. However, in e-commerce, it is relatively easy to set up a website and display commodities. Thus, businesses can upload false information without the fear of facing the wrath of the law as it might be challenging to locate them physically. Typical forms of deceptive practices include misrepresentation[163], delivery of inferior goods[164], non-delivery or late delivery of goods[165], deliberate inadequate disclosure of refund policies, warranties and terms of cancellation[166], deliberately giving elusive information about the total cost of the transaction (tax, shipping and handling fees)[167] and the deliberate default on the contract[168]

On the other hand, businesses have developed several technologies to reduce risks associated with online marketplaces to curb these deceptive practices and boost consumer confidence in e-commerce. Unfortunately, unscrupulous companies have used this to exploit consumers. For instance, online marketplaces allow consumers to post reviews about products and commodities. However, businesses can pose as consumers by creating fake accounts to post biased reviews about their products to deceive consumers. Also, online marketplaces ensure that vendors with higher ratings can get higher prices for their commodities[169]. Vendors can equally manipulate such platforms to get high ratings to sell at higher prices.[170]

Another common trend is "delayed information disclosure"[171]. Timely disclosure[172] of important information and terms are essential to help consumers choose the fairest price for their purchases. Unfortunately, the internet has provided an opportunity for internet businesses to delay information. Some companies have created a culture where it is acceptable for consumers to become aware of essential terms that would have altered their decision to purchase the commodity after paying for it[173]. However, even where this information is displayed on the website, it is usually hidden in an obscure place[174] . When it is even located, the terms are written in long paragraphs with many legal terms difficult for an average person to understand[175]. This trend is

[163] Ilobinso (n4) 82.
[164] Xiao & Bonbasat (n18)170.
[165] Ilobinso (n24) 83.
[166] Braucher (n19) 1807.
[167] Goel (n7) 11.
[168] As above.
[169] As above.
[170] As above.
[171] Braucher (n19) 1807.
[172] Braucher (n19) 1806.
[173] Davidson (n18) 67.
[174] Braucher (n19) 1807.
[175] As above.

most popular amongst internet businesses that sell services and intangible products such as Software[176].

2.8.4 Cybercrimes

The rapid adoption of e-commerce globally has equally created an opportunity for cybercrime activities[177]. Cybercrime is defined as wrongful actions by internet users (usually organised groups) who gain unlawful access to computers and take advantage of vulnerable processor networks and the internet to commit crimes[178]. Such persons are referred to as "*hackers with malicious intent*[179]". E-commerce is like "candy" for hackers as it creates an avenue to cause harm both to businesses and consumers[180]. These crimes usually result in enormous losses for both parties[181]. Thus, while companies and consumers are excited about e-commerce's opportunities, they also have to worry about hackers[182]. Criminal activities on the internet include identity theft, credit/debit card fraud, fraudulent online sales, fraudulent electronic funds transfer, cyber-stalking, and phishing.

The prevalence of online crimes has made consumers sceptical about the use of e-commerce platforms such that wary consumers use e-commerce platforms to compare products and prices and then make purchases from physical stores[183]. However, innovative businesses are creating ingenious ways to mitigate cybercrimes. For instance, online marketplaces operate semi-virtual platforms whereby consumers have the option to make payment for purchases physically when goods are delivered[184]. However, while this seems like a good business model for products, it might not work for the purchase of services and intangible goods.

2.8.5 Jurisdiction, Choice of Law and Effective Dispute Resolution Methods

The issue of jurisdiction in e-commerce is filled with complexities[185]; this is usually due to its cross-border nature; this is because several countries with various legal systems are typically

[176] A Davidson (n18) 67
[177] S Munjai & A Ahere "Cybercrime Threats for E-commerce(2016) Social Science Research Network Electronic Journal at 3 https://publication/306401151_Cyber_Crimes_Threat_for_E-commerce (accessed 25 August 2021).
[178] R Apau, F Korantey & S Gyamfi "Cybercrimes and its Effects on E-commerce Technologies" (2019) 5 Journal of Information Technologies at 40.
[179] Davidson (n18) 339.
[180] Munjai & Ahere (n20) 3.
[181] Apau, Korantey & Gyamfi (n21) 39.
[182] Munjai & Ahere (n20) 3.
[183] D Ndonga" E-commerce in Africa: Challenges and solutions" (2012) 5 African Journal of Legal Studies 254
[184] Ndonga (n21) 255.
[185] Akomolede (n14)9.

involved in a single transaction[186]. Although some disputes in e-commerce might be resolved informally[187] by companies providing technical support platforms where customers can get refunds or have technical issues resolved, some disputes require formal dispute resolution mechanisms[188]. Where parties seek proper forums for dispute resolution raises the following questions: Which country has jurisdiction[189]? What court will be approached[190]? How will the judgment be enforced against a foreign defendant[191]? As a result, there is usually a conflict of interest between the vendors and the purchasers[192]. The vendors do not want to be sued in foreign courts, while the purchaser would prefer to take action in his home state[193].

Another pertinent issue in the resolution of e-commerce disputes is that of choice of law[194]. The complexities and trans-national nature of the internet make it difficult to apply the rule of a single jurisdiction[195]. Moreover, it is often impossible to determine which country's law is the most appropriate law to be used[196]. Consequently, the principles of private international law will be applied where these difficulties arise[197]. Generally, in practice, companies try to avoid the complexities of applying the principles of private international law by inserting the jurisdiction and choice of law clauses in the standard electronic contracts provided by them[198]. Thus when customers click on "agree", they are bound by those clauses. Unfortunately, the consumer is usually on the receiving end[199]. Since he is the weaker party, he will be subjected to a foreign forum with different laws and languages, which is ultimately stressful and costly[200].

Furthermore, there is equally the problem of effective mechanisms for the resolution of disputes. The pursuit of formal dispute resolution mechanisms such as litigation and arbitration is considered

[186] FF Wang *Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US & China* (2010) 17.
[187] S Jawahitha "Cyber Jurisdiction and Consumer Protection in E-commerce" (2005) 21 Computer and Law Security Report at 154.
[188] Jawahitha (n22) 154.
[189] As above.
[190] As above.
[191] As above.
[192] Wang (n21) 19.
[193] Wang (n21) 19.
[194] D Shaik & V Poojasree "Consumer Protection in E-commerce: A Legal and Compliance Framework for the Digital Market" (2020) 549 Advances in Social Science, Education and Human Research 20.
[195] Akomolede (n14) 10.
[196] As above.
[197] Davidson (n18) 183.
[198] Wang (n21) 19.
[199] Jawahitha (n22) 154.
[200] As above.

costly for Small & Medium Scale Enterprises[201] and Consumers alike because most e-commerce claims disputes claims are usually from low-value transactions.[202] Consumers would thereby prefer to purchase goods via traditional means. The above issues consequently have a hard-knock effect[203] on the growth of digital businesses.[204]

2.9 Conclusion

Above, the discussion provided insights into the concept of e-commerce and consumer protection. First, the research brought to light the concept of e-commerce and the rationale behind consumer protection. Second, it also examined the United Nations guidelines on consumer protection and revealed that it gives no specific guide to member states on how to address the peculiar challenges consumers face under e-commerce. Third, it identified consumers' issues in e-commerce, such as privacy breaches, formation of contracts, deceptive trade practices, cybercrimes, jurisdiction, choice of law and effective dispute resolution mechanisms. Overall, this chapter revealed that consumers are the weaker parties in e-commerce as they are at the mercy of businesses. Therefore, there is a need for the promulgation of robust laws and regulations to address these concerns.

[201] P Cortes & AP Ladder "Consumer Dispute Resolution Goes Online: Reflections on the Evolution of European Law for Out-of-Court Redress (2014) 21 Maastrict Journal of European & Comparative Law at 15.
[202] Ilobinso (n4) 82.
[203] Cortes & AP Ladder (n25) 15.
[204] As above.

CHAPTER THREE

INTERNATIONAL INSTRUMENTS ON CONSUMER PROTECTION UNDER E-COMMERCE

3.1 INTRODUCTION

The key objective of this study is to examine the legal and regulatory frameworks governing consumer protection in e-commerce landscape in Nigeria. Thus, it is pertinent to discuss the international instruments governing e-commerce as they will be used as a comparator to determine whether Nigeria's e-commerce laws robustly protect consumers. To this end, this chapter will (i) examine the global, continental and regional frameworks on e-commerce; (ii) outline the shortcomings or challenges in implementing these instruments; and (iii) conclude by drawing out key provisions that countries must have in order to achieve a robust consumer driven regulatory framework.

3.2 THE UNCITRAL MODEL LAW ON E-COMMERCE

The rapid growth of e-commerce in the early 1990s brought about bright prospects for the future of global trade. However, there were concerns that the following issues would stifle its growth: first, the existing traditional legal frameworks governing commercial activities did not recognise the peculiarities of digital trade[205] and secondly, the absence of harmonised laws on the subject of e-commerce posed a threat of irregularities and uncertainties.[206] In 1985, the working group on e-commerce under the UNCITRAL stated a need to formulate a harmonised set of laws that recognised digital forms of documents, signatures and writing, and other issues peculiar to e-commerce.[207] In 1992, the Working Group prepared a Model Law on e-commerce which the General Assembly adopted in 1996.[208]

[205] UNCTAD (n22) 302.
[206] T Pistorius "Contract formation: A comparative perspective on the Model law on electronic commerce" (2002) 35 Comparative and International Law Journal of Southern Africa 131 https://journals-co-za.uplib.idm.oclc.org/doi/10.10520/AJA00104051_178 (accessed 31 August 2021).
[207] UNCTAD (n22) 303 .
[208] M Nurudeen & Y Yusof "A Comparative analysis of the Legal Norms for E-commerce and Consumer. Protection"(2021) 26 Malaysian Journal of Consumers and Family Economics 22.

Countries were expected to use the model law as a guide in preparing their laws for the regulation of e-commerce.[209] Also, they were expected to modify the provisions to suit their socio-economic circumstances. In furtherance of this, a guide to the enactment of the model law was published. It contains background and explanations to each of the provisions in the model law.

3.2.1 OBJECTIVES OF THE MODEL LAW ON E-COMMERCE

The model law offers internationally acceptable rules to remove the legal impediments affecting online transactions to create a secure and predictable environment for e-commerce.[210] Also, the principles expressed in the model law are to aid users of e-commerce in drafting contractual solutions needed to overcome the legal impediments in e-commerce.[211] In addition, the model law seeks to remove the disparities in national laws[212]; this would further enable growth in the economy as it would serve as a platform for businesses to access the global markets[213]. It would also ensure efficiency in international trade[214]. Finally, it is essential to note that though this model law makes no explicit reference to consumers, it impliedly covers consumer protection. Its provisions serve as a foundation for protecting consumers in e-commerce due to its recognition and legalisation[215] of online transactions.

3.2.2 THE SCOPE OF THE MODEL LAW

The model law is divided into two parts. The first part covers e-commerce in general, while the second part covers e-commerce in specific areas. The Model law seeks to provide a predictable and safe legal environment for both businesses and consumers. Three essential principles are contained in the provisions of the model law and these are:

The functional equivalence principle[216] – Paper-based documents and electronic documents must be treated equally under the law.

The technology neutrality principle[217] – There must be no discrimination against different kinds of technology.

[209] UNCTAD (n22) 303.
[210] Guide to the UNCITRAL Model Law on E-commerce at 32.
[211] As above.
[212] As above.
[213] As above.
[214] As above.
[215] As above.
[216] Pistorius (n22) at 33.
[217] Pistorius (n24) 34.

Party autonomy principle[218]**-** Parties have the freedom to choose whom they contract with and the terms and conditions within which they would be bound.

3.2.3 Relevant provisions under the model law

Article 2 of the model law defines various e-commerce concepts such as data messages, electronic data interchange and information systems. However, it does not define e-commerce. The model law defines data messages as a means of information created, received, sent or stored by any electronic means, including but not limited to emails, telegrams, electronic data exchanges and telexes[219]. This means that the model law authenticates the various means of entering into online transactions such as emails, text messages, EDI, instant messages, telephone and web trading. Article 4 of the model law makes provision for party autonomy; it provides that parties involved in electronic transactions are allowed to vary specific provisions of the model law such as formulation of contracts, recognition of parties, time, place and dispatch of data messages.

The model law embodies the principle of non-discrimination; it provides that electronic information will not be denied validity solely because it is not paper-based.[220] The model law further states that even where terms and conditions are not expressly stated in a data message, as long as references were made to such terms and conditions, they must be treated as though they were explicitly contained in the data message.[221]

The model law also takes note of the issues of signatures and the concept of originality. It prescribes that electronic signatures must be considered valid signatures where it meets the following requirements.[222]First, the method of signature used must identify the party[223] and secondly, such method must also indicate the party's approval of the electronic information

[218] C Connolloy & P Ravindra "First UN Convention on ecommerce finalised" (2006) 22 Computer Law & Security Report at 32 https://wwwsciencedirectcom.uplib.idm.oclc.org/science/article/pii/S026736490500186X (accessed 31 August 2021).
[219] UNCITRAL Model Law on E-commerce 1996, Article 2.
[220] UNCITRAL Model Law on E-commerce 1996, Article 5.
[221] UNCITRAL Model Law on E-commerce 1996, Article 5*bis.*
[222] UNCITRAL Model Law on E-commerce 1996, Article 7.
[223] As above.

content.[224] On the issue of originality, the model law prescribes that a data message is considered an original document where there is an assurance of the integrity[225] and authenticity of the information. This assurance can be provided by showing that the data is void of omissions and alterations.[226]In addition, the model law equally addresses the issue of admissibility[227] and the evidential weight[228] of data messages. It prescribes that data messages should not be denied admissibility[229] because it is not a paper-based document. Also, evidential weight must be given to data messages[230] (this depends on whether they were created, transmitted, communicated or stored reliably[231]).The formation and validity of contracts under online transactions have been a topic of debate. To create some form of certainty, it provides that offers and acceptance communicated through the means of data messages are regarded as valid contracts.[232] However, the model law did not definite what constitutes a good contract, neither did it define what amounts to an offer and acceptance; this is to prevent a conflict with the definitions given to the concept of offers and acceptance by various jurisdictions.[233]

The model law recognises that the peculiarities of e-commerce transactions might make it difficult to determine the time and place when the information was sent and received.[234] Thus it provides that the time and place of dispatch is determined by the principal place of business for both parties and not the location of computer systems.[235]The principle of neutrality can be seen throughout the provisions of the model law. It placed no form of technology above the other, neither did it exclude any form of technology.[236] It impliedly created room for the inclusion of future technologies by not giving a conclusive definition to data messages, as seen in Article 2.

[224] As above.
[225] UNCITRAL Model Law on E-commerce1996, Article 8.
[226] Guide to the Enactment of the UNCITRAL Model law on E-commerce (1996) 42.
[227] UNCITRAL Model Law on E-commerce 1996, Article 9.
[228] As above.
[229] As above.
[230] As above.
[231] Guide to the Enactment of the UNCITRAL Model Law on E-commerce (1996) 43
[232] UNCITRAL Model Law on E-commerce 1996, Article 11.
[233] Guide to the Enactment of the UNCITRAL Model Law on E-commerce (1996) 48.
[234] Guide to the Enactment of the UNCITRAL Model Law on E-commerce (1996) 55.
[235] UNICTRAL Model Law on E-commerce, Article 12.
[236] Nuruddeen & Yusof (n23) 27.

3.3 UNCITRAL MODEL LAW ON ELECTRONIC SIGNATURES

The UNCITRAL model law on e-commerce was a huge success as several countries enacted its provisions into their national legislation[237]. However, the increased use of electronic signatures in e-commerce called for the need to create a separate legal framework on digital signatures[238]; this was because countries soon realised that the growth of e-commerce was hinged on the provision of a legal structure for the authentication of digital signatures.[239] Thus, in 2001, the General Assembly adopted the model law on electronic signatures.

The model law on electronic signatures builds on Article 7 of the Model Law on E-commerce[240]. It creates a robust set of uniform rules on the legal structure for authentication of digital signatures[241] and the legal effects of using these technologies.[242] It also makes rules for the status of third-party service providers.[243]

3.4 SHORTCOMINGS OF THE UNCITRAL MODEL LAWS

The model laws only serve as guides for countries in enacting their local laws on e-commerce[244]; they have no force of law. Thus, the non-binding nature of these UNCITRAL model laws makes it easy for states to pick and choose specific provisions to enact in local rules.[245] This then reduces uniformity and harmonisation in e-commerce laws globally.[246]

Also, these model laws provide a foundation for the protection of consumers as they authenticate electronic contracts and signatures. However, they do not provide sufficient consumer protection provision; they do not address most of the problems consumers face in e-commerce, such as unfair trade practices, privacy and fraud, and the liabilities of various parties.[247] The model laws equally

[237] Guide to the Enactment of the UNCITRAL Model Law on Electronic Signatures 7.
[238] As above.
[239] UNCTAD Information Economy Report (n24) 302.
[240] Guide to the Enactment of the UNCITRAL Model Law on Electronic Signatures at 7.
[241] UNCTAD Information Economy Report (n24) 302.
[242] Guide to the Enactment of the UNCITRAL Model Law on Electronic Signatures 8.
[243] As above.
[244] Connolloy & Ravindra (n25) 32.
[245] UNCTAD Information Economy Report (n24) 301
[246] Connolloy & Ravindra (n25) 32.
[247] AM Nadal & JF Gomila "Comments to the UNCITRAL Model Law on Electronic Signatures" (2002) 5th International Conference on Information Security 241.

do not provide for the institutional frameworks governing e-commerce nor mention mechanisms for dispute settlement and remedies available to aggrieved parties[248].

3.5 UNITED NATIONS GUIDELINES ON CONSUMER PROTECTION IN E-COMMERCE (UNCGP)

The UNGCP guidelines, as explained in chapter two, provides rules and procedures countries may wish to follow when promulgating laws on consumer protection. In addition, guidelines 63-65 provides a guide for countries on consumer protection in e-commerce. The guidelines state that countries should build consumer confidence in e-commerce by developing clear and effective policies that adequately protect consumers.[249] Such protection offered to consumers must be no less favourable than those offered to consumers in other types of commerce.[250] Also, countries should review their current consumer laws to accommodate the peculiarities of e-commerce and ensure that consumers and businesses are educated about their rights and obligations in electronic transactions[251].

This study finds that the above provisions are vague as it did not provide any specific guidance to member states on how to deal with the peculiar challenges of online consumers. On the other hand, the UNGCP endorses the guidelines provided by the Organisation of Economic Cooperation and Development (OECD) as standards that countries may wish to incorporate in their consumer laws on e-commerce[252], this guideline provided by the OECD is quite detailed. Therefore, it is pertinent to examine the provisions of the OECD guidelines to determine whether they fully covers all areas affecting online consumers. The relevant provisions of these guidelines are enumerated below:

3.6 OECD GUIDELINES FOR CONSUMER PROTECTION IN THE CONTEXT OF E-COMMERCE

The OECD is an international organisation that creates policies in various fields to improve the quality of human lives. It created guidelines for consumer protection in online business-to-consumer transactions due to the absence of international standards in this significant area. The

[248] Nuruddeen & Yusof (n23) 30.
[249] United Nations Guidelines on Consumer Protection, Guideline 63.
[250] As above.
[251] United Nations Guidelines on Consumer Protection, Guideline 64.
[252] United Nations Guidelines on Consumer Protection, Guideline 65.

objective of the guideline are to create a minimum standard of protection to be afforded to consumers online. These guidelines have played a significant role in assisting governments in providing rules to protect consumers online without building barriers to trade.

3.6.1 Relevant Provisions of the Guidelines

The OECD enumerates eight principles that serve as minimum considerations that countries should consider in formulating regulations to protect digital consumers. These principles are summarised below.

- **Transparent and Effective Protection**

  Governments should create policies that are transparent and efficient[253]. In providing such policies, insights from behavioural economics should be taken into consideration[254]. Also, vulnerable consumers such as children and the disadvantaged in society should be considered[255].

- **Fair Business, Advertising, and Marketing Practices**

  Governments should ensure that businesses must adhere to fair business, advertising and marketing practices. Also, businesses engaged in e-commerce should pay due regard to the interests of consumers. The relevant provisions of this principle will be summarised in the following paragraphs:

  First, businesses must not make deceptive, fraudulent or misleading representations, whether expressly or impliedly, through words, pictures, audio or videos. They should also state disclaimers clearly, and they should be placed boldly on the part of the screen where they can easily be seen[256]. Second, businesses should refrain from using unfair contractual terms[257]; they must also refrain from limiting the consumer's abilities to make negative reviews about their products or services, contest unwarranted charges or file complaints with the governments or specialised agencies[258].

[253] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 1
[254] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 2
[255] As above
[256] OECD Guidelines for Consumer Protection in the Context of E-commerce 2016, Guideline 3
[257] OECD Guidelines for Consumer Protection in the Context of E-commerce 2016, Guideline 6
[258] OECD Guidelines for Consumer Protection in the Context of E-commerce 2016, Guideline 12

Third, businesses must ensure that the advertisements are not fraudulent and misleading[259]; the advert's content must be consistent with the product's features and usage[260]. Also, Adverts must show the total cost of a product or service[261]. They must take special care when it comes to the advertisement targeted at children or vulnerable consumers[262]. Businesses must, in appropriate circumstances, allow the consumer to withdraw from a transaction[263].

Fourth, businesses should not take advantage of the unique features of e-commerce to hide their identity or location or evade compliance with consumer protection regulations and enforcement measures.[264] Lastly, they should also use simple procedures that provide the consumer with the option of not receiving unsolicited emails. When consumers have chosen not to get such emails, their choices should be respected[265].

- **Online disclosures**

Businesses are required to provide sufficient information about themselves, the goods and services and the transaction itself. These components will be explained below:

- **Information about the business**

The guideline stipulates that online disclosures should be crystal clear, correct and easily accessible so that consumers have ample information to make decisions[266]. Also, the language of such disclosures must be plain and simple[267]. In providing necessary information, businesses should equally consider the technological limitation or notable features of various devices or platforms[268] (for example, businesses should take cognisance of the wide use of mobile phones with small screens).Businesses are to provide the following information about themselves: the legal name of the business as well as the name it trades with, its physical address, telephone number or other forms of electronic contact[269], appropriate domain names for websites as well

[259] OECD Guidelines for Consumer Protection in the Context of E-commerce 2016, Guideline 17
[260] OECD Guidelines for Consumer Protection in the Context of E-commerce 2016, Guideline 15
[261] OECD Guidelines for Consumer Protection in the Context of E-commerce 2016, Guideline 16
[262] OECD Guidelines for Consumer Protection in the Context of E-commerce 2016, Guideline 18
[263] OECD Guidelines for Consumer Protection in the Context of E-commerce 2016, Guideline 19
[264] OECD Guidelines for Consumer Protection in the Context of E-commerce 2016, Guideline 21
[265] OECD Guidelines for Consumer Protection in the Context of E-commerce 2016, Guideline 22
[266] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 25
[267] As above
[268] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 27
[269] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 29

any pertinent government licence[270]. Businesses should also provide information on relevant memberships, self-regulatory bodies, or dispute resolution organisations that it belongs[271].

- **Information about the goods and services**

Businesses should provide consumers with sufficient information on their goods and services[272]. Such information must contain the following: key functions, technical requirements that might limit the consumer's ability to use the product, health and safety information, and any age restrictions[273].

- **Information about the transaction**

Businesses should inform consumers about terms and conditions[274]. These terms and conditions should contain information such as the initial price of commodities, fixed charges, optional charges, payment methods, recurring charges, automatic renewals and subscriptions, terms of delivery, conditions for termination or cancellation of purchase, after-sale services, refunds, exchanges, warranties, privacy policies and dispute resolution methods[275].

- **Confirmation process of transactions**

Businesses must ensure that the confirmation process for transactions are straightforward, especially when a new payment mechanism is introduced[276]. Businesses should afford consumers summary product information and the price and delivery costs before consumers are asked to confirm the transaction.[277] There should also be an opportunity for consumers to correct errors, adjust or cancel the transaction before completion of the transaction process[278].In addition, transactions should not be processed unless the consumer has given express, informed consent[279]. Businesses should provide consumers with a complete, accurate

[270] As above
[271] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 30
[272] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 31
[273] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 32
[274] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 33
[275] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 34
[276] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 36
[277] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 37
[278] As above
[279] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 38

and durable electronic receipt that confirms the completion of transactions. Such receipt must be in a format compatible with various devices[280].

- **Payment**

Businesses should provide consumers with payment mechanisms that are secure and easy to use. The security measures must protect consumers from payment-related risks such as identity theft, privacy breaches and fraud[281]. Governments and stakeholders should collaborate to formulate minimum standards for the protection of consumers for e-payments[282].

- **Dispute resolution mechanisms and redress**

Government should ensure that consumers have access to fair, transparent and effective measures to resolve disputes. Dispute resolution methods should include out-of-court mechanisms such as alternative dispute resolution (ADR) and internal complaint systems by businesses[283]. These internal complaint systems must be accessible and provide an opportunity for consumers to engage with the businesses directly, in an informal manner, at the earliest time possible[284]. The government should ensure that consumers have access to ADR mechanisms, including Online Dispute Resolution Systems to facilitate disputes on low value or cross border e-commerce transactions. ODR is currently being used in the European Union[285] for e-commerce disputes and other countries are already considering incorporating it into their e-commerce regimes. To this end, the UNICTRAL Working Group Three[286] is already working on a model law that will govern online dispute resolution for cross border e-commerce disputes. These mechanisms must be fast and affordable, objective, impartial and must not create any unnecessary burden on the consumer[287]. Subject to the applicable law in each jurisdiction, the use of out-of-court mechanisms should not preclude consumers from pursuing other forms of dispute resolution and redress[288]. Businesses should provide

[280] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 39
[281] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 40
[282] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 41
[283] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 43.
[284] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 44.
[285] Council Directive 2013/11/EU of 21 May 2013 on Alternative Dispute Resolution for Consumer Dispute.
[286] UNCITRAL Working Group Three "Online Dispute Resolution for Cross Border E-commerce Disputes: Draft Outline Document Reflecting Elements and Principles for ODR Process" https://undocs.org/en/a/cn.9/wg.iii/wp.140 accessed 30 September 2021.
[287] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 45.
[288] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 43.

appropriate redress where the consumer has suffered damages, for example, defective or substandard goods, late or no delivery. In addition, governments and stakeholders are to deliberate on how to provide redress to consumers in situations involving non-monetary transactions[289] such as gifts or services given to consumers. Government should ensure that consumer protection agencies or self-regulatory organisations have the authority to take action and obtain redress on behalf of consumers, including monetary compensation.[290]

- **Privacy and security**

Businesses should protect consumers' privacy and use lawful, transparent, and fair methods to collect and store data.[291] Businesses should also take security measures in the protection of data in order to mitigate risks.[292]

- **Education, awareness and digital competence**

Government and stakeholders should work together to educate businesses and consumers on consumer protection in the context of e-commerce. Such education should include knowledge on the rights and obligations of both parties at the local and cross border levels.[293] They should work together to develop the digital proficiency of consumers through education and awareness programmes; this will equip consumers with the requisite knowledge and skill to participate in e-commerce. The programme should be tailored to meet the needs of specific groups and consider factors such as age, income and literacy.[294]

[289] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 46.
[290] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 47.
[291] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 47.
[292] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 48.
[293] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 50.
[294] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 51.

- **Other relevant provisions of the OECD guidelines**

The OECD guidelines provide principles government should consider in implementing policies on consumer protection under e-commerce. The guideline also outlines provisions on global cooperation. These aspects will be discussed below:

In formulating policies on consumer protection in e-commerce, governments and stakeholders should use empirical research data on consumer complaints. In addition, in adopting laws for e-commerce, the government should consider the principle of technology neutrality[295] as enunciated in the UNCITRAL Model Law on E-commerce. Also, the government should establish or make use of existing consumer protection enforcement agencies that will investigate and take action to protect consumers from fraudulent and unfair trade practices perpetuated both locally and internationally. These agencies must have also the requisite technical expertise to implement their powers effectively.[296] Furthermore, to provide consumers with effective protection in the global context, governments should enable communication and cooperation amongst themselves, and where possible, develop joint initiatives[297]. Also, to achieve such cooperation, governments should use existing global networks to enter into multilateral/bilateral arrangements[298].

3.6.2 Challenges to the implementation of the OECD Principles on consumer protection in e-Commerce.

The OECD guidelines provide a robust and comprehensive framework for the consumer protection in e-commerce. It covered all the pertinent issues facing consumers under e-commerce. It even further emphasised the need for legal frameworks and institutional frameworks (regulatory agencies and the courts) to ensure consumers are adequately protected. However, just like the model laws, the OECD guidelines only serve as a guide to assist countries in formulating their laws. Thus countries may choose not to implement its provisions. Also, the members of the OECD are primarily developed countries; thus, there is a perception that their guidelines might be too advanced for developing countries. However, the provisions of the guidelines as outlined above are not complex; the UNGCP endorsed these guidelines;

[295] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 53(ii).
[296] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 53(iii).
[297] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 54(i).
[298] OECD Guideline for Consumer Protection in the Context of E-commerce 2016, Guideline 54(iii).

thus, it means that developing countries can equally benefit from the use of the guidelines. Furthermore, the OECD guidelines introduced online dispute resolution, particularly for cross border e-commerce or transactions of low value. This research finds that the guidelines should have elaborated on this concept to give countries a sense of what a sound ODR mechanism entails.

3.7 THE AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION

Nigeria is a member of the African Union. Thus, this study needs to examine the relevant frameworks covering e-commerce at the continental level. Over the last 20 years, there has been a rapid growth of internet penetration on the continent.[299] As a result, the African Union (AU) saw the need to establish a continental treaty on cyber security and data protection. The Convention on Cyber Security and Personal Data Protection Convention was established in June 2014.[300] The Convention covers the subject of e-commerce, cyber security and personal data protection. Unfortunately, this Convention has not come into force as it requires 15 countries to ratify its provisions. Only eight countries (Angola, Ghana, Guinea, Mozambique, Mauritius, South Africa, Senegal and Rwanda) have ratified this convention.[301] However, for this study, it is pertinent to examine its relevant provisions.

3.7.1 Relevant provisions of the convention

Under the convention, member states are obligated to ensure that e-commerce activities can be freely exercised in their territories except gambling, legal services and activities of notaries[302]. Also, member states must ensure that businesses engaged in e-commerce within their territories must give consumers easy and direct access to the following information:[303] the corporate name of the business, the principal address, emails, phone numbers, relevant government licences, member organisations etc. In addition, businesses must state clearly the prices of commodities includes taxes and delivery fees.[304]

[299] U Orji "The African Union Convention on Cyber Security: A Regional Response towards Cyber Stability (2018) 12 Masaryk University Journal of Law and Technology 117.
[300] Orji (n29) 112
[301] Orji (n29) 112
[302] African Union Convention on Cyber Security and Personal Data Protection, Article 2(1).
[303] African Union Convention on Cyber Security and Personal Data Protection, Article (2).
[304] African Union Convention on Cyber Security and Personal Data Protection, Article 2(2)(a)(b)(c).

The convention recognises the use of electronic contracts as a valid means of contracting between parties[305]. However, the terms and conditions laid out by businesses must be in tandem with the domestic laws of member states[306]. Also, under the act, it provides that for an electronic contract to be validly concluded, the "offeree" must have had the opportunity to verify the order, particularly the price, on the other hand, before confirming the order, businesses must then confirm receipt of the order without unjustifiable delay.[307] The acceptance of the offer and the acknowledgement of the receipt are deemed to be received when the party it was addressed to has received them[308]. Thus this provision means that businesses are the ones who make an offer, and the consumer accepts by placing an order. In order to ensure security in payments, the convention stipulates that businesses must use payment methods approved by the member state[309].

Each state must establish legislation to protect consumers' data and punish any violation of such privacy. [310] In addition, the convention mandates each state to establish an authority in charge of protecting personal data. This authority must be independent and ensure that the personal data is processed in line with the provisions of the convention.[311] The authority must also ensure that the use of information communication technologies must not impede the freedom and privacy of citizens.[312]Citizens equally have rights under the convention when it comes to processing their data; they have the right to know who is processing their data purpose for which it is being processed and what period the data would be stored in their database.[313] Citizens also have the right to object to the processing of their personal information.[314] The convention requires each state to develop laws and regulations on cyber security.[315] These laws must contain the following provisions: laws on cybercrimes[316], the establishment of a regulatory authority[317] or empowering

[305] African Union Convention on Cyber Security and Personal Data Protection, Article 5(1).
[306] African Union Convention on Cyber Security and Personal Data Protection, Article 5(2).
[307] African Union Convention on Cyber Security and Personal Data Protection, Article 5(3).
[308] African Union Convention on Cyber Security and Personal Data Protection, Article 5(4).
[309] African Union Convention on Cyber Security and Personal Data Protection, Article 7 (1).
[310] African Union Convention on Cyber Security and Personal Data Protection, Article 8(1).
[311] African Union Convention on Cyber Security and Personal Data Protection, Article 11(a)(b).
[312] African Union Convention on Cyber Security and Personal Data Protection, Article 12 (1).
[313] African Union Convention on Cyber Security and Personal Data Protection, Article 16.
[314] African Union Convention on Cyber Security and Personal Data Protection, Article 18.
[315] African Union Convention on Cyber Security and Personal Data Protection, Article25.
[316] African Union Convention on Cyber Security and Personal Data Protection, Article 25(1).
[317] African Union Convention on Cyber Security and Personal Data Protection, Article 25 (2).

pre-existing authorities to regulate cyber security in the state[318], rights of citizens and the protection of sensitive sectors in the state.[319]This convention enhances cyber security awareness amongst member states. It facilitates the harmonisation of cyber security and data protection laws in Africa. In addition, it also enforces an array of progressive obligations on member states to establish national cyber security and data protection regimes.[320] There are, however, challenges of implementing this treaty which will be discussed below.

3.7.2 Challenges of implementing the convention

The convention does not fully establish a model legal framework that member states can adopt. It merely provides a guide for African countries to establish legislation for electronic transactions, cyber security and personal data protection[321]. This study finds that the above explains the slow ratification of this convention by African countries. Although there are already several international model laws on cyber security and personal data protection, the problem is that African states would adopt various versions on this subject; this will defeat the aim of this convention, which seeks to harmonise cyber security laws across Africa[322]. Apart from this, there is still a lack of cyber security awareness in several African countries and the lack of institutional capacity in this area; many enforcement authorities lack the requisite capacity to detect, investigate, and prosecute cybercrimes[323]. However, this is majorly caused by the reluctance of the government to create awareness and build the requisite expertise in this area. Although this study finds that the lack of awareness can be solved regionally, most African countries belong to regional blocs. Thus, in each regional bloc, some countries are more technologically advanced than others; for example, South Africa, Kenya, Nigeria and Egypt can assist other countries within their regional blocs. Furthermore, the provision on factors that determine the validity of online contracts is problematic because countries like Nigeria follow the common law approach to the definition of contract and under the common law, display of goods are regarded as an invitation to treat[324], thus it is consumer

[318] African Union Convention on Cyber Security and Personal Data Protection, Article 25(3).
[319] African Union Convention on Cyber Security and Personal Data Protection, Article 25 (4).
[320] U Orji "The African Union Convention on Cyber Security: A Regional Response towards Cyber Stability (2018) 12 Masaryk University Journal of Law and Technology 117.
[321] U Orji "Examining Missing Cyber Security Governance Mechanisms in the African Union Convention on Cyber Security and Personal Data Protection" (2014) 15 Computer Law Review International 132.
[322] Orji (n28) 133.
[323] Orji (29) 119.
[324] This principle was determined in the case of *Pharmaceutical Society of Great Britain v Boots Cash Chemists (Southern) Ltd* [1953] EWCA CIV 6.

that makes the offer by placing an order while the vendor accept the offer by acknowledging the order.

3.8 ECOWAS AGREEMENTS ON THE REGULATION OF INTERNET ACTIVITIES

Nigeria is located in the Western part of Africa, and it is a member of the Economic Community of West African States (ECOWAS). Thus it is pertinent to examine the extant frameworks regulating e-commerce. Due to the steady growth of electronic transactions, particularly in trade, payments, and mobile bank transfers within the West African region, the member states adopted three supplementary Acts to regulate ICT activities within the region; they are as follows:

- Supplementary Act A/SA.2/01/10 on Electronic Transactions
- Supplementary Act A/SA.1/01/10 on Personal Data Protection
- Directive C/DIR/1/08/11 of the 19th day of August 2011 on Cybercrime

3.9 ECOWAS SUPPLEMENTARY ACT ON ELECTRONIC TRANSACTIONS

The Heads of State and Government of the ECOWAS adopted the Supplementary Act A/SA.2/01/10 on Electronic Transactions as a regional legal framework to govern electronic transactions within the region.[325] The Act applies to all electronic transactions that make use of data messages.[326] Just like the AU Convention on cyber security, this Act does not apply to gambling, legal representation and activities of notaries public.[327] The Act also mandates businesses to ensure that consumers have direct and easy access to information such as the name and physical address of the business, emails, member organisations, relevant government licences[328], and an indication of accurate prices for the commodity.[329] In addition, the Act prohibits businesses from sending unsolicited electronic advertisements to consumers.[330]

The Act recognises that negotiations of contracts can take place electronically.[331] Also, the Act permits parties to electronically transmit all information necessary for the execution of the contract where they agree to do so[332]. In the determination of a valid contract, the act takes the same

[325] Supplementary Act A/SA.2/01/10 on Electronic Transactions, Article 2.
[326] As above.
[327] Supplementary Act A/SA.2/01/10 on Electronic Transactions, Article 3.
[328] Supplementary Act A/SA.2/01/10 on Electronic Transactions, Article 4.
[329] Supplementary Act A/SA.2/01/10 on Electronic Transactions, Article 5.
[330] Supplementary Act A/SA.2/01/10 on Electronic Transactions, Article 11.
[331] Supplementary Act A/SA.2/01/10 on Electronic Transactions, Article 15.
[332] Supplementary Act A/SA.2/01/10 on Electronic Transactions, Article 16.

approach as the AU Convention, it refers to consumers as recipient of the offer, and when the consumer has reviewed the order, especially the price, the confirmation of his order amounts to an acceptance[333]. This means that the business makes the offer through its display of goods, while the consumer accepts the offer by confirming the order. Also, The Act compels them to provide consumers with the terms and conditions of the electronic contract in a way that can be recorded and reproduced.[334] Such terms must contain the following: the language proposed for executing the contract[335], the various steps required to conclude the contract electronically[336], how the consumer can identify errors made when entering data, and how such errors can be corrected before the conclusion of the contract.[337] In addition, businesses are obligated to acknowledge receipt of a consumer's order without unnecessary delay[338]. Once these factors are met, this means that a valid contract has come into existence.

Under the Act, both electronic and physical documents are granted the same legal status. The Act permits electronic documents to be accepted for invoicing the same way hard copies are accepted[339]. Electronic documents are also admissible as evidence in court[340]. The Act equally permits the use of electronic signatures for online transactions[341]. However, for an electronic signature to be recognised, the signature must have been created by a secure device under the exclusive control of the party making the signature[342].

3.9.1 Shortcomings of the Supplementary Act Electronic Transactions

While this Act contains comprehensive provisions, some pertinent provisions are still missing, such as provisions on the time and price for dispatch of data messages, unfair trade practices, the institutional framework for regulating electronic transactions, dispute resolution mechanisms, and remedies available to consumers. While member states might fill these gaps in their respective laws, this essay believes that these are pertinent areas that also require harmonisation amongst member states to avoid discrepancies. Although this Act has not been ratified by any member

[333] Supplementary Act A/SA.2/01/10 on Electronic Transactions, Article 19.
[334] Supplementary Act A/SA.2/01/10 on Electronic Transactions, Article 18.
[335] Supplementary Act A/SA.2/01/10 on Electronic Transactions, Article 18 (3).
[336] Supplementary Act A/SA.2/01/10 on Electronic Transactions, Article 18 (1).
[337] Supplementary Act A/SA.2/01/10 on Electronic Transactions, Article 18 (2).
[338] Supplementary Act A/SA.2/01/10 on Electronic Transactions, Article 19.
[339] Supplementary Act A/SA.2/01/10 on Electronic Transactions, Article 29.
[340] Supplementary Act A/SA.2/01/10 on Electronic Transactions, Article 33.
[341] Supplementary Act A/SA.2/01/10 on Electronic Transactions, Article 34.
[342] Supplementary Act A/SA.2/01/10 on Electronic Transactions, Article 35.

states, some countries within the community have related legislation. Countries such as Ghana, Burkina Faso, Cape Verde, Ivory Coast, Gambia, Liberia and Senegal have enacted laws on electronic transactions. Also, just like the AU Convention, its factors in determining a valid contract is problematic because countries like Nigeria follow the common law approach to the definition of contract, and under the common law, display of goods is regarded as an invitation to treat; thus it is the consumer that makes the offer by placing an order while the vendor accepts the offer by acknowledging the order.

3.10 ECOWAS SUPPLEMENTARY ACT ON PERSONAL DATA PROTECTION

The ECOWAS Heads of State and Government adopted the *Supplementary Act A/ SA.1/01/10 on Personal Data Protection* in 2010 to serve as a regional legal framework on data protection regulation within the ECOWAS[343]. The Act aims to impose an obligation on member states to enact laws to protect the use, collection, processing and storage of personal data[344]. The Act equally requires member states to establish data protection authorities[345] within their jurisdictions who are independent[346] and enjoy immunity in the exercise of their functions[347]. The Act outlines the duties of these data protection authorities; they include informing data subjects and data controllers about their rights and responsibilities[348], receiving complaints and petitions on the breach of data privacy[349], imposing fines and sanctions[350], informing judicial authorities of offences where necessary[351] and authorise cross border transfer of personal data[352]. The Act outlines the principles that should govern data processing; they are as follows:

- The principle of consent and legitimacy.[353]
- The principle of legality and fairness.[354]
- The principle of purpose, relevance and preservation.[355]

[343] U Orji "A Comparative Review of the ECOWAS Data Protection Act" (2016) 4 Computer Law Review International at 109
[344] Supplementary Act A/ SA.1/01/10 on Personal Data Protection, Article 2.
[345] Supplementary Act A/ SA.1/01/10 on Personal Data Protection, Article 14.
[346] Supplementary Act A/ SA.1/01/10 on Personal Data Protection, Article 14(2).
[347] Supplementary Act A/ SA.1/01/10 on Personal Data Protection, Article 17(2).
[348] Supplementary Act A/ SA.1/01/10 on Personal Data Protection, Article 19 (a).
[349] Supplementary Act A/ SA.1/01/10 on Personal Data Protection, Article 19 (f).
[350] Supplementary Act A/ SA.1/01/10 on Personal Data Protection, Article 19 (i).
[351] Supplementary Act A/ SA.1/01/10 on Personal Data Protection, Article 19 (g).
[352] Supplementary Act A/ SA.1/01/10 on Personal Data Protection, Article 19 (i).
[353] Supplementary Act A/ SA.1/01/10 on Personal Data Protection, Article 23.
[354] Supplementary Act A/ SA.1/01/10 on Personal Data Protection, Article 24.
[355] Supplementary Act A/ SA.1/01/10 on Personal Data Protection, Article 25.

- The principle of accuracy.[356]
- The principle of transparency.[357]
- The principle of confidentiality and security.[358]
- The principle of choice of a data Processor.[359]

In addition, the Act prohibits the use of personal data for prospecting a data subject without his consent[360]. The Act also provides for the rights of data subjects; these rights include the right to know the identity of the data controller, [361]the right to know the purpose for which the data is being processed[362] , the right to know the period of storage of the processed data[363], the right to object to his data being processed[364] and the right to have his data rectified, updated or destroyed as appropriate[365]. Apart from the rights of the data subjects, the Act confers specific duties on the Data controller; this includes the duty to ensure that the processed data remains confidential[366], the duty to ensure that the data is secure and is inaccessible to third parties[367], the duty to ensure that the data is only preserved by the period prescribed by regulations[368] and the duty to ensure that the processed data is durable[369].

3.10.1 Shortcomings of This Act

This study finds that the Act contains a robust framework on data protection; however, it does not provide judicial remedies available to data subjects against data controllers or even the supervisory authority in the event of a breach[370] of privacy.

[356] Supplementary Act A/ SA.1/01/10 on Personal Data Protection, Article 26.
[357] Supplementary Act A/ SA.1/01/10 on Personal Data Protection, Article 27.
[358] Supplementary Act A/ SA.1/01/10 on Personal Data Protection, Article 28.
[359] Supplementary Act A/ SA.1/01/10 on Personal Data Protection, Article 29.
[360] Supplementary Act A/ SA.1/01/10 on Personal Data Protection, Article 34.
[361] Supplementary Act A/ SA.1/01/10 on Personal Data Protection, Article 38.
[362] Supplementary Act A/ SA.1/01/10 on Personal Data Protection, Article 38(2).
[363] Supplementary Act A/ SA.1/01/10 on Personal Data Protection, Article 38 (7).
[364] Supplementary Act A/ SA.1/01/10 on Personal Data Protection, Article 40.
[365] Supplementary Act A/ SA.1/01/10 on Personal Data Protection, Article 41.
[366] Supplementary Act A/ SA.1/01/10 on Personal Data Protection, Article 42.
[367] Supplementary A ct A/ SA.1/01/10 on Personal Data Protection, Article 43.
[368] Supplementary Act A/ SA.1/01/10 on Personal Data Protection, Article 44.
[369] Supplementary Act A/ SA.1/01/10 on Personal Data Protection, Article 45.
[370] Orji (n28) 118

3.11 THE ECOWAS DIRECTIVE ON CYBERCRIME

In pursuit of harmonisation of laws within the ECOWAS region and the need to curb internet-related crimes[371], the Heads of State and Government enacted the *Directive C/DIR.1/08/11 on Fighting Cybercrime within ECOWAS*. (Hereinafter referred to as the directive). The directive prescribes legal provisions for the regulation of cybercrimes within the region. The directive divides cybercrime offences into two categories: Offences specifically related to information and communication technologies and traditional offences relating to Information and Communication technologies. However, this study is interested in the former. The directive criminalises several acts such as fraudulently accessing computer systems[372], interfering with the operation of a computer system[373], fraudulently manipulating personal data[374], fraudulently intercepting computer data[375], computer data forgery[376], threat through computer systems[377]. (Simply put, the directive criminalises offences such as hacking, payment scams, identity theft, web cloning and phishing).[378]Apart from the substantive laws, the directive provides for procedural laws; the directive permits the relevant agencies to conduct searches or seize any computer system for investigation[379]. Furthermore, it permits the use of electronic evidence as proof to establish an offence[380]. In addition, it places an obligation on member states to cooperate where necessary in the area of searches and investigations[381].

3.11.1 Challenges of the Directive

This study finds that the directive provides substantial provisions for cybercrime regulation; however, it makes no mention of the institutional framework required to enforce these laws; the institutional frameworks include establishing a body or empowering an existing agency and outlining its roles and obligations. Furthermore, the directive has been said to be challenging to

[371] U Oriji "An Inquiry into the Legal Status of the ECOWAS Cybercrime Directive and the Implication of its Obligations for Member States (2019) 35 Computer Law and Security Review 7.
[372] Directive C/DIR.1/08/11 on Fighting Cybercrime within ECOWAS, Article 4.
[373] Directive C/DIR.1/08/11 on Fighting Cybercrime within ECOWAS, Article 6.
[374] Directive C/DIR.1/08/11 on Fighting Cybercrime within ECOWAS, Article 7.
[375] Directive C/DIR.1/08/11 on Fighting Cybercrime within ECOWAS, Article 8.
[376] Directive C/DIR.1/08/11 on Fighting Cybercrime within ECOWAS, Article 10.
[377] Directive C/DIR.1/08/11 on Fighting Cybercrime within ECOWAS, Article 21.
[378] Orji (n29) 4.
[379] Directive C/DIR.1/08/11 on Fighting Cybercrime within ECOWAS, Article 30.
[380] Directive C/DIR.1/08/11 on Fighting Cybercrime within ECOWAS, Article 32.
[381] Directive C/DIR.1/08/11 on Fighting Cybercrime within ECOWAS, Article 33.

implement due to the lack of technical experts to assist in this area and the lack of a regional agency responsible for monitoring the implementation of this directive[382]. However, some states have been able to enact cyber laws, whether as a separate act or as a part of existing legislation (countries such as Nigeria and Ghana); thus, this essay believes that these two states can assist other member states in the implementation of these laws. Concerning the need for a regional body to ensure the implementation of cybercrime regimes, this study recognises it as a challenge. However, it might be impractical to constitute one due to the cost involved. Therefore, the best alternative is to create sanctions in this Directive to ensure that member states adopt these directives within a reasonable time.

3.12 SUMMARY OF FINDINGS FROM THE EXAMINATION OF INTERNATIONAL INSTRUMENTS.

In light of the above, this study finds that for a country to have a robust framework for the protection of consumers in e-commerce, the legal framework must cover the following issues;

- The law must recognise online contracts and signatures as having the same legal status as traditional contracts and signatures.
- Businesses must be mandated to engage in fair trade practices by ensuring that they use fair contractual terms and refrain from misrepresentation.
- Businesses must be mandated to give complete and accurate information about their business, the product/ service and the transaction itself. Details about the transaction must include terms and conditions, payment methods, fixed charges, warranties and refunds.
- Cybercrime laws should criminalize identity theft, credit/ debit card fraud, cyber-stalking and phishing.
- Provision of laws that protect the use, storage and processing of the personal data of consumers.
- Payment methods must be secure. Therefore, the government must provide a minimum standard for the protection of consumers using e-payments.
- Due to the borderless nature of e-commerce, Countries should promote global cooperation amongst themselves.

[382] Orji (n29) 14.

- In addition to the legal framework, institutional frameworks must be in place; the law must establish or empower existing agencies that will regulate the activities of online marketplaces, investigate and take action to protect consumers. This study finds that e-commerce involves various sectors of the economy; this means that more than one regulator must be involved to ensure that consumers are protected across all sectors. However, to ensure simplicity, there should be a central law and a central regulator.
- Apart from regulators, effective alternative dispute resolution mechanisms must be put in place. For example, litigation is not suitable for resolving disputes under B2C e-commerce due to the small volume of transactions. Also, due to the borderless nature of e-commerce, countries should consider Online Dispute Resolution Mechanisms.

3.13 CONCLUSION

Above, the chapter examined the global, continental and regional frameworks governing e-commerce. It drew out the vital issues that a country's legal and regulatory framework must address to protect consumers robustly and found that once these measures are in place, governments will secure the trust and confidence of consumers in using e-commerce platforms.

CHAPTER FOUR

THE LEGAL AND REGULATORY FRAMEWORK FOR CONSUMER PROTECTION IN E-COMMERCE LANDSCAPE IN NIGERIA

4.1 INTRODUCTION

Nigeria is the largest economy in terms of the Gross Domestic Product in Africa. It is also one of the leading giants in e-commerce on the continent. Nigeria is ranked as the largest market for B2C e-commerce transactions in Africa[383]. However, there have been questions about the country's legal and regulatory framework for e-commerce, particularly as it borders on consumer protection. Thus, this chapter sets out to do the following (i) discuss the e-commerce landscape in Nigeria; (ii) outline the relevant provisions in the laws regulating consumer protection under e-commerce in Nigeria; (iii) critically examine these laws to determine whether they are in line with international best practices and (iv) to make a conclusion with the need for Nigeria to improve on its current legal and regulatory framework for consumer protection in e-commerce.

4.2 E-COMMERCE LANDSCAPE IN NIGERIA

The growth of e-commerce in Nigeria can be attributed to the high internet penetration, and mobile phones. Nigeria is equally endowed with a growing young population[384] whose average age is 18 years[385]. There are currently 104.4 million internet users in Nigeria[386] and over 170 million mobile phone subscribers[387]. Apart from the large population, Nigeria has a growing middle class; the purchasing power parity for the middle class is an average of $6,200[388].

[383] V Olumide "Nigeria is Africa's Largest B2C E-commerce Market in terms of numbers of shoppers and revenue" Business Insider Africa, 4 May 2021 https://africa.businessinsider.com/local/markets/nigeria-is-africas-largest-b2c-e-commerce-market-in-terms-of-number-of-shoppers-and/qrvfn07 (accessed 21 September 2021).
[384] International Trade Centre (n6) 5.
[385] Population of Nigeria https://www.worldometers.info/world-population/nigeria-population/ (accessed 6 October 2021).
[386] Data Reportal "Digital 2021: Nigeria" https://datareportal.com/reports/digital-2021-nigeria (accessed 22 September 2021).
[387] Jumia "Nigeria Mobile Report 2019" https://www.jumia.com.ng/sp-mobile-report/ (accessed 22nd September 2019).
[388] International Trade Centre (n6) 6.

There are over fifty-eight e-commerce marketplaces in Nigeria, but the most prominent platforms are Jumia[389], Konga[390], and Slotng[391]. The total number of online visitors to e-commerce marketplaces in Nigeria from 2017-2019 was estimated at 250.7 million[392]. As a result of the COVID 19 pandemic, online stores like Jumia recorded a 23% [393]increase in the growth of users. The annual revenue turn over by e-commerce platforms in Nigeria in 2020 was estimated at $6 billion[394]. As a whole, the e-commerce industry in Nigeria is worth $USD13 billion. However, as stated in Chapter one, the e-commerce industry in Nigeria is still in its infancy; it can grow exponentially, and a critical factor in ensuring its sporadic growth is to enhance consumer's trust in the e-commerce landscape. To this end, the extant laws on e-commerce in Nigeria will be examined. However, this study will limit its scope to the relevant laws that protect consumers.

4.3 THE EXTANT LEGAL AND REGULATORY FRAMEWORKS ON CONSUMER PROTECTION IN THE NIGERIAN E-COMMERCE LANDSCAPE.

The Nigerian constitution is the apex law in Nigeria, and all other laws must be in line with its provisions. Amongst other rights, the constitution guarantees the right to privacy[395]. As highlighted in chapter 2, this right is essential for the protection of consumers especially under e-commerce. However, Nigeria has not enacted any unified law on e-commerce. Different aspects of the legal regime including as it relates to cybercrimes, consumer protection, payments and data protection are covered by different legal frameworks. In the same way, there is no single institution or regulator that has oversight over all these aspects. This section discusses these laws with a focus on how they relate to consumer protection for e-commerce. Also, the regulatory authorities are simultaneously highlighted. Furthermore, this section examines the electronic transactions bill 2015 which is the proposed legal framework for electronic transactions in Nigeria.

---

[389] Jumia Nigeria https://www.jumia.com.ng/ (accessed 22 September 2021).
[390] Konga https://www.konga.com/?gclid=Cj0KCQjwqKuKBhCxARIsACf4XuGxH9BRI7qPVgQihWND-UzTQBpKAH9YJA7L6CbBdJsLjcplttgk43AaAiU4EALw_wcB (accessed 22 September 2021).
[391] Slotng https://slot.ng/ (accessed 22 September 2021).
[392] S Vanella "E-commerce in Nigeria-Statistics and Facts" Statistica, (13 November 2020) https://www.statista.com/topics/6786/e-commerce-in-nigeria/ (accessed 22 September 2020)
[393] Proshare " Opportunties for Nigeria's E-commerce"(12 February 2021) https://www.proshareng.com/news/ECOMMERCE/Opportunities-for-Nigeria-s-e-commerce/55738 (accessed 22 September 2021).
[394] EcommerceDB "E-commerce Market in Nigeria" https://ecommercedb.com/en/markets/ng/all#:~:text=The%20eCommerce%20market%20in%20Nigeria,rate%20of%2026%25%20in%202020 (accessed 22 September 2021).
[395] The Constitution of the Federal Republic of Nigeria 1999, Section 37.

4.3.1 The Cyber Crimes (Prohibition and Preventions Act) 2015

The Nigerian Cybercrimes (Prohibition and Prevention) Act, 2015 (the Act) was enacted into law by National Assembly on 5 May 2015; its main objective is to provide a comprehensive legal and regulatory framework for detection, prevention, and punishment [396]of cybercrime in Nigeria. It also seeks to ensure the protection of computers systems, electronic communication and privacy[397]. As it pertains to consumer protection under e-commerce, the Act outlines the following activities as cybercrimes: hacking[398], unauthorised interference with computer systems[399], unlawfully obtaining details from emails, credit and debit cards under false pretences[400], electronic fraud[401], fraudulent manipulation of payment systems[402], identity theft[403], impersonation[404], child pornography[405], cyber stalking[406], bullying[407] phishing[408] and spamming[409].

The Act places a duty on financial institutions[410] and service providers[411] to ensure that they provide security measures for the protection of the information of customers to prevent online breaches. The Act equally provides that the National Security Adviser will supervise the administration and enforcement of its provisions[412]. In addition, the act permits international cooperation; the Attorney General of Nigeria is vested with the power to ask for assistance from foreign jurisdictions for the investigation and prosecution of cybercrimes[413].

4.3.3 Federal Competition and Consumer Protection Act 2018

The Federal Competition and Consumer Protection Act (The FCCPA) provides the legal and institutional framework for regulating competition and consumer protection in Nigeria. The Act

[396] Cybercrimes (Prohibition and Prevention Act) 2015, section 1(a).
[397] Cybercrimes (Prohibition and Prevention Act) 2015, section 1(c) .
[398] Cybercrimes (Prohibition and Prevention Act) 2015, Section 6 (1).
[399] Cybercrimes (Prohibition and Prevention Act) 2015, Section 8 (2).
[400] Cybercrimes (Prohibition and Prevention Act) 2015, section 12(2).
[401] Cybercrimes (Prohibition and Prevention Act) 2015, Section 13(2).
[402] Cybercrimes (Prohibition and Prevention Act) 2015, Section 14 (4).
[403] Cybercrimes (Prohibition and Prevention Act) 2015, Section 22(1).
[404] Cybercrimes (Prohibition and Prevention Act) 2015, Section 22 (2).
[405] Cybercrimes (Prohibition and Prevention Act) 2015, Section 23 (2).
[406] Cybercrimes (Prohibition and Prevention Act) 2015, Section 24 (1).
[407] Cybercrimes (Prohibition and Prevention Act) 2015, Section 24(2).
[408] Cybercrimes (Prohibition and Prevention Act) 2015, Section 32 (1).
[409] Cybercrimes (Prohibition and Prevention Act) 2015, Section 32(2).
[410] Cybercrimes (Prohibition and Prevention Act) 2015, Section 19(3).
[411] Cybercrimes (Prohibition and Prevention Act) 2015, Section 38 (2).
[412] Cybercrimes (Prohibition and Prevention Act) 2015, Section 41 (a).
[413] Cybercrimes (Prohibition and Prevention Act) 2015, Section 52(1).

defines a consumer as anyone who purchases goods and services for consumption. Furthermore, it outlines several rights of the consumer, some of which are:

1. **The right to information**: A consumer has the right to be given information on products and services in simple and understandable language[414].
2. **The right to the disclosure of prices:** Sellers must ensure that the prices of goods and services are displayed[415].
3. **Right to receive goods that match description:** Where a consumer decides to receive goods based on the description of the seller, the seller must ensure that the goods match the description presented to the consumer[416] and such goods must be fit for purpose, where the goods fail to meet the description, the consumer has a right to reject such goods[417].
4. **Right to fair and reasonable contractual terms**: A seller is expected not to subject consumers to unreasonable and unfair trade terms[418].

The FCCPA also establishes the Federal Competition and Consumer Protection Commission[419] , whose duty is to implement and enforce the FCCPA, which includes the protection of consumers[420]. Also, it establishes the Competition and Consumer Protection Tribunal, which adjudicate activities prohibited by the FCCPA[421].

In addition, the FCCPA provides for how consumers can enforce their rights[422]. They can do so through the following means: report complaints to the commission[423], industry-specific regulators[424] or civil society groups.[425] The consumer can also seek redress from the court after the commission has carried out an investigation and finds that the consumers' rights have been gravely violated[426].

[414] The Federal Competition and Consumer Protection Act, Section 114.
[415] The Federal Competition and Consumer Protection Act 2018, Section 115.
[416] The Federal Competition and Consumer Protection Act 2018, Section 121.
[417] The Federal Competition and Consumer Protection Act 2018, Section 122.
[418] The Federal Competition and Consumer Protection Act 2018, Section 127.
[419] The Federal Competition and Consumer Protection Ac 2018t, Section 3.
[420] The Federal Competition and Consumer Protection Act 2018, Section 17.
[421] The Federal Competition and Consumer Protection Act 2018, Section 39.
[422] The Federal Competition and Consumer Protection Act 2018, Section 146.
[423] The Federal Competition and Consumer Protection Act 2018, Section 148.
[424] The Federal Competition and Consumer Protection Act 2018, Section 147.
[425] The Federal Competition and Consumer Protection Act 2018, Section 151.
[426] The Federal Competition and Consumer Protection Act 2018, Section 152.

4.3.4 Central Bank Consumer Protection Framework for Banks and Other Financial Institutions 2016

The Central Bank of Nigeria (CBN) is the primary regulator of banks and financial institutions in Nigeria. It has done a great job in ensuring that electronic payment systems are safe and affordable. Online shoppers in Nigeria no longer have to worry about the safety of using e-commerce platforms due to the effectiveness of the CBN and its regulations. In furtherance of its duties to ensure financial stability within the economy, it created a framework for protecting consumers of financial services. The provisions relevant to this research will be outlined below:

The framework mandates financial institutions to provide security measures for the protection of the assets of consumers[427]. These include the protection of electronic payment systems and gateways[428]. Financial institutions are to ensure that these technologies used undergo regular updates to prevent hacking or fraud[429]. The framework provides that the CBN will provide the minimum technology required to secure electronic payments[430]. The framework equally mandates financial institutions to respect consumers' privacy and protect their data from third parties[431].

The framework also mandates financial institutions to provide internal redress mechanisms for handling and resolving consumers' complaints[432]. They should also inform consumers on the available alternative dispute resolution mechanisms available to them[433]. These redress mechanisms must be effective, affordable and accessible[434].

[427] Central Bank Consumer Protection Framework for Banks and Other Financial Institutions 2016, paragraph 2.6.
[428] Central Bank Consumer Protection Framework for Banks and Other Financial Institutions 2016, paragraph 2.6(2).
[429] Central Bank Consumer Protection Framework for Banks and Other Financial Institutions, paragraph 2.6 (2)(a).
[430] As above
[431] Central Bank Consumer Protection Framework for Banks and Other Financial Institutions 2016, paragraph 2.6.2.
[432] Central Bank Consumer Protection Framework for Banks and Other Financial Institutions 2016, paragraph 2.7.
[433] Central Bank Consumer Protection Framework for Banks and Other Financial Institutions 2016, paragraph 2.7.1.
[434] Central Bank Consumer Protection Framework for Banks and Other Financial Institutions 2016, paragraph 2.7.2

4.3.5 The Nigerian Data Protection Regulation 2019

The National Information Technology Department Agency introduced the Nigerian Data Protection Regulation (NDPR) to protect personal data[435] and prevent its manipulation[436] by unscrupulous people. The NDPR defines a "Data Controller"[437] as any person or body that determines how data is to be processed[438], while a "Data subject|"[439] is any person who can be identified by reference to an identification number[440] or peculiar factors such as cultural[441], physiological[442] or social[443] characteristics.

The NDPR requires data controllers to obtain the consent[444] of data subjects before processing their data. Data controllers must ensure that they use effective security[445] measures to protect the data belonging to data subjects. The data subject has a right to reject the data being processed[446]. Also, the NDPR provides for penalties in the event of a breach of its provisions[447]. The Attorney General of the Federation must supervise any data meant to be transferred out of Nigeria[448]. The NDPR also establishes the Administrative Redress Panel[449] responsible for investigating complaints and determining the appropriate redress.

4.3.6 Consumer Code of Practice Regulations (CCPR) 2008

The Nigerian Communications Commission released a consumer code to regulate the operations of licenced telecommunications operators in Nigeria. This code is relevant to this study as telecommunications companies engage in mobile payment services used in e-commerce. This code contains the minimum standards for the protection of consumers by these licenced telecommunications operators. The CCPR mandates telecommunications companies to collect and process data lawfully. This data must also be adequately stored and not longer than necessary.

[435] The Nigerian Data Protection Regulation 2019, Paragraph 1.1 (a).
[436] The Nigerian Data Protection Regulation 2019, Paragraph 1.1 (c).
[437] The Nigerian Data Protection Regulation 2019, Paragraph 1.3 (x).
[438] As above.
[439] The Nigerian Data Protection Regulation 2019, Paragraph 1.1 (xiv).
[440] As above.
[441] As above.
[442] As above.
[443] As above.
[444] The Nigerian Data Protection Regulation 2019, Paragraph 2.2.
[445] The Nigerian Data Protection Regulation 2019, Paragraph 2.6.
[446] The Nigerian Data Protection Regulation 2019, Paragraph 2.8.
[447] The Nigerian Data Protection Regulation 2019, Paragraph 2.10.
[448] The Nigerian Data Protection Regulation 2019, Paragraph 2.11.
[449] The Nigerian Data Protection Regulation 2019, Paragraph 4.2.

In addition, the CCPR provides that the telecommunications companies must provide accessible internal complaints handling mechanisms. In the event of a breach, consumers can send complaints to the NCC after they have first issued complaints with the relevant telecommunications company.

4.3.7 The Electronic Transactions Bill 2015

The Electronic Transactions Bill (The bill) is designed to enable electronic transactions in Nigeria. The relevant provisions in this bill are outlined below:

The bill provides that any regulatory authority can make regulations for the facilitation of any of its provisions[450]. The bill validates electronic records[451], electronic signatures[452] and electronic contracts[453]. Whilst the bill has not been passed into law, the Evidence Act 2011 is the existing legal framework that recognises the validity of contracts signed electronically[454]. Online businesses are required to provide clear and precise information about their products and services[455]. They are also required to provide accurate and verifiable information about the business itself[456]. A consumer must not be held liable for charges where the goods or service does not match the description[457] displayed by the vendor or was not delivered in good condition[458] . The vendor must refund the consumer's money within a reasonable time[459]. In addition, the bill also makes provision for the protection of consumers' data; it requires that vendors keep the personal data of consumers confidential and make their privacy policies public and easily accessible to consumers[460]. The bill also admonishes vendors to give consumers the option to refuse to receive unsolicited messages[461].

[450] Electronic Transactions Bill 2015, Section 2(2), section 43.
[451] Electronic Transactions Bill 2015, Section 3.
[452] Electronic Transactions Bill 2015, Section 11.
[453] Electronic Transactions Bill 2015, Section 26.
[454] Evidence Act 2011, Section 93 (2) (3)
[455] Electronic Transactions Bill 2015, Section 33.
[456] Electronic Transactions Bill 2015, Section 33 (3).
[457] Electronic Transactions Bill 2015, Section 34 (4) (b.)
[458] Electronic Transactions Bill 2015, Section 34 (d).
[459] Electronic Transactions Bill 2015, Section 34 (5).
[460] Electronic Transactions Bill 2015, Section 35 (2).
[461] Electronic Transactions Bill 2015, Section 36.

4.4 CRITICAL EXAMINATION OF THE EXTANT NATIONAL LAWS, REGULATIONS AND BILLS

As highlighted in Chapter 1, one of the problems that have motivated this study is the inadequacy of the legal regime for consumer protection under e-commerce in Nigeria. Having presented an overview of the extant and proposed legal frameworks on consumer protection under e-commerce in the preceding section, it becomes imperative to undertake further assessment of these frameworks to underscore their weaknesses. This assessment will form the basis for some of the recommendations of the study.

4.4. 1The Cybercrime (Prohibition and Prevention Act) 2015

The Act, as discussed above, regulates cybercrime activities in Nigeria. A key provision in the Act provides that where a breach occurs and results in a loss for the consumer, the onus lies on the consumer to prove negligence on the bank that it could have done more to protect the consumer. This study finds that the provision seems to have put consumers in an unfair position; financial institutions are the stronger party in these relationships[462]. They also owe the fiduciary duty of confidentiality[463] to their consumers. On the other hand, consumers are usually the weak party in this situation as they have little to no knowledge of the security measures to protect their vital information. The implication of this provision is that it has reduced consumers' confidence in online payments. They will be wary of carrying out online transactions since the law places a greater burden on them. Interestingly, the Act provides that where financial institutions make unauthorised debits from a customer's account, such monies must be refunded within 72 hours[464]. Unfortunately, the Act does not establish measures to determine when the financial institution or the consumer is liable in the instance of an unauthorised transaction that occurred as a result of fraud[465].

Also, the Act does not provide for a specific regulatory authority responsible for the enforcement of its provisions; it only states that the relevant authorities have the power to implement its provisions[466]. This provision is problematic because this act focuses on technology. Thus it is not

[462] U Orji "Protecting Consumers from Cybercrime in the Banking & Financial Sector: An analysis of the Legal Response of Nigeria" (2019) 24 Journal of International & European Law 113. https://tilburglawreview.com/articles/10.5334/tilr.137/- accessed 22 September 2021
[463] As above.
[464] Cybercrimes (Prohibition and Prevention Act) 2015, Section 37 (2).
[465] Orji (n30) 118.
[466] Cybercrimes (Prohibition and Prevention Act) 2015, Section 47(1).

every agency that can implement or enforce its provisions[467]. Therefore, this study believes that there is the need to either empower a relevant agency or establish a separate one. Also, this study finds that the absence of a specific enforcement agency creates confusion for consumers as there is no specific authority they can reach in the event of a cyber-attack. .

4.4.2 The Federal Competition and Consumer Protection Act (FCCPA)

The FCCPA provides a sound legal framework for the protection of consumers and the enforcement of their rights. However, the FCCPA does not mention e-commerce at all. The implication of this is that the FCCPA will not address the peculiar challenges of online consumers. Although it covers some of the potential issues, consumers may face. This study finds that it does not address critical areas affecting online consumers. First, the protection of consumers' privacy as unscrupulous traders can use the consumers' personal information to gain profit. Second, the FCCPA does not address how to deal with unfair contractual terms under e-commerce, unlike traditional commerce, where the purchaser can negotiate terms and conditions. Under e-commerce, the purchaser cannot negotiate the terms of the agreement. Instead, the seller usually provides such information, and it is left for the purchaser to either accept it or not. Sometimes, these terms and conditions are not available to the consumer until he has purchased the goods.

Third, the FCCPA does not address electronic payment concerns, which is one of the primary reasons consumers do not participate in e-commerce. Thus, it ought to be addressed. Furthermore, It does not provide alternative dispute resolution (whether an ombudsman or online dispute resolution). The nature of e-commerce requires an easy and effective dispute resolution method, especially B2C e-commerce that usually involves low value transactions.

4.4.3 Central Bank Consumer Protection Framework for Banks and Other Financial Institutions

This framework provides comprehensive directives to financial institutions on the protection of consumers. However, it has some loopholes. First, although the framework mandates the financial institutions to protect consumers' information, it is silent on who bears the burden to prove

[467] F Eboibi "A Critical Exposition of the Nigerian Cybercrimes (Prohibition & Preventions) Act 2015" (2019) 5 Delsu Law Review at 88 https://www.delsulawreview.com/critical-exposition-of-the-nigerian-cybercrimes-prohibition-prevention-etc-act-2015-by-f-e-eboibi/ accessed 22 September 2021.

negligence where a consumer suffers a loss due to this[468]. Second, the framework does not provide for a precise and transparent method for internal complaints mechanisms[469]. It is essential to have one as it prevents confusion for consumers and reduces complexities[470]. Third, the framework also does not provide a uniform means of addressing external complaints[471]. It merely admonishes Financial institutions to point consumers to available alternative dispute resolution[472]. The problem is that some financial institutions put compulsory arbitration clauses in consumer agreements, limiting the consumer's option[473]. Also, a consumer can face challenges that involve more than one financial institution[474]. Thus, there is a need for the CBN to recommend one central effective alternative dispute resolution centre where consumers can lay complaints and access redress against various financial institutions[475].

4.4.4 The Nigerian Data Protection Regulation 2019 (NDPR)

The NDPR provides applicable provisions for the regulation of personal data in Nigeria. A key innovation is the establishment of the Administrative Redress Panel. However, it does not provide for when the panel would be set up[476], neither did it provide for its membership[477], qualification[478], tenure[479] and scope of operation. It equally does not provide for the procedures on investigation and the determination of redress. Also, while the NDPR provides for fines against breaches by data controllers, it does not provide the remedies available to data subjects whose rights have been violated.

4.4.5 Consumer Code of Practice Regulations 2007 (CCPR)

The CCPR was established in 2007, and as a result, it does not contain provisions peculiar to mobile banking and payments. For instance, it is silent on the redress available for consumers in

---

[468] Orji (n30) 114.
[469] World Bank Group *Diagnostic Review of Financial Consumer Protection: Key Findings and Recommendation* (2017) 24.
[470] As above.
[471] World Bank Group (n61) 25.
[472] As above.
[473] World Bank Group (n61) 26.
[474] As above.
[475] World Bank Group (n61) 27.
[476] Olumide Babalola "The Inadequacies of the Nigerian Data Protection Regulation 2019: Review" Olumide Babalola Legal Practitioners https://olumidebabalolalp.com/nigeria-data-protection-regulation-2019/ accessed 23 September 2021.
[477] As above.
[478] As above.
[479] As above.

the event of loss of money occasioned by the negligence of telecommunication companies. Also, the CCPR does not provide the minimum security measures required to protect vital information such as passwords and codes. It is essential to also examine the Electronic Transactions Bill as the Nigerian senate is considering it.

4.4.6 The Electronic Transactions Bill 2015

The Electronic Transactions Bill does not refer to any authority for implementing and enforcing its provisions; this seems like a reasonable thing to do due to the fragmented nature of e-commerce. However, this will only cause confusion. Instead, there should either be a central agency, ministry or committee regulating activities of e-commerce businesses, particularly for the benefit of consumers.

Also, the bill is silent on the issue of electronic payments and the parties that bear liabilities where a consumer has suffered a loss. In addition, it does not provide for any agency within which consumers can lay complaints neither does it provide dispute resolution mechanisms available to consumers where their rights have been violated. The absence of this will diminish consumer interest in e-commerce because they may not have recourse to remedies where their rights have been breached.

4.5 SUMMARY OF EXAMINATION

Chapter three set out the critical criteria a country needs to create a robust consumer protection regime in e-commerce. Nigeria has done a fair job in meeting some of them by providing the following: recognising online contracts and signatures, mandating businesses to provide accurate information, securing online payments and enacting laws on cybercrimes and privacy. However, it has failed in the rest. First, this study revealed that e-commerce regime in Nigeria is fragmented; the extant laws regulating the sector is scattered in different pieces of legislation. Second, the FCCPA does not cater for the peculiar needs of online consumers. Third, the institutional frameworks for consumer protection appear weak; the Cybercrimes Act does not provide any regulatory authority to enforce its provisions. The Federal Competition and Consumer Protection Commission clearly cannot protect online consumers under e-commerce as its provisions do not cater to their challenges. The Electronic Transactions Bill equally does not refer to any specific regulatory authority that will enforce its provisions. Fourth, the dispute resolution mechanisms are inadequate; neither the FCCPA nor the bill provides alternative dispute settlement mechanisms.

Finally, the NDPR establishes the Administrative redress panel but makes no provision for their mode of operations.

4.6 CONCLUSION

This chapter discussed the landscape of e-commerce in Nigeria. It equally examined the legal and regulatory frameworks governing the protection of consumers under e-commerce in Nigeria. This study brought to light the deficiencies in these frameworks and showed that Nigeria's current legal regime did not robustly protect online consumers. Thus, the above issues raised must be resolved to improve consumer trust in e-commerce in Nigeria.

CHAPTER FIVE

THE LEGAL AND REGULATORY FRAMEWORK OF CONSUMER PROTECTION IN E-COMMERCE IN SOUTH AFRICA: LESSONS FOR NIGERIA

5.1 INTRODUCTION

The growth of B2C e-commerce in any country is dependent on the robust protection it gives to its consumers under frameworks dealing with electronic transactions, consumer protection, electronic transactions, data protection and payments. South Africa has been commended for having such a regime that covers all these areas. The previous chapter examined the legal and regulatory framework in Nigeria and discovered its deficiencies. Thus it has become essential to compare Nigeria's framework with that of South Africa to draw lessons. In addition to the commendable legal frameworks that the Country has, South Africa has been selected as a comparator for these other reasons: Both countries are the largest economies in Africa. They are both the leading giants of e-commerce within the continent and are both developing countries. Against this background, this chapter will (i) discuss the e-commerce landscape in South Africa; (ii) outline its extant legal and regulatory framework; (iii) comparatively analyse South Africa's framework against that of Nigeria; and (iv) draw out the lessons Nigeria can learn from South Africa.

5.2 THE E-COMMERCE LANDSCAPE IN SOUTH AFRICA

South Africa is one of the leading giants of e-commerce in Africa, and the sector is growing steadily. The revenue gained from B2C e-commerce in 2019 was US$3 billion[480]. Rand Merchant Bank predicts that e-commerce will grow 150% by 2025[481]. The major e-commerce stores in South Africa are Takealot,[482]Makro,[483] Builders[484], Woolworths[485] and Nike[486]. The steady growth of

[480]E-commerce DB "E-commerce Report in South Africa 2020" https://www.statista.com/study/70380/ecommerce-in-south-africa/ (accessed 6 October 2021).
[481] A Thenga "E-commerce to be worth 225 Billion Rand in SA in the Next Five Years" Rand Merchant Bank. https://www.rmb.co.za/news/ecommerce-to-be-worth-r225bn-in-sa-in-5-years (accessed 6 October 2021).
[482] www.takealot.com (accessed 6 October 2021).
[483] https://www.makro.co.za/ (accessed 6 October 2021).
[484] https://www.builders.co.za/ (accessed 6 October 2021).
[485] https://www.woolworths.co.za/ (accessed 6 October 2021).
[486] www.nike.com (accessed 6 October 2021).

B2C e-commerce can be attributed to the country's high rate of internet penetration[487]. The internet penetration rate is averaged at 64%[488]; there are about 38[489] million internet users within the country. The COVID 19 pandemic further accelerated the growth of B2C e-commerce within the country[490]. A recent study carried out by First National Bank (FNB) showed that the spending activities in e-commerce grew by 30%[491] in 2020 compared to 2019, while traditional stores witnessed a decline of 12%[492]. The pandemic also brought about an increase in the number of online businesses; there are now about 5000 online businesses with an average turnover of US$6000[493]. Furthermore, the e-commerce landscape will soon take a further leap as Amazon[494] recently announced that it would be opening its first African office in South Africa.

5.3 LEGAL FRAMEWORK OF E-COMMERCE IN SOUTH AFRICA

South Africa has done a commendable job in providing a robust legal and regulatory framework for the protection of consumers under e-commerce. The principal laws regulating e-commerce in South Africa are the Electronic Communications and Transactions Act, the Protection of the Personal Information Act and the Consumer Protection Act. This study will outline the relevant provisions in these legislations.

5.3.1 The Electronic Transactions and Communications Act 2002 (ETCA)

The South African government enacted this law in 2002 due to the growth of electronic transactions within the country. The ETCA recognises electronic contracts[495] and signatures[496] as having the same legal status as their traditional equivalent. Therefore, businesses must make complete disclosures on the following information: its legal name, physical address, emails and

[487] As above
[488] Digital Report 2021: South Africa https://datareportal.com/reports/digital-2021-south-africa (accessed 7 October 2021).
[489] J Johnson "South Africa: Digital Population as of January 2021" (Statistica, 7 September 2021). https://www.statista.com/statistics/685134/south-africa-digital-population/#:~:text (accessed 6 October 2021).
[490] Deloitte "Digital Commerce Acceleration: Increased Online Purchases Present New Opportunities for Digital Commerce Players" (2021) 3 https://www2.deloitte.com/content/dam/Deloitte/za/Documents/strategy/za-Digital-Commerce-Acceleration-2021-Digital.p (accessed 6 October 2021).
[491] A Thenga "E-commerce to be worth 225 Billion Rand in SA in the Next Five Years" First National Bank https://www.fnbcib.com/news/ecommerce-to-be-worth-r225bn-in-sa-in-5-years accessed (6 October 2021).
[492] As above.
[493] As above.
[494] Business Tech "Amazon to Set Up South African Headquarters in 4 Billion Rand Development" https://businesstech.co.za/news/cloud-hosting/484385/amazon-to-set-up-south-african-headquarters-in-r4-billion-cape-town-development/ (accessed 6 October 2021).
[495] Electronic Transactions and Communications Act, Section 22.
[496] Electronic Transactions and Communications Act, Section 13.

membership organisation[497]. In addition, businesses are to give consumers the opportunity to review the entire transaction and correct mistakes before completing the transaction[498]. The ETCA mandates businesses to use secure payment methods in line with the minimum standards[499] required in South Africa. Where it fails to comply with these provisions, it will be liable for any loss suffered by the consumer[500]. Consumers are to report any complaints to the Consumers Affairs Committee[501]. The ETCA also makes provision for the protection for the storage and processing of consumers' data[502]. In addition, it makes provision for cybercrimes[503] and the appointment of cyber inspectors[504] to implement the provisions on cybercrimes. The Courts have the jurisdiction to persecute offences under the Act[505].

Under the ETCA, consumers have a "cooling off"[506] period where they are allowed to cancel as transaction without reason.[507] They cannot be penalised for this provided such cancellation is made within seven days after the goods or services were received[508] or within seven days after the conclusion of the contract.[509] In addition, where a consumer has already made a payment, the consumer is entitled to a refund within 30 days from the date of cancellation.

5.3.2 The Consumer Protection Act 2008

The Consumer Protection Act (CPA) was enacted to protect both traditional and online consumers. The CPA recognises the peculiarities of online transactions; thus, it provides that issues such as the delivery rights[510] of consumers and cooling periods[511] for online consumers fall under the purview of the ETCA; Under the CPA, delivery must be done at the time agreed[512] by both parties. However, under the ETCA, delivery must be completed within 30 days after the order was made[513].

[497] Electronic Transactions and Communications Act 2002, Section 43.
[498] Electronic Transactions and Communications Act 2002, Section 43(2).
[499] Electronic Transactions and Communications Act 2002, Section 43(5).
[500] Electronic Transactions and Communications Act 2002, Section 43 (6).
[501] Electronic Transactions and Communications Act 2002, Section 49.
[502] Electronic Transactions and Communications Act 2002, Section 50.
[503] Electronic Transactions and Communications Act 2002, Section 85.
[504] Electronic Transactions and Communications Act 2002, Section 81.
[505] Electronic Transactions and Communications Act 2002, Section 90.
[506] Electronic Transactions and Communications Act 2002, Section 44.
[507] Electronic Transactions and Communications Act 2002, Section 44 (1).
[508] Electronic Transactions and Communications Act 2002, Section 44 (1) (a).
[509] Electronic Transactions and Communications Act 2002, Section 44 (1) (b).
[510] The Consumer Protection Act 2008, Section 19.
[511] The Consumer Protection Act 2008, Section 16.
[512] The Consumer Protection Act 2008, Section.
[513] Electronic Transactions and Communications Act 2002, Section 46.

The Cooling period under the ETCA is seven days[514], while the cooling period under the CPA is five[515] days. The CPA provides for a sound institutional framework for the protection of consumers. It establishes the National Consumer Commission[516] responsible for the implementation of its provisions. (The establishment of this commission abolished the consumer affairs committee). The CPA also provides a plethora of options for consumers to seek redress. Consumers can seek redress by filing complaints to the Commission[517] or the Tribunal[518] on Consumer Protection directly. They can also file actions at the Provincial Consumer Courts[519] or explore Alternative Dispute Resolution Mechanisms such as Mediation[520], Conciliation[521] or Ombudsmen[522]. In addition, the South African Government established the Consumer Goods and Services Ombud[523] (CSGO). This body receives and deals with consumer complaints free of charge[524]. The next sub-heading will discuss the CSGO and its functions.

5.3.3 The Consumer Goods and Services Industry Code of Conduct and the Office of the Consumer Goods and Services Ombud (The Code)

The code is an offshoot of the CPA. It was enacted by the Minister of Trade and Industry on the recommendation of the National Consumer Commission to create a standard code of conduct for companies in handling internal complaints and provide a scheme for alternative dispute resolution[525]. Under the code, businesses must establish an effective internal complaints-handling mechanism that is easily accessible to consumers[526]. In addition, businesses are equally required to record all complaints for at least three years. The purpose of this is to highlight repeated complaints and share this information with the ministry to ensure that businesses are complying with the code, CPA and its internal complaints system[527].

[514] Electronic Transactions and Communications Act 2002, Section 44.
[515] The Consumer Protection Act 2008, Section 16.
[516] The Consumer Protection Act 2008, Section 85.
[517] The Consumer Protection Act 2008, Section 69 (c) (iv).
[518] The Consumer Protection Act 2008, Section 69 (a).
[519] The Consumer Protection Act 2008, Section 69(c).
[520] The Consumer Protection Act 2008, Section 70 (c).
[521] The Consumer Protection Act 2008, Section 70 (c).
[522] The Consumer Protection Act 2008, Section 70 (a).
[523] Consumer Goods and Services Ombud https://www.cgso.org.za/cgso/ (accessed 28 September 2021).
[524] As above.
[525] As above.
[526] The Consumer Goods and Services Industry Code of Conduct and the Office of the Consumer Goods and Services Ombud, Code 5.1.
[527] The Consumer Goods and Services Industry Code of Conduct and the Office of the Consumer Goods and Services Ombud, Code 5.1.7.

The code establishes the Consumer Goods and Services Ombud (CGSO), which provides an external platform for resolving consumer disputes informally[528]. Businesses are mandated to register under the CSGO except those exempted by the CPA[529]. They must also display on their websites and places of business that they are part of this scheme[530]. In addition, they must also provide a summary of the code and their internal complaints system on their website and place of business[531]. The CGSO is funded through annual fees[532] paid by businesses and special fees[533] as determined by the board of the CGSO. Also, Ombudsmen must be independent[534] and must carry out their roles objectively, fairly and equitably[535].

The CGSO is to receive complaints, carry out investigations and make recommendations. Such recommendations will be submitted to the Consumer Tribunal or a High Court to convert this into a consent judgment where the parties agree. The CGSO can also conduct mediation where the parties agree for this to happen. They are also to refer complaints that can be dealt with more appropriately by other agencies. The code also mandates them to compile data on complaints, identify reoccurring complaints and make recommendations to businesses on how they can deal with this. The operation of the CSGO has been quite successful in South Africa; According to its 2020-2021 Annual Report, the total number of complaints filed were 14,438[536] from 9,529[537] the previous year. As a result of the COVID-19 pandemic, many businesses were forced to open

[528] The Consumer Goods and Services Industry Code of Conduct and the Office of the Consumer Goods and Services Ombud, Code 6.1.2.
[529] The Consumer Goods and Services Industry Code of Conduct and the Office of the Consumer Goods and Services Ombud, Code 4.2.
[530] The Consumer Goods and Services Industry Code of Conduct and the Office of the Consumer Goods and Services Ombud, Code 5.1.3.
[531] The Consumer Goods and Services Industry Code of Conduct and the Office of the Consumer Goods and Services Ombud, Code 5.1.4.
[532] The Consumer Goods and Services Industry Code of Conduct and the Office of the Consumer Goods and Services Ombud, Code 6.2.1.
[533] The Consumer Goods and Services Industry Code of Conduct and the Office of the Consumer Goods and Services Ombud, Code 6.2.3.
[534][534] The Consumer Goods and Services Industry Code of Conduct and the Office of the Consumer Goods and Services Ombud, Code 8.3.
[535] The Consumer Goods and Services Industry Code of Conduct and the Office of the Consumer Goods and Services Ombud, Code 8.5.
[536] CGSO "2020-2021 Annual Report" at 3 https://www.cgso.org.za/cgso/download/cgso-2020-21-annual-report/ (accessed 30 September 2021).
[537] As above.

websites and consumers were compelled to use online shopping platforms. Thus e-commerce complaints increased from 6%[538] to 27%[539].

5.3.4 The Protection of Personal Information Act 2013 (POPIA)

The South African government enacted the POPIA to facilitate the protection of citizens' data by providing minimum requirements for collecting, processing, storing, and sharing personal data[540]. The Act provides for the right of data subjects[541] which include the right for their data to be processed lawfully[542], the right to be notified where their data is collected for processing[543], the right to object to their data being processed[544], the right to file complaints to a regulator[545] or institute an action[546] where their rights under the Act have been breached.

The Act establishes the Information Registrar[547] as the body responsible for implementing the act. It is responsible for educating the populace on data protection[548] and ensuring compliance with the Act's provisions. In addition, the Act mandates the Information Registrar to establish an enforcement committee[549] responsible for the determination of issues arising from the breach of the provisions of the Act. Members of the committee must include a judge and legal practitioner. The Act permits the data subject to submit its complaints to the Information Registrar for breach of their privacy rights[550]. Where the Information Regulator takes up a complaint, after investigation, the matter will be referred to the Enforcement Committee to determine the issues and provide its recommendations. The Act permits the Information Registrar to refer the complaints to other agencies where the Information Regulator believes the complaint is within the expertise of another agency[551]. Organisations are to appoint an Information Officer[552] that will encourage compliance with the Act within the organisation.[553] A data subject equally has a right

[538] CSGO (n60) 6.
[539] As above.
[540] The Protection of Personal Information Act 2013, Section 2.
[541] The Protection of Personal Information Act 2013, Section 5.
[542] The Protection of Personal Information Act 2013, Section 5(a).
[543] The Protection of Personal Information Act 2013, Section 5 (d).
[544] The Protection of Personal Information Act 2013, Section 5 (e).
[545] The Protection of Personal Information Act 2013, Section 5 (h).
[546] The Protection of Personal Information Act 2013, Section 5 (i).
[547] The Protection of Personal Information Act 2013, Section 39.
[548] The Protection of Personal Information Act 2013, Section 40 (1)(a).
[549] The Protection of Personal Information Act 2013, Section 50.
[550] The Protection of Personal Information Act 2013, Section 74.
[551] The Protection of Personal Information Act 2013, Section 78.
[552] The Protection of Personal Information Ac 2013, Section 55.
[553] The Protection of Personal Information Act 2013, Section 92.

to institute a suit in court[554] asking for the following remedies: damages for compensation[555]aggravated damages[556] and cost of the suit[557].

From the above, it can be seen that South Africa has provided a sound legal and institutional framework for the protection of consumers in South Africa. The country has met most of the criteria set out in Chapter four. However, the country can improve its legal framework in the following ways. First, as established in chapter 2 and 3, e-commerce is borderless; thus, the government of South Africa should set up the mechanisms for ensuring global cooperation on the subject of e-commerce. Such global cooperation can be in agreements through treaties, mutual recognition, international networks or other forms of cooperation. Second, South Africa can start considering incorporating a regime for ODR to deal with cross border disputes. ODR is currently being used in the European Union[558] for e-commerce disputes, and other countries are already considering incorporating it into their e-commerce regimes. To this end, the UNICTRAL Working Group Three[559] is already working on a model law that will govern online dispute resolution for cross border e-commerce disputes. Third, this study finds South Africa's approach to the protection of consumers under e-commerce to be fragmented. A better approach would be to have representatives from each agency form an umbrella body or committee to supervise e-commerce activities better.

5.4 COMPARATIVE ANALYSIS OF THE LEGAL AND REGULATORY FRAMEWORK OF NIGERIA AND SOUTH AFRICA

The Landscape of e-commerce in Nigeria and South Africa are similar as they are both the leading giants of e-commerce within the Continent. However, it is apparent from the above discussions that while South Africa has enacted sound legal and institutional frameworks for the protection of consumers under e-commerce, Nigeria is still grappling with this. Thus, this chapter undertakes a comparative analysis of the legal and regulatory frameworks of South Africa and Nigeria below:

[554] The Protection of Personal Information Act 2013, Section 99.
[555] The Protection of Personal Information Act 2013, Section 99(a).
[556] The Protection of Personal Information Act 2013, Section 99 (b).
[557] The Protection of Personal Information Act 2013, Section 99 (c).
[558] Council Directive 2013/11/EU of 21 May 2013 on Alternative Dispute Resolution for Consumer Dispute.
[559] UNCITRAL Working Group Three "Online Dispute Resolution for Cross Border E-commerce Disputes: Draft Outline Document Reflecting Elements and Principles for ODR Process" https://undocs.org/en/a/cn.9/wg.iii/wp.140 (accessed 30 September 2021).

The South African law on consumer protection (CPA) applies to both traditional and online consumers. Although the Act does not mention e-commerce, it recognises the ETCA and leaves specific peculiar issues such as delivery periods and "cooling-off periods" to its purview. The CPA also makes provision for a plethora of options within which consumers can resolve disputes. These options include filing complaints with the Tribunal, National Consumer Commission or Provincial Consumer Courts. Consumers can also make use of Alternative Dispute Mechanisms. The South African Government established the Consumer Goods and Services Ombud, an alternative dispute mechanism. It receives and determines complaints for free. This body is regulated by the government but funded by businesses through annual levies. The government mandates businesses to register with this platform and ensure it notifies consumers by indicating its registration on its website. In Nigeria, the FCCPA is silent about e-commerce and does not entirely make provisions on issues peculiar to online consumers, such as dealing with unfair contractual terms. While its provisions allow consumers to report complaints to the Federal Competition and Consumer Protection Commission or a specific Industry Regulator, it makes no provisions for Alternative Dispute Resolution Mechanisms. Also, no specialised courts are dealing with consumer protection issues; regular courts deal with such cases.

The South African government enacted the ETCA, which regulates Electronic Transactions within the country. The ETCA is modelled after the UNCITRAL Model Law on E-commerce but further makes provisions on consumer protection. A notable provision is on payments methods; businesses are mandated to use the recommended payment systems. Where businesses fail to do, they must bear any loss suffered by consumers. The ETCA also makes provision for complaints by consumers to be submitted to the Consumer Affairs Committee. The establishment of the Consumer Commission has abolished this committee. Thus complaints would be taken up by the Commission. Nigeria does not yet have an Act to regulate Electronic Transactions. Although it has prepared a bill in this regard, The Bill is also modelled after the UNCITRAL Model Law on e-commerce and, just like South Africa, also makes provisions for consumer protection. Unfortunately, the bill does not provide payment methods, nor does it mention any authority within which consumers can lay complaints.

The South African government subsumed cybercrimes into the ETCA. It also established the Cyber Inspector who is responsible for investigating and enforcing these provisions. Nigeria created a separate Act on Cybercrimes but failed to enact a regulatory authority or empower an existing agency responsible for implementing and enforcing its provisions.

The South African government enacted the POPIA for the protection of the data privacy of its citizens. It establishes the Information Regulator who is responsible for the implementation of this Act. It also establishes the Enforcement Committee tasked with the responsibility of determining complaints submitted to the Information Regulator. The POPIA gives a breakdown of the qualification of this Committee as well as its mode of operation. In addition, The POPIA lists several remedies available to data subjects where they choose to file an action in court. Such remedies include damages for compensation, aggravated damages, interest and the cost of the suit. The National Information Technology Development Agency enacted the NDPR to protect personal data in Nigeria; the NDPR made provisions establishing the Administrative Redress Panel responsible for investigating and determining a complaint against a breach. However, there is no provision for who would constitute the Panel, their qualification and their mode of operation.

5.5 CONCLUSION

This chapter outlined the legal framework for consumer protection in South Africa and compared it with Nigeria's legal framework. It brought to light the deficiencies in Nigeria's legal framework, particularly in its institutional frameworks. Thus Nigeria can learn the following lessons from South Africa's framework i) there must be a regulatory body that online consumers can report complaints both for civil complaints and cybercrimes ii) consumers must have access to alternative dispute resolution methods such as the Ombudsman system in South Africa iii) remedies must be made available for breach of the rights of data subjects. iv) the FCCPA must make provisions for peculiar issues that affect online consumers.

CHAPTER SIX

FINDINGS AND RECOMMENDATIONS AND CONCLUSION

6.1 FINDINGS

E-commerce provides numerous benefits to consumers, traders and the economy as a whole. The impressive growth of the internet and mobile connectivity in Nigeria has made the country a leading giant in e-commerce on the continent. However, this growth is slow; to facilitate the growth of e-commerce in Nigeria, consumer confidence is crucial. This confidence is gained by ensuring that the legal and regulatory frameworks provide robust protection for consumers.

The overall question this study sought to answer as outlined in chapter one is: what measure can Nigeria adopt to improve protection for consumers under e-commerce? The study also outlined the following sub questions which were addressed in subsequent chapters: (i) What is the conceptual framework of e-commerce and consumer protection? (ii)What are the international instruments governing consumer protection under e-commerce? (iii) What is the current legal and regulatory framework for e-commerce in Nigeria? (iv) Do the extant regulatory and institutional frameworks for e-commerce in Nigeria offer consumers adequate protection compared to South Africa (v) How can Nigeria improve on its current legal and regulatory framework on consumer protection in e-commerce? The findings of these chapters are summarised as follows:

In chapter two, the study provided an introduction to the concept of e-commerce and the rationale behind consumer protection. It identified consumers' issues under e-commerce, such as privacy breaches, formation of contracts, deceptive trade practices, cybercrimes, jurisdiction, choice of law and effective dispute resolution mechanisms. However, this study revealed the vulnerability of consumers in e-commerce, thereby creating the need for the promulgation of robust laws and regulations to protect online consumers by addressing these concerns adequately.

In chapter three, the study examined the global, continental and regional frameworks governing e-commerce. It revealed that both legal and institutional frameworks are needed to protect consumers and then drew out the key provisions that countries must have in order to achieve a robust consumer-driven regulatory framework.

In chapter four, this study scrutinized the legal and regulatory framework governing consumer protection under e-commerce in Nigeria. It revealed that Nigeria's current framework did not provide robust protection for its online consumers as they were not entirely in line with international practices.

Lastly, in chapter five, this study conducted a comparative analysis of Nigeria's legal framework with South Africa, an equally leading giant in e-commerce within the continent. It revealed that South Africa had a robust consumer protection-driven framework for online consumers and drew out lessons that Nigeria could learn to improve its framework to increase consumer trust in e-commerce.

6.2 RECOMMENDATIONS

In view of the above analysis, this study recommends that the Electronic Transactions bill should be recalled and reviewed to input necessary changes. First, the bill should provide for an agency that will implement its provisions. Since e-commerce encompasses various sectors, the agency should constitute representatives from agencies such as the National Information Technology Development Agency, Central Bank of Nigeria, Nigerian Communications Commission, the Federal Competition and Consumer Protection, the Corporate Affairs Commission and other relevant agencies. This will prevent duplication of roles and foster easy co-operation between the agencies. The Bill should also grant the Federal Competition and Consumer Protection jurisdiction to deal with consumer complaints. Online Consumers need an agency that can attend to their issues. This agency can also refer complaints to the other regulatory bodies listed above where the complaint is beyond its expertise and powers.

Secondly, the Federal Competition and Consumer Protection must provide a minimum standard for handling internal complaints. This can be done through the use of regulations or codes, just like in South Africa. Also, the extant laws and regulations should provide a central ADR body, particularly for low-value transactions. An excellent example of a practical mode of resolving consumer disputes is the CGSO in South Africa. The government can release a regulation mandating companies to register on to the service, including e-commerce platforms. This platform should also be accessible for consumers. The complaints can be subject to a particular threshold, after which parties have to resort to the court. Annual subscriptions from companies can be used to support this platform. The code should also provide the duties of the body as well as its mode

of operation. The body should also refer its recommendation to the court to be registered as a consent judgment. Also, rather than creating special courts for consumer protection, a better approach would be to appoint more judges in each court to deal with cases in electronic transactions. Such judges can equally have the jurisdiction to handle consumer protection issues in e-commerce; this will prevent duplication. In addition, such judges will handle consumer protection disputes that cannot be resolved by ADR or cases that are higher than the threshold allowed.

Thirdly, the Nigerian government needs to either constitute a body or empower an existing agency that will implement and enforce the provisions of the Cybercrimes (Prohibition, Prevention Act) 2015. This is because consumers need to be able to report criminal complaints to the appropriate body. In addition, the government needs to take proactive steps in protecting consumers as opposed to taking a reactive approach. A fundamental way for the government to be proactive is by collating and analysing consumer complaints gathered by the central ADR body, courts and regulators. Also, conducting research and surveys to study patterns and future trends to create policies that better protect online consumers.

Lastly, one prominent feature of e-commerce is its cross-border nature; thus, Nigeria needs to foster global cooperation with other countries through treaties, mutual recognition, or other forms of cooperation. Also, the government should start looking at ODR. ODR is currently being used in the European Union for e-commerce disputes, and other countries are already considering incorporating it into their e-commerce regimes. To this end, the UNICTRAL working group three is already working on a model law that will govern online dispute resolution for cross border e-commerce disputes. Nigeria can begin to look at how it will incorporate this into its e-commerce regime.

In conclusion, trust is critical to unlocking the potentials of e-commerce in Nigeria, and unless consumers fully safe and protected, the sector will not experience sustainable growth. Currently, Nigeria's extant regulatory framework on e-commerce does not adequately protect consumers. Therefore, it is pertinent that the extant frameworks are revised to engender consumer confidence in e-commerce leading to rapid growth in the sector and economic prosperity.

BIBLIOGRAPHY

BOOKS

Becker, S *Electronic Commerce: Concept, Methodologies, Tools and Application* (Hershey 2008).

Davidson, A *The Law of Electronic Commerce* (Cambridge University Press 2009).

Hornle, J *Internet Jurisdiction Law and Practice* (Oxford University Press 2021).

Kim, N *Wrap Contracts: Foundations & Ramifications* (Oxford University Press 2013).

Shilling, D *Lawyer's Desk Book* (Walter Kluwer Law & Business 2018).

Idowu S, Capaldi, N Gupta, A *Encyclopedia of Corporate Social Responsibility* (Springer2013).

Talloo, T *Business Organization and Management* (Tata Mcgraw Hill Education 2008).

Turban E, White side J, King E, Outland J *Introduction to Electronic Commerce and Social Commerce* (Springer 2017).

Turner, C *Contract Law* (Routledge Taylor & Francis Group 2014).

Wang, F *Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US & China* (Cambridge University Press 2010).

Yuthayotin, S *Access to Justice in Transnational B2C E-commerce* (Springer 2014).

JOURNALS

Apau, R Korantey, F & Gyamfi, S "Cybercrimes and its Effects on E-commerce Technologies" (2019) 5 Journal of Information Technologies at 40.

Binding, J & Purnhagen, K "Regulations on E-commerce Protection Rules in China and Europe compared –same but different (2011) 2 Journal of Intellectual Property, Information Technology & Electronic Commerce Law 187.

Cortes, P & Ladder, A “Consumer Dispute Resolution Goes Online: Reflections on the Evolution of European Law for Out-of-Court Redress (2014) 21 Maastrict Journal of European & Comparative Law 15.

Filani, A “E-Commerce and Enforcement of Consumer Rights in Nigeria: Issues, Prospects and Challenges” Journal of Law and Judicial system, Volume 3, Issue 1, 2020.

Gladys, E 'Legal Framework for the Protection of Online Products Consumers in Nigeria' (2018) 21 Nigerian Law Journal.

ILobinso, I 'Paving the Path to an Enhanced Consumer Protection for the Nigerian Online Market: Theories and Concepts' (2017) 8 Nnamdi Azikiwe University Journal.

Jawahitha, S “Cyber Jurisdiction and Consumer Protection in E-commerce” (2005) 21 Computer and Law Security Report 154.

Ndonga, D” E-commerce in Africa: Challenges and solutions” (2012) 5 African Journal of Legal Studies 254.

Nuruddeen M, Yusof Y, and Abdullahi A “Electronic Commerce Transaction in Nigeria: A critical literature review” (UUM International Legal Conference 2017, Malaysia, July 2017).

Nuruddeen, M Yusof, Y and Abdullahi, A “An examination of Judicial Mechanism of Protecting the Rights of E-commerce in Nigeria” Journal of Governance and Development (2017)

Nurudeen, M & Yusof, Y “A Comparative analysis of the Legal Norms for E-commerce and Consumer. Protection” (2021) 26 Malaysian Journal of Consumers and Family Economics 22.

Orji, U “An Inquiry into the Legal Status of the ECOWAS Cybercrime Directive and the Implication of its Obligations for Member States (2019) 35 Computer Law and Security Review

Orji, U “Examining Missing Cyber Security Governance Mechanisms in the African Union Convention on Cyber Security and Personal Data Protection” (2014) 15 Computer Law Review International at 132.

Orji, U "The African Union Convention on Cyber Security: A Regional Response Towards Cyber Stability (2018) 12 Masaryk University Journal of Law and Technology 117.

Polanski, P "International Electronic Contracting in the Newest UN Convention" (2007) 2 Journal of International Commercial Law and Technology at 112.

Santos, V Morais, G, Sabino, L and Goncalves C "E-commerce: A Short History Follow up on Trends" (2017) 8 International Journal of Business Administration 131.

Shaik, D & Poojasree, V "Consumer Protection in E-commerce: A Legal and Compliance Framework for the Digital Market" (2020) 549 Advances in Social Science, Education and Human Research 20.

White, D & Ariguzo G "The First Decade of E-commerce" (2008) Journal of International Business Information 1 Systems 239

Xiao B & Bonbasat I "Product Related Deception in E-commerce: A Theoretical Perspective" 29

ONLINE ARTICLES

African Union Convention on Cyber Security and Personal Data Protection, Article 1.

Boasiko, A "E-commerce development in Ghana/West Africa & Cybersecurity challenges" UNCTAD expert meeting on cyberlaw & regulation for enhancing e-commerce" E-commerce Development in Ghana/West Africa & Cyber Security Challenges (unctad.org) (accessed 5th April 2021)

Cabel, D Bilstad, B & Enright, K "Consumer Privacy" (2000) Berman Online Lecture and Discussion Series Harvard Law School at 1 https://cyber.harvard.edu/olds/ecommerce/privacytext.html (accessed 24th August 2021)

Chawla N & Kumar B "E-commerce and Consumer Protection in India: The Emerging Trend" (2021) Journal of Business Ethics at 6 https://doi.org/10.1007/s10551-021-04884-3 (accessed 1st August 2021).

Coetzee J "The Convention on the Use of Electronic Communications in International Contracts: Creating an International Legal Framework for Electronic Contracting" (2006) 18 SA Mercantile Law Journal at 247. https://journals-co-za.uplib.idm.oclc.org/doi/10.10520/EJC54209 (accessed 1 September 2021).

Connolloy C & Ravindra P "First UN Convention on ecommerce finalised" (2006) 22 Computer Law & Security Report at 32 https://wwwsciencedirectcom.uplib.idm.oclc.org/science/article/pii/S026736490500186X (accessed 31 August 2021).

Dobias, J "Privacy Effects of Web Bugs Amplified by Web 2.0" In: Hübner F, Duquenoy S, Hansen P, Leenes M, Zhang R (eds) *Privacy and Identity Management for Life Privacy and Identity (2010)* 244 https://doi.org/10.1007/978-3-642-20769-3_20 (accessed 24th August 2021).

Eboibi, F "A Critical Exposition of the Nigerian Cybercrimes (Prohibition & Preventions) Act 2015" (2019) 5 Delsu Law Review at 88 https://www.delsulawreview.com/critical-exposition-of-the-nigerian-cybercrimes-prohibition-prevention-etc-act-2015-by-f-e-eboibi/ accessed 22 September 2021.

Jayabalan, S "E-commerce & Consumer Protection: The Importance of Legislative Measures" (2012) 15 Journal of the National University of Malaysia 1 https://ejournal.ukm.my/juum/article/view/7523/3045 (accessed 20th September 2021).

Joseph B "The Roles of Information & Communications Technology (ICTs) and E-commerce as Agents of Nigeria's Economic Development: Review of Challenges and Prospects" (2019) 10 Wireless Engineering and Technology Journal 43 https://www.scirp.org/pdf/wet_2020041415315688.pdf (accessed 6 October 2021)

Khare R & Rajvanshi G "E-commerce & Consumer Protection: A Critical Analysis of Legal Regulation (2013) International Journal on Consumer Law and Practice 62.

Munjai, S & Ahere, A "Cybercrime Threats for E-commerce(2016) Social Science Research Network Electronic Journal at 3 https://publication/306401151_Cyber_Crimes_Threat_for_E-commerce accessed 25th August 2021.

Orji U "Protecting Consumers from Cybercrime in the Banking & Financial Sector: An analysis of the Legal Response of Nigeria" (2019) 24 Journal of International & European Law 113. https://tilburglawreview.com/articles/10.5334/tilr.137/- accessed 22 September 2021

Pistorius, T "Contract formation: A comparative perspective on the Model law on electronic commerce" (2002) 35 Comparative and International Law Journal of Southern Africa 131 https://journals-co-za.uplib.idm.oclc.org/doi/10.10520/AJA00104051_178 (accessed 31 August 2021).

S Velagapudi & H Gupta, "Privacy, Security of Cookies in HTTP Transmission" (*2019)* 4th International Conference on Information Systems and Computer Networks (ISCON) at 22 https://ieeexplore-ieee org.uplib.idm.oclc.org/document/9036289 (accessed 24th August 2021).

FOREIGN CASE LAW

Steven J Caspi v Microsoft Network 323 NJ Super 118 (1999).

Specht v Netscape Communications Corp (2001) 150 F. Supp. 2d 585.

REPORTS/PAPERS

Grand View Research "Market Analysis Report" (2021) https://www.grandviewresearch.com/industry-analysis/b2c-e-commerce-market (accessed 20th September 2021).

International Trade Centre "*International E-commerce in Africa: The way forward" 2015* Microsoft Word - E-commerce_111215 (intracen.org) (accessed 5th April 2021).

International Trade Centre *International E-commerce in Africa: The way forward (2015)4* Microsoft Word -commerce_111215 (intracen.org) (accessed 21st May 2021) .

JF Kennedy "Special Message to the Congress of the United States on the Protection of Consumers Rights" (1962)

Liu H &Liu X, "The protection of the privacy right in electronic commerce" (2012) 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet) at 691doi:10.1109/CECNet.2012.6201744.https://ieeexplore-ieee org.uplib.idm.oclc.org/document/6201744 (accessed 23rd August 2021).

Nadal A & Gomila J "Comments to the UNCITRAL Model Law on Electronic Signatures" (2002) 5th International Conference on Information Security 241.

UNCITRAL Working Group Three "Online Dispute Resolution for Cross Border E-commerce Disputes: Draft Outline Document Reflecting Elements and Principles for ODR Process" https://undocs.org/en/a/cn.9/wg.iii/wp.140 (accessed 30 September 2021)

UNCTAD *Manual on Consumer Protection* (2016) 3 https://unctad.org/system/files/official-document/webditcclp2016d1.pdf accessed 13th August 2021

United Nations Division on Trade and Development "*COVID 19 & E-commerce: A Global Review"* (2021) dtlstict2020d13_en.pdf (unctad.org) (accessed 2nd April 2021).

United Nations *Transforming our world: The 2030 Agenda for Sustainable Development* *https://sustainabledevelopment.un.org/content/documents/21252030%20Agenda%20for%20Sustainable%20Development%20web.pdf* (accessed 20th August 2021)

World Bank Group *Diagnostic Review of Financial Consumer Protection: Key Findings and Recommendation* (2017).

INTERNATIONAL INSTRUMENTS

African Union Convention on Cyber Security and Personal Data Protection.

Council Directive 2013/11/EU of 21 May 2013 on Alternative Dispute Resolution for Consumer Dispute.

Directive C/DIR.1/08/11 on Fighting Cybercrime within ECOWAS

OECD Guideline for Consumer Protection in the Context of E-commerce 2016.

Supplementary Act A/ SA.1/01/10 on Personal Data Protection

Supplementary Act A/SA.2/01/10 on Electronic Transactions.

The UNCITRAL Model law on electronic commerce

UNCITRAL Model Law on E-commerce 1996, Article 2.

United Nations Convention on the Use of Electronic Communication in International Contracts,

United Nations Guidelines on Consumer Protection.

NIGERIAN LEGISLATION

Central Bank Consumer Protection Framework for Banks and Other Financial Institutions.

Cybercrimes (Prohibition and Prevention Act) 2015, section 1(a).

The Constitution of the Federal Republic of Nigeria 1999, Section

The Electronic Transactions Bill 2015.

The Federal Competition and Consumer Protection Act, Section 114.

The Nigerian Data Protection Regulation

SOUTH AFRICAN LEGISLATION

Electronic Transactions and Communications Act, 2002.

The Consumer Protection Act 2008

The Protection of Personal Information Act 2013.

The South Reserve Bank Act 90 1989

WEBSITES

Kongahttps://www.konga.com/?gclid=Cj0KCQjwqKuKBhCxARIsACf4XuGxH9BRI7qPVgQihWND-UzTQBpKAH9YJA7L6CbBdJsLjcplttgk43AaAiU4EALw_wcB (accessed 22 September 2021).

A Thenga "E-commerce to be worth 225 Billion Rand in SA in the Next Five Years" Rand Merchant Bank. https://www.rmb.co.za/news/ecommerce-to-be-worth-r225bn-in-sa-in-5-years (accessed 6 October 2021).

Babalola, O "The Inadequacies of the Nigerian Data Protection Regulation 2019: Review"

Bank for International Settlements "Payment Systems in South Africa" https://www.bis.org/cpmi/paysys/southafrica.pdf (accessed 7 October 2021)

Business Tech "Amazon to Set up South African Headquarters in 4 Billion Rand Development" https://businesstech.co.za/news/cloud-hosting/484385/amazon-to-set-up-south-african-headquarters-in-r4-billion-cape-town-development/ (accessed 6 October 2021).

CGSO "2020-2021 Annual Report" at 3 https://www.cgso.org.za/cgso/download/cgso-2020-21-annual-report/ (accessed 30 September 2021).

Data Reportal "Digital 2021: Nigeria" https://datareportal.com/reports/digital-2021-nigeria (accessed 22 September 2021).

Deloitte “Digital Commerce Acceleration: Increased Online Purchases Present New Opportunities for Digital Commerce Players” (2021) 3

Digital Report 2021: South Africa https://datareportal.com/reports/digital-2021-south-africa (accessed 7 October 2021).

E-commerce DB “E-commerce Report in South Africa 2020” https://www.statista.com/study/70380/ecommerce-in-south-africa/ (accessed 6 October 2021).

EcommerceDB “E-commerce Market in Nigeria” https://ecommercedb.com/en/markets/ng/all#:~:text=The%20eCommerce%20market%20in%20Nigeria,rate%20of%2026%25%20in%202020 (accessed 22 September 2021).

https://www.builders.co.za/ (accessed 6 October 2021).

https://www.makro.co.za/ (accessed 6 October 2021).

https://www.woolworths.co.za/ (accessed 6 October 2021).

https://www2.deloitte.com/content/dam/Deloitte/za/Documents/strategy/za-Digital-Commerce-Acceleration-2021-Digital.p (accessed 6 October 2021).

Johnson J “South Africa: Digital Population as of January 2021” (Statistica, 7 September 2021). https://www.statista.com/statistics/685134/south-africa-digital-population/#:~:text (accessed 6 October 2021).

Jumia “Nigeria Mobile Report 2019” https://www.jumia.com.ng/sp-mobile-report/ (accessed 22nd September 2019).

Jumia Nigeria https://www.jumia.com.ng/ (accessed 22 September 2021).

Olumide V “Nigeria is Africa’s Largest B2C E-commerce Market in terms of numbers of shoppers and revenue” Business Insider Africa, 4 May 2021 https://africa.businessinsider.com/local/markets/nigeria-is-africas-largest-b2c-e-commerce-market-in-terms-of-number-of-shoppers-and/qrvfn07 (accessed 21 September 2021).

Olumide Babalola Legal Practitioners https://olumidebabalolalp.com/nigeria-data-protection-regulation-2019/ (accessed 23 September 2021).

Proshare " Opportunties for Nigeria's E-commerce"(12 February 2021) https://www.proshareng.com/news/ECOMMERCE/Opportunities-for-Nigeria-s-e-commerce/55738 (accessed 22 September 2021).

Slotng https://slot.ng/ (accessed 22 September 2021).

Thenga, A "E-commerce to be worth 225 Billion Rand in SA in the Next Five Years" First National Bank https://www.fnbcib.com/news/ecommerce-to-be-worth-r225bn-in-sa-in-5-years accessed (6 October 2021).

Vanella, S "E-commerce in Nigeria: Statistics and facts (Statistica, 13th November 2020) https://www.statista.com/topics/6786/e-commerce-in-nigeria/ (accessed 1st May 2020)

Vanella, S "E-commerce in Nigeria-Statistics and Facts" Statistica, (13 November 2020) https://www.statista.com/topics/6786/e-commerce-in-nigeria/ (accessed 22 September 2020)

www.nike.com (accessed 6 October 2021).

www.takealot.com (accessed 6 October 2021).