FINANCIAL TECHNOLOGY AND THE INCIDENCE OF CYBER CRIME IN NIGERIA

BY

EGBE NGOZI MARYANN

MGS1706529

DEPARTMENT OF BANKING AND FINANCE

FACULTY OF MANAGEMENT SCIENCES

UNIVERSITY OF BENIN,

BENIN CITY

DECEMBER, 2022

FINANCIAL TECHNOLOGY AND THE INCIDENCE OF CYBER CRIME IN NIGERIA

BY

EGBE NGOZI MARYANN

MGS1706529

A RESEARCH PROJECT SUBMITTED TO THE DEPARTMENT OF BANKING AND FINANCE FACULTY OF MANAGEMENT SCIENCES UNIVERSITY OF BENIN, BENIN CITY, IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE BACHELOR OF SCIENCE (B.SC.) DEGREE IN BANKING AND FINANCE

DECEMBER, 2022

CERTIFICATION

We the undersigned, certify that this project was carried out by **EGBE NGOZI MARYANN** in the Department of Banking and Finance, University of Benin, Benin City and approved as adequate in scope and quality for the partial fulfilment of the requirements of the award of Bachelor of Science Degree (B.Sc.) in Banking and Finance.

Dr. Nosakhare Ikponmwosa
(Project Supervisor)

Date:

_____

_____

Dr. J. Obayangbona
(Project Co-ordinator)

Date:_____

_____

Dr. O.G Omorokunwa
(Head of Department)

Date:

_____

_____

DEDICATION

This work is dedicated to God Almighty, the reason for my living. He is the one who made this work possible. To Him be all the glory and honor now and forever.

ACKNOWLEDGMENTS

My utmost gratitude goes to God Almighty for His infinite mercies throughout my stay in the University of Benin. I would also like to express my sincerest appreciation to my Mother, Mrs. Rosemary U. Egbe, for being my biggest strength throughout this journey, Thank you for teaching me what a strong woman looks like. To my father, Mr. Joseph O. Egbe, thank you for everything. To my sisters, I owe you everything, thank you guys for always being my "one call away".

My profound gratitude goes to my project supervisor Dr Ikponmwosa Nosakhare, thank you for making this project extremely easy and for guiding me through it. For constantly holding me down and being there for me; Nosa-Ehima M. Uwagbae; I am forever grateful. To the family that I didn't know I needed that this department gave to me; Elvis (my educational guide); John (my best friend); Rosa (my sister); Osazee (the comic relief) and Prince(my support system). I love you all and thank you for the endless memories. To my Best Friends, Osuyali Tobechukwu, Jude, Ibingha Emem Karen thank you all for your constant support.

TABLE OF CONTENT

Cover Page i

Title page ii

Certification iii

Dedication iv

Acknowledgement v

Table of content vi

Abstract ix

CHAPTER ONE: INTRODUCTION

1.1 Background of the study 1

1.2 Statement of Research Problem 3

1.3 Research Questions 4

1.4 Objectives of the study. 4

1.5 Statement of hypothesis. 4

1.6 Significance of Research 5

1.7 Scope of the Study 5

1.8 Limitations to the Study. 5

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction. 6

2.2 Conceptual Review 6

2.2.1 Concept of Cybercrime 6

2.2.2 Categories of Cyber crime 6

2.2.3 Dimensions of Cyber Crime 8
2.2.4 Causes Of Cyber Crime 8
2.2.5 Effects Of Cyber Crime. 10
2.2.6 Cyber Crime in Nigeria. 11
2.2.7 Impact of Cyber crime on Nigeria Banking System. 12
2.2.8 The Cybercrime (Prohibition, Prevention, Etc)
Act, 2015. 16
2.2.9 Role of NDIC 17
2.2.10 Policing Cybercrime in Nigeria 17
2.2.11 Solutions to Cybercrime in Nigeria 19
2.2.12 Role of Individuals, Financial institutions and Business
in Combating Cybercrime. 20
2.3 Theoretical Review 20
2.3.1 Routine Activity Theory (RAT). 20
2.3.2 General Deterrence Theory. 21
2.3.3 Theory of Technology-Enabled Crime 21
2.3.4 General Theory of Crime 22
2.4 Empirical Review. 23
CHAPTER THREE: METHODOLOGY
3.1 Introduction. 27
3.2 Research Design. 27
3.3 Population and Sample of the Study 27

3.4 Sources of Data 28

3.5 Theoretical Framework 28

3.6 Model Specification. 29

3.7 Measurement and Operationalization of Variables. 31

3.8 Method of Data Analysis 32

CHAPTER FOUR: DATA PRESENTATION, ANALYSIS AND INTERPRETATION

4.1 Introduction. 33

4.2 Empirical Results 34

4.3 Test of Hypothesis 36

4.4 Discussion of Finding and Policy Implication 37

CHAPTER FIVE: SUMMARY OF FINDINGS, CONCLUSION, AND POLICY RECOMMENDATION

5.1 Summary and Findings 39

5.2 Conclusion 40

5.3 Policy Recommendations 41

5.4 Further Research. 42

APPENDIX

REFERENCES

ABSTRACT

This study empirically examines the link between financial technology and the rise of cybercrime in Nigeria. The intensity of detected cybercrime (measured in billions of naira) was used as the dependent variable, with three financial technologies, ATMs, internet services, mobile banking and a control variable (an organizational dummy involved in combating cybercrime). are regressed on four explanatory variables consisting of In Nigeria, like EFCC. The ordinary least squares (OLS) econometric method was used for estimation. Empirical evidence shows that financial technology has a significant impact on cybercrime in Nigeria. ATMs, Internet, and mobile banking facilities in particular are positively and significantly associated with cybercrime in Nigeria. Further evidence shows that cybercrime-fighting agencies such as the EFCC have a negative relationship with cybercrime rates, albeit with a weaker impact, with more active efforts on the part of the EFCCC to curb cybercrime in Nigeria. This suggests that more efforts are needed. Given the empirical evidence, the development of sophisticated new and innovative cybercriminals to tame technological devices is essential. This should go hand in hand with strong institutional capacity such as the EFCC and strengthening the legal and judicial framework.

Reducing the incidence of cybercrime in Nigeria to negligible levels.

CHAPTER ONE

INTRODUCTION

1.1 Background to the Study

It is recognized that society mainly relies on the internet and other information technology tools to engage in personal communication and conduct business activities, among other benefits. The advent of the Internet and other information technologies has brought financial technology. Fintech companies can be traced back to some of the regulatory changes made after the Great Depression of the 1920s. The interest that a typical bank depositor could earn on a deposit his own) - stimulated, in the 1970s, the emergence of wealth management firms and other shadowy forms of banking - aka FinTech companies today. However, it was the global financial crisis of 2008 and the near collapse of the financial system that caused the rise of FinTech companies and triggered the FinTech transition that the world is experiencing.
present witness (Lakshmi, 2015). Over the years, financial institutions in Nigeria have changed positively to compete with international business standards. The main role of a financial institution is to facilitate financial transactions, protect customer information/records, provide other financial services, and provide security if required. Information technology is a major means of communication
has facilitated customer satisfaction, but has come with demanding security challenges

interests of financial institutions and clients in Nigeria. Almost all financial institutions today use a centralized application to manage their day-to-day operations from their headquarters, under the supervision and control of the central bank. Nigeria (CBN) through its affiliates.

The emergence of fintech has added value to the Nigerian financial system. It has brought services such as Online Transfer, Mobile Payment and Banking, Semantic Data Warehouse, ATM, Electronic Funds Transfer, Point of Sale and Electronic Checking among others. Nigeria has the highest number of internet users and mobile telecommunications subscribers in the world, which has fueled the patronage of e-banking (Ibrahim, 2020). Trading is now simplified and user-friendly as customers can now trade from the comfort of their own home, using the app,
shortcodes and other after-sales services.

As fintech companies and startups continue to disrupt the global financial landscape, the biggest benefit is that they are not held back or burdened by laws, regulations, or legacy systems. In addition, they are more agile, more aggressive, and more willing to explore and make risky choices. However, to mitigate the threat posed by fintech, financial institutions must hire cybersecurity experts to help them manage cybersecurity challenges, build high-strength firewalls, Implement strong authentication controls, train employees on security measures, and improve physical security. The Nigerian government has also taken remedial action by establishing a National Cyberspace Administration.
Security Initiative (NCI) in 2013 and the Nigeria Cybercrime Working Group (NCWG).

1.2 Statement of Research Problem

With the development of the online financial environment comes new and existing threats. The shift to centralized control of financial management, information sharing and customer service in the Nigerian financial system has increased the number of cybercriminals making it difficult to track, detect and prevent crimes. that becomes difficult. A number of cyberattacks are causing financial institutions to cause major damage in new and important ways, some of which are online fraud and Internet identity theft (Gercke, 2006).). Cybercrime not only affects financial institutions in Nigeria but also prevents foreign investors from investing in Nigeria (Ogunlere, 2013). Nigerian commercial banks lost more than NGN 15 billion ($39 million) in 2018 due to cybercrime and wire fraud, after which the rate of cyber fraud increased, customer deposits were lost loss was recorded totaling 1.9 billion NGN on every year (Ogbonnaya, 2020). Cybercrime has an increasing tendency to affect the financial sector in the form of website fraud, credit card fraud, ATM fraud, identity theft, and denial of service attacks. The loose nature of the Internet, lack of national functional databases, corruption, lack of standards and central control of the country affect the rate of cybercrime in the country. Banks are also in dire need of help, as a total of NGN 203 billion has been lost to debit and credit fraud over the past 14 years, with some cases going unreported (Adelmola, 2019). Although the provisions of law and
Security measures were put in place to limit this threat, he made little or no effort.

Furthermore, a scan of the existing literature shows that there is empirical evidence of a relationship between cybercrime and fintech in Nigeria. So this study wanted to examine the relationship between cybercrime and fintech in Nigeria.

1.3 Research Questions

i. What is the relationship between incidence of cybercrime and financial technology in Nigeria?

ii. To what extent does the incidence of cybercrime influence financial technology in Nigeria?

1.4 Objectives of the Study

The main objective of the study is:

To critically examine the relationship between cybercrime and financial technology in Nigeria.

The specific objectives are to:

i. Investigate the relationship between incidence of cybercrime and fintech in Nigeria.

ii. Examine the extent to which cybercrime influences financial technology in Nigeria.

1.5 Statement of Hypotheses

The hypotheses of the study will be tested in null form:

Ho1: There is no significant relationship between incidence of cybercrime and financial technology

Ho2: Incidence of cybercrime does not influence financial technology to any significant extent

1.6 Significance of the Research

The significance of this study cannot be over emphasized.

First, it will shed light on financial technology and the incidence of cybercrime in Nigeria and hence aid the formulation of policies to reduce the incidence of cybercrime in Nigeria.

Secondly, it will provide the foundation for researchers to embark on further study in the subject area. Finally, the study will provide useful insight to government policy makers and management of cybercrime in Nigeria.

1.7 Scope of the Study

The scope of this study covers deposit money banks that uses technology to improve activities in the financial industry.

1.8 Limitations to the Study

One of the main limitations of this study was the problem that previous researchers extracted consistent and accurate data from a relevant data source. However, this limitation will be mitigated by trying as much as possible to stick to recent data from CBN annual report and newsletter, as these sources are more reliable than in Nigeria.

Other limitations stem from the failures and pitfalls of various preliminary testing and estimation techniques used by the previous researchers behind the study. However, efforts will be made to ensure that the results of the study are accurate and reliable. for political significance.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This chapter provides an overview of the prevalence of cybercrime and financial technology in Nigeria in keeping with the goals of this study. This chapter also provides a brief overview of earlier research that was conducted by different researchers to address issues related to the study's research issues. An effort was made to examine their various conclusions and determine whether they were similar or incompatible in order to establish the
There is a need for more study on this subject.

2.2 Conceptual Review

2.2.1 Concept of Cybercrime

According to Halder and Jaishankar (2011), cybercrime is an offense committed against a person or group of people with the purpose to ruin their reputations as well as irreparably destroy the hardware of crucial infrastructure, such as the internet and mobile phones. Similarly, the largest computer security firm in the world, Symantec Corporation, defines cybercrime as any crime committed using a computer, network, or hardware devices (Theohary & Finklea, 2015).
During the 10th conference on Prevention of Crime and Treatment of Offenders, conference devoted to combating computer cybercrime was conducted by the United Nations General Assembly, cybercrime activity was divided into two define. First, cybercrime in the narrow sense of the definition is illegal activity directed at

by electronic operations to secure computer systems and the data they process. Second, cybercrime in the broader sense of the definition is illegal activity carried out using or about a computer system, including crimes such as the unauthorized possession and provision or distribution of information using a computer. system (United Nations, 2005).

2.2.2 Categories of Cyber Crime

i. Hacking: It uses vulnerabilities and weaknesses in the operating system to destroy data and steal important information from the victim's computer. This is usually done through the use of a backdoor program installed on the computer. Similarly, some hackers try to access resources with password cracking software. Sometimes hackers can install some programs on the system without the user's knowledge. These programs can be used to steal personal information such as passwords and credit cards. information.

ii. Cyber-Theft: It involves the use of computers to steal crucial data stored electronically. Bank systems are hacked by cybercriminals, who then transfer funds to their own accounts. The quantity of money that can be transmitted illegally is greater. Because they are concerned about alienating their shareholders and clients, the majority of banks and businesses choose not to disclose that they have been the victims of cyber-theft. One of the most common cybercrimes is cyber theft since competent cybercriminals may quickly earn a substantial sum of money from it with little effort.

iii. Viruses and worms:

it is a major threat to computer users and businesses. Viruses are dangerous programs designed to damage the computer. It's called a virus because it spread from one computer to another like a biological virus. Viruses are usually attached to some program or document through which it enters the computer.

iv. Spamming: It entails sending a significant volume of email to advertise and promote goods and websites. Due to the high overhead costs it generates from bandwidth use and the time required to download and remove spam email, email spam is a severe problem for organizations. Additionally, spammers are coming up with sophisticated strategies to get past spam filters, like permuting the substance of emails and using imagery that is invisible to spam filters.

v. Financial Fraud- They are also known as "Phishing" schemes. It takes some social engineering because the criminals must assume the identity of a reliable employee of a company, frequently the victim's bank.

vi. Phishing (Identity Theft, Credit Card Theft, Fraudulent Electronic Mails): This involves sending a user an email while making up the identity of a well-known, reputable company in order to trick them into handing over personal information that will be utilized for identity theft.

vii. Cyber harassment:

This involves purposely doing threatening activities against people using electronic means, such as cyberstalking.

viii. Cyber laundering:

This is an electronic transfer of money that was obtained unlawfully with the intention of concealing its origin and perhaps its final destination.

ix. Website Cloning:The rise of phony "copy-cat" websites that prey on customers who do not know the precise website address of the actual business they intend to visit is a current trend in cybercrime. The client might think they are

When you enter credit card information to buy things from the intended retailer, you're actually unintentionally adding that information to a fraudster's personal database. The fraudster will then utilize this information for his personal gain or to sell to other people who want to steal credit card details.

2.2.3 Dimension of Cybercrimes

According to Broadhurst (2006), computer crime includes traditional crimes in which computers play a key role in the offense as well as criminal actions that are best defined by its distinct typology of computer-related crime. The following are included but not limited to the following:

i. Interference with lawful use of a computer: cyber vandalism and terrorism; denial of service; insertion of viruses, worms, ransomware and other malicious code.

ii. Dissemination of offensive materials: pornography/child pornography; on-line gaming/betting; racist content; treasonous or sacrilegious content.

iii. Threatening communications: extortion; cyber-stalking.

iv. Forgery/counterfeiting: ID theft; IP offences; software, CD, DVD piracy; copyright breaches et cetera.

v. Fraud: payment card fraud and e-funds transfer fraud; theft of Internet and telephone services; auction house and catalogue fraud; consumer fraud and direct sales (e.g. virtual ‘snake oils’); on-line securities fraud.

vi. Others include illegal interception of communications; commercial/corporate espionage; communications in furtherance of criminal conspiracies; electronic money

laundering.

2.2.4 Causes of Cybercrime in Nigeria

Hassan (2012) identified the following causes of cybercrimes in Nigeria, they are:

i. Urbanization – The rapid urbanization in Nigeria, manifested mainly in the rapid population growth, is a challenge for policymakers. The urban population is growing at an annual rate of 4.3% (WDI, 2016). It is much higher than the sub-Saharan African average and continues to put pressure on available resources in Nigeria's cities. For example, only 32.8% of the urban population had access to improved sanitation facilities in 2015 and about 68.5% of the urban population had access to a safe water supply during the period. this (WDI, 2016). According to Meke (2012), urbanization only benefits when many good jobs are created in cities, in the context of high population growth. His research concludes that urbanization is one of the main causes of the increase Cybercrime in Nigeria.

(ii) Unemployment – The unemployment rate in Nigeria is high and stood at 23.1% in the fourth quarter of 2018. The youth unemployment rate is now above 47%. According to Okafor (2011), high unemployment in Nigeria has socioeconomic, political and psychological consequences. This phenomenon favors the growth of street youth and urban children ("neighborhood boys"), who grow up in a culture that encourages delinquency.
behavior

(iii)Quest for wealth -

The carnal instinct to seek wealth is another cause of Cybercrime in Nigeria. For a business to be successful, it is expected that the rate of return on investments that are growing at a geometric speed, with minimal risk. Cybercriminals want to invest the minimum amount of capital in a favorable environment to get the maximum benefit when They try to get rich in the fastest ways possible.

(iv)Poor Implementation of Cybercrime Laws and Inadequately Equipped Law Enforcement Agencies – According to Laura (2011), African countries have been heavily criticized for inadequately handling cybercrime due to inadequate infrastructure and capacity of designated law enforcement agencies. The private sector is also lagging behind in protecting itself from smart cybercrime, including Nigeria. There is no sophisticated hardware to hunt down cybercriminals in a forensic way. In some cases, cybercrime laws are circumvented by criminals. It should be noted that law enforcement agencies in Nigeria such as EFCC and ICPC have successfully prosecuted cybercriminals over the years. However, many
Improvements can still be made.

(v) Negative Role Models - bYouth are the mirror of society. According to Meke (2012), many parents transmit criminal tendencies to their children through socialization. If this continues unchecked and values are absorbed by the younger generation, they will see there's nothing wrong with cybercrime.

(vi)Corruption – Nigeria continues to occupy a disdainful place in the global corruption rankings. In 2018, Nigeria was ranked the 144th most corrupt country in the world out of 176 countries studied by Transparency International5. People celebrate wealth without questioning the source of that wealth. It is common to hear about people
Suspicious character and famous wealth in society. This bad arrangement To Wealth encourages a get-rich-quick mindset that can be pursued through Cybercrime .

(vii) Gullibility/Greed – Most victims of cybercrime display some degree of gullibility and/or greed. Some people trade in the hope of making a profit without in-depth investigations. These people fall prey to cybercriminals.

(viii) Poverty - Jolaosho (1996) defined poverty as the inability to afford a sufficient supply of food, shelter, clothing, and leisure activities. Therefore, lack of fundamental necessities for human comfort and existence constitutes poverty. A person in need may unintentionally turn to crime to survive. As of 2018, almost 50% of Nigerians were living in extreme poverty.

(ix)The Proliferation of Cyber Cafes and the Porous Nature of the Internet –

It's important to remember that due to the nature of the internet, attacks can originate from anywhere in the world and be carried out wherever the criminals see fit. As a result, geographical and political boundaries are irrelevant. Another significant factor contributing to the rise in cybercrime is the development of cybercafés.

2.2.5 Effects of Cybercrime

Hassan (2012) listed the following impact of cybercrime:

(i) Reduction in Competitive Edge-When a hacker takes a company's private data and future plans and sells it to a rival, the company may lose its competitive advantage and incur losses. The time that IT staff spent repairing damaging situations brought on by cybercriminals could have been used to generate revenue for the company.

(ii) Productivity Losses and Rising Cost-Additionally, cybercrime lowers an organization's productivity because enterprises must take precautions to stop it by securing their networks. This takes time and has an impact on production. Organizations also purchase security software to control malware and viruses and lessen the likelihood of assaults. This results in higher overhead costs and lower profit margins due to computer crime. In addition, removing undesirable communications costs time and attention from people and uses up resources on the computer and network.

(iii) Monetary Losses- Cyber assaults have a financial impact on economies and enterprises in the form of intellectual property loss, financial fraud, reputational harm, decreased productivity, and third-party responsibility. A percentage of the stated cost of cyberattacks and viruses is made up of opportunity cost (missed sales, poorer productivity, etc.). Opportunity costs, however, may not necessarily result in costs to the national economy. Financial fraud and online intellectual property theft cause more harm to businesses. Therefore, there will undoubtedly be enormous financial repercussions in areas where cybercrime is rampant (particularly in relation to enterprises and financial institutions).

(iv)Destroys Country's Image- The reputation of a nation is damaged by cybercrime, which is one of its main negative effects. Whenever a nation is identified as a haven for cybercrime, potential investors are reluctant to make investments there. The macroeconomic stability of the country will be severely impacted by this.

(v) Retards Financial Inclusion-

Financial inclusion is discouraged in a country where cybercrime is prevalent because people are afraid of being attacked online.

2.2.6 Cybercrime in Nigeria

Salawawa Today, technology is readily available, making it accessible to both offenders and victims (Clough, 2010). Clough (2010) argues that with the development of information technology and the convergence of communication and digital devices, the Internet has changed the way we interact and conduct business around the world. While this is a positive development, it also has a dark side, as virtually every advancement in the digital realm comes with a "corresponding niche for criminal

exploitation." . According to Longe et al. (2009), Sub-Saharan Africa (SSA) is the last continent to adopt Internet and mobile technologies. Internet usage rates in sub-Saharan Africa have increased, with most countries relying on private Internet hotspots such as as Internet cafes for their daily Internet activities. In Nigeria, it is recognized that cybercrime is one of the problems hindering global online transactions due to the pervasive nature of fraud and computer-related crime. Abubakar & Salawa (2014) reported that due to the integration of digital technologies worldwide, the economies of most countries in the world are accessible through the use of information technology. and media. Adesina (2017) states that Cybercrime is a very common crime in Nigeria as criminals are widely known to attract people all over the planet into various phishing scams like spam and "smart" Cooperative scam designed but laundered.
Nigeria has about 186 million inhabitants and about 97 million internet users, accounting for a penetration rate of about 52% (Internet World Stats, 2016). However, Nigeria is currently ranked 24th in the world in terms of cybercrime reported by complainants and 12th in losses caused by complainants (Internet Crime Complaint Center, 2014). This is considered a significant improvement over the Internet Crime Report (2010) which ranked Nigeria in third place with 5.8% just behind the United States.
with the highest prevalence of cybercrime activities in the world.

2.2.7 **Impact of Cyber Crime on Nigeria Banking System**

It has been observed that a vibrant economy thrives on an efficient and efficient financial system. Cyber attacks are often aimed at financial gain. financial institutions, especially banks, suffer the consequences of such acts. The effects of cybercrime on the Nigerian banking system include:

i. Huge increases in the operating cost of banks due to huge expenses incurred on purchase of security software applications to reduce the rate of cyber attacks.

ii. Serious failures of institutions lead to huge losses due to cybercriminals - this can lead to loss of confidence in financial institutions and possible withdrawals from them (when relevant banks), with possible contagion effects.

iii. This results in higher provisions - while provisions for loan loss are predictable with To some extent, losses due to cybercrime are unpredictable; leading to an increase in bad provisions and consequent depletion of capital of banks and commercial organizations. This can reduce the level of confidence in the national financial system.

iv.
Regulators and supervisors of licensed depository institutions may be required to use taxpayer funds to address issues arising from cybercrime. This can be in the form of problematic deposit institutions receiving relief through prompt remedial actions, or when institutions (banks) eventually go bankrupt and deplete the Deposit Insurance Fund. DIF) to reimburse depositors. Various methods by cybercriminals in Nigeria include: stealing/copying customers' bank cards; fraudulent transfers or withdrawals of customers; hack into banking software to transfer money; clone bank/corporate websites to fool customers and send emails/text messages asking for personal information or help from unsuspecting people. Over the years, automated teller machines (ATMs) and web-based fraud (online banking) have contributed significantly to frauds in the Nigerian banking system.

Table 1 shows the contribution of cybercrime to total fraud losses in Nigeria banking system in the period 2011-2016.

Table 1: Contribution of Cybercrime to Total Fraud Loss in the Nigerian Banking

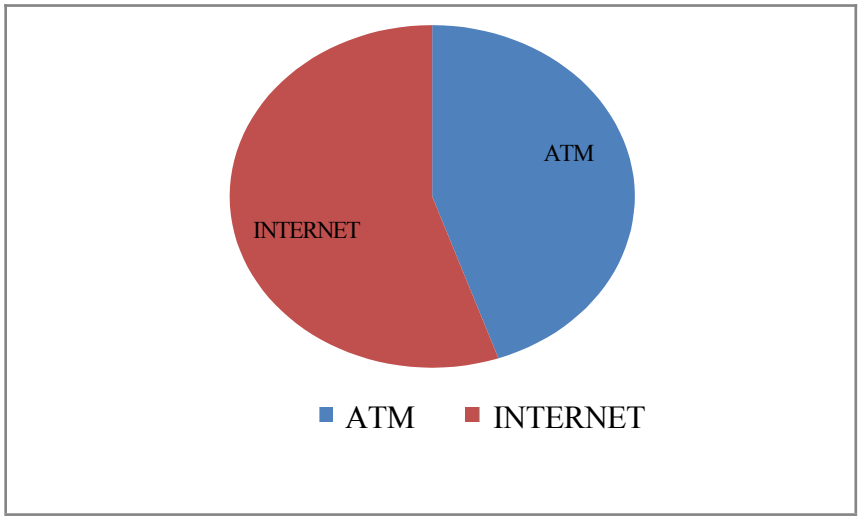
Industry (2011 - 2016)

Year	Cybercrime losses(ATM & INTERNET) (₦ billion)	Growth rate of cybercrime losses (%) year-on- year	Total Fraud Loss (₦ billion)	Contribution Of Cyber Crimes To Total Fraud (%)
2011	0.115	-	4.071	2.82
2012	0.794	590.4	4.516	17.58
2013	2.268	185.6	5.757	39.40
2014	4.438	95.6	6.193	71.66
2015	1.361	-69.3	3.173	42.89
2016	1.058	-22.2	2.4459	43.26

Source: NDIC Annual Report (2011-2016)

The second column shows actual cybercrime damage over the years, while the third column shows year-over-year growth. From 2015, one can infer a gradual decrease in losses due to cybercrime in Nigeria. It fell further in 2016 to 22.2%. This largely reflects the positive performance of agencies like the EFCC in the fight against cybercrime. This also shows the effectiveness of the Nigeria Cybercrime Act 2015. On the other hand, Table 2 shows that, in recent times, cybercrime losses accounted for almost half of all reported bank fraud losses. In 2011 it was only 2.8%. It increased significantly to 71.6% in 2014 and gradually decreased to 43.2% in 2016. A
The main inference from this is that cyberspace is a major channel through which Fraud is carried out in the Nigerian banking sector. This repeats the previous position
that increased efforts should be aimed at curbing this criminal activity. Figure 3 analyzes cybercrime in Nigeria by sources in 2016. The two main sources considered are the Internet and Automated Teller Machines (ATMs). It's obvious from that figure; The Internet is the largest channel through which cybercriminals have committed at the bank in 2016.

Figure 3: Cybercrime Dissagregation in Nigeria (2016)



Source: NDIC Annual Report (2011-2016)

Recently, online fraud is a growing concern for investors in financial services. Since the Central Bank of Nigeria (CBN) stepped up efforts to increase cashless transactions in 2014, e-banking fraud has escalated. In 2018 alone, the banking system lost about 15.5 billion naira and about 60% of frauds originated on the internet as banks increased investment in online and related banking services. to technology. Nigerian banks have lost more than 15.5 billion naira ($41.6 million) to fraud, a huge leap from what the industry has recorded
in the previous four years.

The industry lost N12.30 billion to various scams from 2014 to 2017. About 89% of financial services fraud occurs through electronic channels, while only 11% is non-electronic (Nigeria Deposit Insurance Commission, 2018). NIBSS reports that web and mobile also accounted for the highest number of fraudulent channels in Q2 2020, as both accounted for a total of 71.42%, even higher than the 68.65% recorded in the quarter. 3 same year. Mobile fraud volume in the third quarter decreased by 5% compared to the second quarter of 2020.

According to Frank (2021), Nigerian banks lost 3.5 billion naira between July and September 2020 due to fraud-related incidents, an increase of 534% over the same period in 2019 of 552 million naira. The Nigeria Interbank Payments System (NIBSS) in its latest industry fraud report showed the highest number of scams (35.5% of the total) carried out on the web channel, with transactions made using Web browser. Transactions made over the phone resulted in a loss of N410 million, or 11.7% of the total loss. According to NIBSS, the trend since the beginning of 2020 is that web and mobile channels are viable means to profit from fraud exponentially. "Therefore, it is necessary to regularly, proactively measurements around these channels," the report notes.

2.2.8 The Cybercrimes (Prohibition, Prevention, Etc) Act, 2015 Role of Government

The rationale for the Cybercrimes Prohibition ACT 2015 is "to provide an effective, consistent and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrime. provide a framework.
Nigeria". Laws need to be reviewed regularly to adapt to their dynamic nature. A cyber environment to accommodate more crimes and deal with unique cyber-related issues. Similarly, Nigeria's Data Protection Regulation 2019 is another regulation aimed at protecting data both in motion and at rest. However, the Nigerian Criminal Code, Economic and Financial Crimes Commission (EFCC) Act 2004, Advance

Toll Fraud and Other Related Crimes Act, 2006.

According to Okeshola et al., (2013), in order for cybercrime laws to track cybercriminals relatively effectively and efficiently, governments should provide employment and intensive ICT training to law enforcement agencies. graduates should be empowered through the provision of Thus, to reduce cybercrimes in Nigeria, there is the need to create job opportunities for the unemployed youths as well as the need for government, law enforcement, intelligence and security agencies to understand the technology and
individuals engaged in the criminal acts in order to be able to curb their activities.

It has been observed that the impact of cybercrimes is so damming that various tiers of Nigeria governments have come up with different programmes aimed at re-orientating the youth towards positive thinking. Various initiatives directed at protecting the interests of Nigerians in the cyberspace have been put forward. These include National Information Technology Development Agency (NITDA), Nigerian Communication Commission (NCC), Economic and Financial Crimes Commission (EFCC) have all worked toward curbing the menace of cyber-crime in Nigeria. Other notable cyber-crime control initiatives include the setting up of a National Cybercrime Working Group (NCWG) with stakeholders drawn from the law enforcement agencies, the financial sector and ICT

professionals, and a pilot project of a Computer Emergency Response Team (CERT) center by NCWG and NITDA. The upgrade of the Nigerian Financial Intelligence Unit (NFIU) to a full-fledged institution (NFIA) is also a major step for the Nigerian government to step up its fight against cybercrime in the country. On November 12, 2018, in the city of Paris, France, many countries gathered to sign an agreement on safe and secure cyberspace. Paris' call for trust and security in global cyberspace is considered a major achievement in the joint fight against cybercrime. All States reaffirm their willingness to work together to provide support in existing forms and through appropriate organizations and institutions. Pay attention to Areas of cooperation include:

i. Prevents and recovers malicious network activities that pose a significant threat to individuals and critical infrastructure and can lead to system/indiscriminate attacks
harm;

ii.
Verify activities that result in significant damage to the availability or integrity of internet for the majority of people;

iii. Strengthen the collective ability of all members to easily detect and track any interference/misalignment from foreign actors, especially for cyber-harmful actors. attacks on the country's electoral process;

iv. Put in place measures to prevent theft of intellectual property collected in the ICT environment, including trade secrets and other confidential business information. The purpose is to encourage competitive advantage between companies or companies fields;

v.
Capacity building is needed in the areas of preventing the spread of malicious ICT tools and practices to prevent its harmful effects;

vi.
There are identified needs to enhance digital and security processes, as well as products/services, throughout the supply chain lifecycle;

vii. Support efforts to strengthen an advanced cyber hygiene for all actors;

viii. Put in place measures to prevent non-state actors, including the private sector, from carrying out malicious attacks on systems, for their own purposes or for hire. partners in crime;

ix.

Efforts should focus on promoting and implementing internationally acceptable standards, as well as establishing confidence-building measures in cyberspace. .

2.2.9 Role of NDIC

The NDIC is one of the key stakeholders in the national financial system. Deposit insurers and an important part of the nation's financial safety net have recognized the importance of effectively managing all the risks faced by the banking industry, including crime. cyber crime. In carrying out on-site and external oversight duties with the Central Bank of Nigeria (CBN) and other members of the Financial Services Regulation Coordinating Committee (FSRCC), the operations of all companies The custody of licensed financial institutions is subject to regular review by the NDIC. Nigerian banks are required under the provisions of Sections 35 and 36 of NDIC Act No. 16 2006 to submit fraudulent and fraudulent information/reports on a monthly basis to the NDIC. Financial trust organizations should put in place appropriate measures to protect their systems and

combating cybercrime is heavily monitored and enforced by the NDIC. Due to NDIC's efforts to protect depositors and combat violations such as problems between customers and their bankers, from arbitrary interest calculation, account balance manipulation to fraud absolutely as well as cybercrime issues, the NDIC has introduced a 24-hour toll-free number. line: 080063424257 to facilitate bank customers and Publicly report financial abuse for possible investigation and resolution.

2.2.10 Policing Cybercrime in Nigeria

Adesina (2017) states that having strong laws to combat cybercrime is one of the among the main measures taken by the Nigerian government to combat crime. Due to the negative financial and economic consequences of cybercrime in Nigeria, the government has continued to take these drastic measures to curb cybercriminal activity. Measure
was:

a. Creation of a central agency to enforce crime laws

b. Regulation of cybercafés

c. Enactment of Cyber laws

d. Government partnership with Microsoft (Adomi & Igun, 2008).

In 2004, the Nigerian government established the Nigeria Cybercrime Task Force, consisting of government and private sector representatives, to develop legislation on cybercrime. In addition, in 2007 the government established the Directorate of Cybersecurity under the Office of the National Security Advisor to address security issues related to the increasing use of ICT in the world.
country (Adesina, 2017). In addition to these initiatives, new laws have been created such as the Economic and Financial Crimes Act 2004 and the Prepayment Fraud and Other Fraud Act 2006 (Adesina, 2017). However, because the law is not effective in restricting the activities of cybercriminals, the Cybercrime Bill was enacted in May 2015, thus correctly defining cybercrime as illegal. legal. accompanied by penalties for any violations of the law.
The Cybercrime (Prohibition, Prevention, etc.) Act of 2015 was passed to promote cybersecurity and prevent cybercrime. The Cybercrime Act provides for the obligation of ISPs, telecommunications operators and financial institutions to report to and cooperate with law enforcement agencies and the Nigeria Computer Emergency

Response Team (ng-CERT).). Similarly, it requires the National Security Advisor and the Attorney General to coordinate and be accountable for the legal and institutional framework while establishing the Cybercrime Advisory Board to facilitate effective, efficient enforcement. inter-agency/international cooperation, capacity building and multi-stakeholder engagement. (Council of Europe, 2017). For decades, cybercrime has been a key agenda item for the Nigerian government. Fraud investigations carried out by the Department of Economics and Finance Crime Commission (EFCC).
While the admissibility of electronic evidence was revised by the Congressional Evidence Act of 2011, the lack of an adequate legal framework for cybercrime rendered criminal justice remedies invalid. until 2015, when the government adopted the national cybersecurity policy and strategy through an inter-ministerial committee. led by
Office of the National Security Advisor (Council of Europe, 2017).

2.2.11 Solutions to Cybercrime in Nigeria

The following are solutions to cybercrime in Nigeria:

i. Education: Nigerians need to be educated on the impact of Cyber Crime, Cybercrime is extremely difficult to prove to Nigerians as there is no lack of any physical evidence that requires knowledge of ICT professionals ; therefore, the good education of Nigerians encourages them when using the internet to be careful with the information they provide online. In addition, different organizations need training on best practices to Effective security management.

ii. Establishment of Information Technology Platform for Youths: Due to the rising unemployment rate has contributed significantly to the wave of cybercrime in Nigeria. The Nigerian government should create jobs for young people and set up IT programs where talented young Nigerians can come together and showcase their skills. This is possible
significantly used to improve IT development in Nigeria.

iii. The use of Address Verification System: The Address Verification System (AVS) should be regularly checked, which can be used to ensure that the address entered on the order form (for those receiving orders from countries such as the United States). period) corresponds to the address where the cardholder's account statement is mailed.

iv. IP Address tracking:
This software can be used to check the IP address of an order of the country specified in the billing and shipping address in the order.
v. Cyber Ethics and Legislation Laws: Cybercrime ethics and laws are developed by many different countries to prevent cybercrime. It is essential that each individual obey the network
ethics and law so that cybercrime is on the rise and fall. In addition, security Software such as anti-spyware products must be installed on all computers to stay safe from cybercriminals. Nigerian internet service providers should also provide a high level of security on their servers to protect their customers from all kinds of viruses and malware.

2.2.12 Role of Individuals, Financial Institutions and Businesses in Combating Cybercrimes

Across the globe, governments and organizations have found commendable ways to combat cybercrime, some of which have been deployed on the shores of Nigeria. Including:

i. The use of robust firewalls to prevent attacks and filter malware or suspicious malicious

codes.

ii. Consistent training of IT personnel to monitor and detect unusual traffic/intrusions within the deployed I.T infrastructure.

iii. The enactment of stringent laws and prosecution of individuals in breach of same.

iv. Implement secure user access interfaces to ensure that only authorized persons are access the corporate network.

v. Regularly update and upgrade software and applications according to the latest trends global best practice.

vi. There is a need for effective linkage and collaboration between banking institutions. For example, when fraudsters use computers or other information and communication technology infrastructure to transfer funds from an individual account, those funds are sent to or transferred to an individual account. . account at another financial institution. Related organizations should cooperate

effective when such fraudulent transactions are detected.

vii. Enhanced Public Awareness**.**

2.3 Theoretical Review

2.3.1 Routine Activity Theory (RAT)

McQuade (2006) noted that within the framework of classical theory and decision theory, recognition of available opportunities to commit crimes is seen as an essential factor. According to Cohen Cohen and Felson, 1979). . Akers and Sellers (2004) point out that a motivated offender must be someone who has the willingness to commit a crime and the opportunity to forgive it. He pointed out that the assets of motivated criminals, such as credit card information, that the target is viewed and accessible by criminals and may be obtained illegally. Finally, competent guardians must be absent. A competent guardian, such as cryptography, antivirus, or law enforcement, is a person or thing It prevents motivated criminals from achieving their goals (Cohen and Felson, 1979).

2.3.2 General Deterrence Theory

This theory is a combination of Choice Theory and Rational Choice Theory. weight, speed,
Certainty of punishment. A common theory of deterrence is that harsher fines and harsher sentences deter people from committing crimes or encourage them to commit lesser crimes. The key part is to publicize the actual penalties that can occur as a form of deterrence. McQuade (2006) further points out that the imposition and publication of penalties imposed on offenders are fundamental concepts underlying general deterrence theory. Sanctions can also act as a deterrent Prevent individuals from committing her IT abuse and cyber crimes.

2.3.3 Theory of Technology-Enabled Crime

Around the world, the advancement of the Internet and the accessibility of computer technology are creating new opportunities for individuals, businesses, and those who engage in fraudulent activities. New technologies and online communications have not

only resulted in an astronomical increase in criminal activity, but have also led to new forms of deviance and criminal activity online. It has challenged legal systems and law enforcement agencies around the world (Brenner, 2007). This theory combines several components of crime theory to better understand why crimes involving "computer and telecommunications technology" are among the most difficult. Crime Prevention, Investigation, and Control (Olayemi, 2014). McQuade too (2006) point out that the theory of technology-enhanced crime takes into account: (b) technological and economic factors that create innovative forms of social abuse and crime; (c) technical Changes in crime, police and security management. This theory provides a framework for understanding all forms of crime, especially deviant behavior, committed online or using telecommunications technology. This theory is also important for studying contemporary threats posed by new trends in cybercrime, transnational crime, and terrorist networks.
(Oraemi, 2014).

2.3.4 General Theory of Crime

A general theory of crime was developed by Gottfredson & Hirschi (1990). Gottfredson & Hirschi (1990) argued that their theory has universal status because it is valid across time and space. Both authors argued that theories of cultural imbalance, defined as theories related only to particular cultures, tended to dominate traditional comparative criminology. proponents of the theory noted that each culture has its own definition of crime and historically identified root causes of crime and deviation. Therefore, it is not possible to develop a theory to explain common "criminal factors in different cultures". Thus Gottfredson and Hirschi (1990) point out that: Real differences between cultures
crime rate. Furthermore, Gottfredson & Hirschi (1990) found that people who commit crimes
They define them as "violent or fraudulent acts of self-interest." Characterized by low self-control that forms the core concept of popular crime theories. They further noted that individuals are ruled by pain, pleasure, and selfishness, and therefore do not have an "innate conscience that needs to transcend them and socialize them to morality." Marenin & Reisig (1995) point out that Nigeria is an oil-rich, but growing, developing country whose population needs depend on the enormous demand generated by income from oil. It suggests that the amount is exceeded. The challenges of population concentration and low per capita income include widening and visible disparities in wealth and lifestyle, the importance of class in public life, and the potential for large-scale corruption within countries. includes gender. Crime in Nigeria can be divided into three categories: ordinary crime, politico-economic crime and seditious crime. A challenge to Gottfredson and Hirschi's (1990) general theory is the different levels of crime in Nigeria. The Gottfredson & Hirschi (1990) theory must take into account key country-specific factors such as status development, political instability, economic uncertainty, and group dynamics. Personal factors such as self-control also play a role in these general contexts. According to Marenin and Reisig (1995), the overwhelming majority of Nigerians are still law-abiding despite all temptations and social pressures. Some people commit crimes according to popular theories of crime, while others do not despite their lack of self-control. According to Odekunle (1986), the activities of the country's elite do much more damage to the country's reputation and public than ordinary crime and working-class crime. Odekunle (1986) further argues that: Their crimes are part of their routine and normal routine and functioning.
The cost to the country of their crimes is immeasurable, but enormous and cumulative,
dangerous. "

2.4 Empirical Review

Haru (2021) explores cybercrime challenges in online banking in Nigeria. This research was a theoretical study based on the risk society theory. The study argues that advances in information and communications technology have had unimaginable consequences, including criminal activity, spam, credit card fraud,

ATM fraud, phishing, identity theft, and other related cybercrime. This research paper found that widespread cybercrime is having a negative impact on online banking systems. This is because it leads to huge economic losses, threatens profitability, tarnishes the country's image on a global scale and often discourages foreign investors from investing in the investor country. The study found that investors and customers can protect themselves from cybercriminals by applying simple security tips, such as up-to-date, legitimate antivirus software, to avoid disclosing personal data to third parties. I conclude that it must be preserved. You can also prevent security by using very strong passwords and changing passwords regularly

violation. Victoria et al., (2018) Examines Internet Banking innaigerie: Cyber Security Breaches, Practices and Capabilities summarizes the findings of a research project on cybersecurity in the Nigerian Internet banking industry by presenting the major cybersecurity breaches. reporting. Experienced cybersecurity skills and practices. For this study, we conducted an online survey of her 100 experienced professionals working in both banking and banking in Nigeria. Bank security services department. The results of the research are Nigeria's cybercrime industry ranges from low-tech cybercrime to sophisticated high-tech breaches involving viruses, worms or Trojan horses. Electronic spam; and hacking are the three most commonly experienced security breaches. When it comes to cybersecurity practices, banking professionals are well-managed, both in support and training. Lack of advanced technology to prevent and mitigate cybersecurity breaches and poor regulatory compliance appear to be the main factors in the decline in cybersecurity capabilities in the sample of banks. Similarly, Omodunbi et al., (2016) reviewed Cybercrime in Nigeria: Analysis, Detection and Prevention. The primary objective was to assess the extent of students' involvement in cybercrime and determine their vulnerability to such crime. The study employs a variety of research questions conducted among students from selected universities in Ekiti state. The research assignments were distributed to the Federal Universities, Oye-Ekiti (FUOYE), Ekiti State University (EKSU) and finally Afe-Babalola University (ABUAD). The survey included a total of 600 students aged 15-26 from the three institutions combined. These universities are specially selected because they cover all kinds of universities, such as state, federal, and private universities that a person can attend. The results of this study show that most crimes committed by young people in our society are primarily due to phishing. While many ways have been proposed to prevent future occurrences of this crime, there is still much that governments and individuals can do to reduce it. We recommend that

Most Important Citizens Relieving Individual Burdens Through Provision Well paid jobs and other basic amenities. Last but not least, this makes people's lives more comfortable and less involved in criminal activities for survival. Only then can bills or laws against cybercrime actually come into force. You should also be smart and follow the precautions above to avoid becoming a victim. Moreover, young people are most involved in this crime and therefore need to be oriented, educated and empowered for the country.

We have a bigger future. Similarly, Fadare (2015) investigated cybercrime and its impact on online her banking facilities in Nigeria. The purpose of this study is to examine the impact of ICT tools to combat cybercrime in online banking in Nigeria. This study addressed the problem of cybercrime in terms of theoretical and practical contributions. Data obtained from these investigative tools were used in descriptive analysis and analysis to illustrate the behavior of Nigerian cybercriminals based on online banking and how ICT tools can be used to prevent these crimes. A regularity analysis was performed. The study concludes that complex cybercrime is, by its very nature, considered difficult to deal with. Combatting malfunctions involves unified and synchronized tactics facilitated by dynamic ICT security systems. Therefore, there is a need for a cyber activity policy that protects outsiders interested in making money within and in Nigeria. Finally, fighting cybercrime and cybersecurity threats in Nigeria requires not only an understanding of information technology, but also intelligence in information technology of all residents.

CHAPTER THREE

METHODOLOGY

3.1 Introduction

This chapter described study design, study population and sample, data sources, theoretical framework and model specification, measurement and operationalization Data analysis variables and methods.

3.2 Research Design

A post hoc study design was used in this study. This applies especially to management and social sciences. The use of secondary data in post-hoc study designs includes investigation of response and individual effects on factor disposition. researchers do not have the ability or opportunity to modify or manipulate them independent variable.

3.3 Population and Sample of the Study

The study population is the entire Nigerian economy, but with a single sample. Annual time series from 2000 to 2021.

3.4 Sources of Data

The data used in the study are secondary data obtained directly from CBN. Statistical Bulletin (various editions) and Nigeria Deposit Insurance Commission (NDIC)

3.5 Theoretical Framework

This research is based on technology-enabled crime theory. This theory is supported by the advancement of the Internet and the accessibility of computer technology. Created new opportunities for individuals, businesses and stakeholders Fraud. Consistent with theory, new technologies and online communications are leading not only to an astronomical increase in cybercrime and criminal activity, but also to new forms of deviance and criminal activity online. posed challenges to both the legal system and law enforcement institutions worldwide (Brenner, 2007). This theory combines several components of criminological theory to understand why "computer and telecommunications technology" related crime is one of the most difficult forms of crime to prevent, investigate, and control. (Olayemi, 2014). Furthermore, McQuade (2006) pointed out that technology-enhanced crime theories take into account: (b) technological and economic factors that create innovative forms of social abuse and crime; (c) technological changes in criminal investigation, police and security management functions; This theory provides a framework for understanding all forms of crime, especially deviant crime.

Conduct committed online or using telecommunications technology. This theory is also important when examining the current threat posed by new trends in cybercrime, transnational crime, and terrorism networks that defy the criminal justice system's traditional approach in preventing and combating crime (Olayemi, 2014, cited in Rogers, 1962). . .The theory further argues that all institutions seeking growth must be open to innovation. This theory posits that innovation has five important attributes. Consistently improve the current mod operand approach to performance, pre-test capability, and easy defect detection (frame & Scott, 2001). According to Hirtle (2005), innovation enables institutions to gain competitive advantage and minimize operating costs. In addition, financial institutions can easily enter new markets and find alternatives to serve them. client.

3.6 Model Specification

The model for this study is functionally expressed as follows;

INCYB = CYBCf(ATM,MMO,IBS)……(3.1)

The econometric form of the model is specified as;

Where;

INCYB= Incidence of cybercrime related frauds in Nigeria, at time t

ATM_{it} = *Automated Teller* cybercrime losses *at time* t

INTER= *Internet* service related cybercrimes *at time t*

MB = Mobile banking related cybercrimes *at time t*

INST= Legal and cybercrimes fighting institutional framework, such as the Economic and Financial Crimes Commission (EFCC) *at time t* .

Including major cybercrime agencies like the EFCC in the model is beneficial. Because containment or suppression of cybercrime in Nigeria cannot be achieved without a strong cybercrime task force like the EFCC. what was in the foreground.

β_1 *-are the coefficients of the independent/explanatory variables of interest.*

Based on theoretical or apriori expectation, the signs of the coefficients are given as; β_1 ->< 0;

3.7 Measurement and Operationalization of Variables

Table 3.1: Operationalization and Measurement of Variables

Item	Operational Definition	Variable Type	Measurement
Incidence of Cybercrimes	INCYB is operationally defined as the intensity of terrific frequency of occurrence of cyber related offences.	Dependent	Intensity of cybercrimes in terms of total recorded
Automated Teller Machine	ATMs are computer-controlled machines that issue cash and other services to customers who provide a personal identification number (PIN).	Independent Variable	Total number of ATM related cybercrimes.

Internet Service	INTER means that a bank's customers can access their account and general information about the bank's products and services through the bank's website without the hassle and hassle of sending letters, faxes, original signatures, and phone confirmations. It is a financial engineering system that makes	Independent variable	Total level of cybercrimes. Cybercrimes carried out through internet transactions/services.
Mobile Banking	MB are licensed mobile money service provider that develops and deploys financial services through mobile phones and mobile telephone networks.	Independent variable	Total number of mobile money related cybercrimes.
Cybercrimes Fighting Institution	Institutions/agencies/commission responsible for fighting cybercrimes in Nigeria, e.g. the EFCC.	Control variable	A dummy variable where 1 represents existence and reforms (strengthening) of EFCC and 0, otherwise.

(Source: Author's compilation, 2022)

3.8 Method of Data Analysis

The empirical model estimation method is the ordinary least squares (OLS) econometric technique. The choice of estimation method is based on the best, linear, unbiased estimator (blue). Econometric software evaluation is used for analysis.

CHAPTER FOUR

DATA PRESENTATION, ANALYSIS AND INTERPRETATION

4.1. Introduction

This chapter focuses on the empirical analysis of the results according to the strategy applied to the study. The study aimed to empirically examine the relationship between fintech and cybercrime in Nigeria. Three key variables were used to capture the fintech dimension and composition of cybercrime (ATM – ATM, internet services and mobile banking), including a control variable – the institutional setting to capture. capture the role of legal authorities and cybercriminals, such as the EFCC. The conventional least squares (OLS) estimation technique was applied to the empirical analysis. The estimated results are presented and then interpreter.

4.2. Empirical Results

The results of the empirical estimation using the OLS econometric technique is presented in Table 4.1.

Table 4.1 OLS Result Estimates

Dependent Variable: INCYB

Variables	Coefficient	T-Ratios	Prob.
C	0.032	1.134	0.30
ATM	0.073	2.188	0.04

INTER	1.163	3.132	0.00
MB	0.052	2.136	0.04
INST	-0.054	- 1.303	0.18
$R^2 = 0.767$	F =22.72[0.00}	DW = 1.82	
Adjusted R^2=0.735			

Source: Author's computation from EVIEWS Output

An examination of the results show an adjusted R^2 of 0.735 for the cybercrimes model, an indication that about 74 percent of the net systematic variations in incidence of cybercrimes is explained by the combined explanatory variables. The model therefore has a good predictive capacity. Invariably, the combined fintech variables, including the control variable, explain the wide variation in cybercrime rates in Nigeria. The overall goodness of fit statistic is expressed as an F value of 22.72 which is statistically significant at the 1% level. Thus, the hypothesis of a significant linear relationship between fintech and the rate of cybercrime in Nigeria has been validated. Durbin Watson's statistic 1.82 indicates that there is no autocorrelation in the model, making it robust and consistency for policy formulation and implementation.
In terms of the contributions of individual variables, the focus is on the sign of the estimated coefficients and their respective t ratios. The coefficient of ATM and internet banking has a positive relationship with cybercrime according to technology theory-
Crime activation and significance at 5% and 1% respectively. Invariably, fintech has contributed greatly to the intensity of cybercrime in Nigeria, especially over the internet, which is huge in size and volume. Information and communication technology has caused unimaginable consequences such as criminal activities, spam, credit card fraud, ATM fraud, fraud, identity theft and cybercrimes. other relevant. These have led to huge financial losses, threatened profits and tarnished the country's image globally, along with a decline in foreign investment. The results support the conclusions of Gercke (2006), Fadare (2015), Omodunbi et al., (2016), Victoria et al., (2018), (Ogbonnaya, 2020) and with Haru's submission, (2021). The mobile banking coefficient has a positive sign and is statistically significant at the 5% level. The positive and significant sign clearly indicates that mobile banking activities significantly promote the rate of cybercrime in Nigeria. discovered is consistent with the conclusions of Gercke (2006) and Omodunbi et al., (2016). The coefficient of institutional frameworks responsible for combating cybercrime-related crime, such as EFCC, is negatively related to cybercrime but is not significant at 5%. Therefore, strong cybercrime legal and institutional authorities have the ability to reduce the rate of cybercrime in Nigeria, but this capacity is weak. For example, the EFCC's low ability to tame cybercrime is due to insufficient funding, weak legal processes and jurisdiction, the latter being very slow in Nigeria due to political interference from major powers and racial prejudice. For example, a number is "highly set" individuals generally have the political and financial means to buy their way and escape justice when convicted, while some are treated like "sacred cows", with the deceptive illusion of being above the law or enjoying something special; exclusive right. These things tend to
undermine the fighting spirit of the EFCC and other cybercrime control organizations.

4.3. Test of Hypotheses

In order to investigate whether the hypotheses stated in the study are accepted or rejected based on the empirical results, they are empirical testing are conducted as follows:

Hypothesis 1

Ho1: There is no significant association between cybercrime rates and financial technology. Experimental results show that the coefficient t-ratios (representing cybercrime enabled by financial technology) of 2.189, 3.13, and 2.14 (in absolute values) for ATM, Internet banking, and mobile banking are significant, respectively. . 5 percent. Therefore, the null hypothesis is rejected in favor of the alternative hypothesis.

Hypothesis 2

Ho2: Financial technology does not does not significantly influence incidence of cybercrimes in Nigeria. Based on the empirical results, the t-ratios of the coefficients of ATM, internet banking and mobile banking (which collectively represent financial technology enabled cybercrimes) of 2.189, 3.13 and 2.14 (in absolute terms) are significant at the 5 percent, respectively. The null hypothesis is therefore rejected, while the alternative hypothesis is accepted.

4.4. Discussion of Findings and Policy Implications

The empirical findings of this study have important policy implications. First, the financial technology of the electronic revolution (fintech) has increased the size and scale of cybercrime in Nigeria to an unimaginable scale due to the sheer number of skills on the part of the perpetrators. The growth of the online financial environment has always been accompanied by new and existing financial threats that have caused economic losses on an increasingly large scale. As a result, new, complex and rigorous technologies must also be developed to tame and nip cybercrime in the bud. Continuous innovation and advanced technology will significantly reduce, if not eliminate, the frequency, severity and scale of cybercrime.
Nigeria. Second, empirical findings show that Internet-induced cybercrime has greater scale and impact than other elements of financial technology-based cybercrime. The use of the Internet has always demystified complex financial codes, deciphering and breaking secret centralized controls of financial controls and other secret lockdowns. With strong local and global collaboration, technologically advanced cybercrime detection devices/software are
It is therefore important alongside a strong agency to contain threats.

CHAPTER FIVE

SUMMARY OF FINDINGS, CONCLUSION AND POLICY RECOMMENDATION

This chapter is concerned with the summary of findings, conclusion and recommendations.

5.1 Summary of Findings

This study empirically examines the relationship between cybercrime occurrence and financial technology in Nigeria. The impact of financial technology (fintech) on Nigeria's banking efficiency, using annual time series data for the period 2000-2021, which characterizes the era of significant cybercrime in Nigeria. Empirical results using the OLS econometric method show a positive and significant relationship between financial technology and cybercrime occurrence in Nigeria. especially issued the following statement:

(i) ATM is positively and significantly related to incidence of cybercrimes in Nigeria.

(ii) Internet service has a positive and significant impact on incidence of cybercrimes in Nigeria.

(iii) Mobile banking is positively and significantly related to incidence of cybercrimes in Nigeria.

(iv) Institutions responsible for fighting cybercrimes, such as the EFCC is negatively related to cybercrimes in Nigeria, but the impact is weak due to the weak institutional structure and will-capacity prevalent in Nigeria

5.2. Conclusion

Undoubtedly, the technological revolution supporting financial technology has played a key role in the scale of cybercrime-related crimes in Nigeria. With the advent of the Internet and other information technologies, Internet fraud and crime have expanded on a massive scale. Financial technology has produced unimaginable consequences such as criminal activity, spam, credit card fraud, internet and he ATM fraud, phishing, identity theft and other related cybercrime. Huge economic losses hit countries around the world

(e.g. Hush Puppies saga. The emergence of financial technology has undoubtedly contributed to the Nigerian financial system in terms of increased effectiveness and efficiency in the rapid delivery of services by services such as online money transfers, payments and mobile banking. Thematic Data Warehousing, ATM, Electronic Money Transfer, POS, and Electronic. Most importantly, the same technology is facilitating cybercrime on a massive and frightening scale. As the speed of technological and innovative revolutions in the financial environment increases, so does the need to develop powerful anti-cybercrime software and other technological devices. This includes cyber experts to face critical cyber security challenges and build and implement strong firewalls. Authentication management, staff training on security measures, physical security enhancement.

5.3. Policy Recommendations

Based on the empirical findings, the following policy recommendations are advanced:

(i) Increased deployment of financial technological and innovation facilities that will help tame incidences of cybercrimes and other technologically-enabled frauds in Nigeria and the global scale.

(ii) Training and re-training of cyber surety experts to help manage tact financial security devices and information in financial institutions, particularly banks.

(iii) Building of strong and intensive firewalls and strong authentication control systems in financial institutions, to significantly combat incidence of cybercrimes in Nigeria.

(iv) Development of strong and sophisticated internet and ATMs monitored sotwares to track and trace cybercrimes at the speed of light.

(v) Creation of strong legal and institutional structures that can effectively tame cybercrimes in Nigeria. In particular, the strengthening of cybercrimes fighting institutions like the EFCC, ICPC and other sister agencies is important. This should be supported by a fearless and independent judiciary that is able to dispense justice speedily.

5.4. Further Research

Further studies in the subject matter should employ disaggregated approach based on a cross-section of banks in order to focused policy prescriptions.

Appendix 1: Empirical Results

Dependent Variable: INCYB

Method: Ordinary Least Squares

Date: 12/02/22 Time: 16:26

Sample: 2000 2021

Periods included: 22

Total observations: 22

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	0.031573	0.027842	1.134006	0.3022
ATM	0.073143	0.033416	2.188855	0.0406
INTER	1.162572	0.370012	3.131985	0.0026
MB	0.052173	0.024420	2.136486	0.0419
INST	-0.054315	-0.041680	-1.303143	0.1764

R-squared	0.767211	Mean dependent var	11.34689
Adjusted R-squared	0.735402	S.D. dependent var	9.278590
S.E. of regression	9.22267	Akaike info criterion	8.248974
Sum squared resid	10165.23	Schwarz criterion	8.302584
Log likelihood	-19.34689	Hannan-Quinn criter.	8.716940
F-statistic	22.71850	Durbin-Watson stat	1.827145
Prob(F-statistic)	0.000000		

Appendix 2: Data

YEAR	INCYB (N'M)	ATM (N'M)	INTERNET (N'M)	MB (N'M)	INST
2000	28111.0	15,210	19,200	5,780	1
2001	2963.1	16,210	12,640	6,809	1
2002	22,137.7	10,170	10,150	7,932	1
2003	28,128.9	12,300	12,,110	10,025	1
2004	23,844.5	13,190	11,060	11,870	1
2005	24,085.8	11,900	10,932	12,820	1
2006	33,189.3	12,666	13,160	12,1950	1
2007	57,990.2	13.050	14,175	11,910	1
2008	31,450.8	13,780	12,886	10,187	1
2009	27,827.2	14,620	15,270	14,536	1
2010	24,770.5	19,200	16,192	16,205	0
2011	20,730.6	12,640	17,,150	18,101	1

2012	31,652.42	10,150	15,3.40	9,890	1
2013	43,506.19	12,110	16,183	10,145	1
2014	32,705.20	16,270	14,230	12,430	1
2015	33,198.42	15,350	17,100	13,752	1
2016	44,230.65	13,060	16,500	15,180	1
2017	35,870.52	14,932	17,340	14,820	1
2018	45,231.30	15,160	18,420	12,,965	1
2019	38,985.22	16,175	17,100	12,160	1
2020	40,165.20	22,886	23,150	16,172	1
2021	43,168.52	37,270	19,650	24,250	1

REFERENCES

Adelmola, A. (2019). Cybercrime and Cybersecurity. FinTech's Greatest Challenges, *AELEX,*

Nigeria.

Adesina, O. (2017). Cybercrime and Poverty in Nigeria. *Canadian Social Science* 13 (4) Adomi, E., & Igun, S. (2008). Combating cybercrime in Nigeria. The Electronic Library 26 (5),

716-725

Ajers, R., Sellers, C. (2004). *Criminological theories: Introduction, evaluation and application*.

4th Ediction. Los Angeles: CA: Roxbury

Brenner, S. (2007). *Law in an Era of Smart Technology.* Oxford: Oxford University Press

Broadhurst, R. (2006): Developments in the global law enforcement of cyber-crime,

Policing:

An International Journal of Police Strategies & Management, 29 Issue: 3,408-433, Emerald Group Publishing Limited.

Clarke, R. & Felson, M. (1998). Opportunity makes the thief: Oractical theory for crime

prevention. *Policing and Reducing Crime Unit: Research, Development and Statistics Directorate, 98, 1-36*

Cohen, L., &Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity

Approach. *American Sociological Review, 44(4), 588-608.*

Council of Europe. (2017). *Nigeria: Cybercrime policies and strategies.*

Retrieved fromhttps://www.coe.int/en/web/octopus/country-wiki/

Clough, J. (2010). *Principles of cybercrime.* Cambridge: Cambridge University Press

Fadare, O. (2015). Impact of ICT tools for Combating Cyber Crime in Nigeria Online Banking: A conceptual Review

Gercke, M. (2006). The slow wake of a global approach against, *Computer Law Review International,* 2(2), 141, 2006.

Gottfredson, M., Hirschi, T. (1990). *A general theory of crime.* Stanford, CA: Stanford University Press

Halder, D. & Jaishankar, K. (2011). Cybercrime and the Victimization of Women: Laws, Rights, and Regulation. Hershey, PA, USA: IGI Global.

Hassan A. B., Lass F. D. & Makinde J. (2012): Cyber-crime in Nigeria: Causes, Effects and the Way Out, ARPN Journal of Science and Technology, vol. 2(7), 626 – 631.

Haru, A. (2021). Challenges of Cybercrime On Online Banking in Nigeria a Review, Idosr Journal of Banking, Economics and Social Sciences. 6(1), 17-23.

Ibrahim, U., (2020). The Impact of Cybercrime On the Nigerian Economy and Banking System. (15).

Internet Crime Complaint Center (2010). 2010 Internet Crime Report. Retrieved 23 July, 2016, from https://pdf.ic3.gov/2010_IC3Report.pdf

Internet Crime Complaint Center (2014). 2014 Internet Crime Report. Retrieved 23 July, 2016, from https://pdf.ic3.gov/2014_IC3Report.pdf

Internet World Stats (2016). Top 20 Countries with the Highest Number of Internet Users. Retrieved 23 July, 2016 from http://www.internetworldstats.com/top20.htm

Jolaosho A.O. (1996): Some Popular Perceptions of Poverty in Nigeria, quoted in UNDP

Human Development Report on Nigeria. Lagos: UNDP.

Kigerl, A. (2012). Routine Activity Theory and the Determinants of High Cybercrime Countries.

Social Science Computer Review, 30(4), 470-486.

Lakshm., I. (2015). *Cyber Crime: Prevention & Detection*," International Journal of Advanced Research in Computer and Communication Engineering, 4(3).

Laura A. (2011). Cyber Crime and National Security: The Role of the Penal and Procedural Law. Longe, O., Mbarika, V., Ngwa, O., Wada, F. (2009). Crimincal Uses of Information and

Communications Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives.

Journal of Information Technology Impact, Vol. 9 (3), 155-172

Marenin, O. & Reisig, M. (1995). "A General Theory of Crime" and Patterns of Crime in Nigeria: An Exploration of Methodological Assumptions. *Journal of Criminal Justice, 23(6), 201-518*

McQuade, S. (2006). *Understanding and Managing Cybercrime.* New York: Allyn and Bacon. Meke, E. (2012): Urbanization and Cyber Crime in Nigeria: Causes and consequences.

Odekunle, F. (1986). The legal order, crime and crime control in Nigeria: Demystification offlase appearances. Nigerian Journal of Policy and Strategy, 1, 78-100

Ogunlere, S. (2013). Impact of Cyber Crime on Nigeria Economy, ResearchGate, 2 (12) 2013. Ogbonnaya, M. (2020). Cybercrime in Nigeria demands public-private action, Senior Research Consultant, ISS Pretoria.

Okafor E.E. (2011): "Youth Unemployment and Implications for Stability of Democracy in Nigeria", Journal of Sustainable Development in Africa Vol.13, No. 1.

Okeshola, F. & Adete, A.K. (2013). The Nature, Causes and Consequences of Cyber Crime in Tertiary Institutions in Zaria-Kaduna State, Nigeria. American International Journal of Contemporary Research, 3(9), 98-114.

Olayemi, O. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. International Journal of Sociology and Anthropology, 6(3), 116-125.

Omodunbi, B., Odiase, P., Olaniyan, O., & Adebimpe, E. (2016). Cybercrimes in Nigeria: Analysis, Detection and Prevention

Saulawa, M., & Abubakar, M. (2014). Cybercrime in Nigeria: An Overview of Cybercrime Act 2013

Theohary, C. & Finklea, K (2015). Cybercrime: Conceptual Issues for Congress and U.S Law Enforcement. Congressional Research Service Report

United Nations Office on Drugs and Crime, (2004). West Africa takes lead in

fighting 419 scams: First regional even on combating cybercrime held in Nigeria. Retrieved from http://www.unodc.org/nigeria/en/1st-west-africa-cybercrime-summit.html.

Victoria, W. (2018). Internet Banking in Nigeria: Cyber Security Breaches, Practices and Capability

WDI (2016). World Development Indicator (WDI), International Bank for Reconstruction and Development/The World Bank; Washington D.C, US