Global Scientific JOURNALS

GSJ: Volume 11, Issue 4, April 2023, Online: ISSN 2320-9186
www.globalscientificjournal.com

AN EXAMINATION OF THE CAUSES OF FINANCIAL CYBER CRIMES AND ELECTRONIC FRAUDS - AS ADVANCED BY SOME YOUNGSTERS.
A JUXTAPOSITION ANALYSIS OF TWO COUNTRIES (NIGERIA AND INDIA)

BY

Omolokun Adetokunbo

Dissertation submitted to the Doctoral College, City University of Cambodia,
in
partial fulfillment of the requirements for the Degree of Doctor of Philosophy Award

Faculty of Information and Communication, Department of Information Technology and Innovation
January, 2023

ABSTRACT

India, is the largest democracy in the World with a GDP per capital of $7,200 as of 2017, while Nigeria - the Most Populous Black Nation in the World has a GDP per capital is $5,900 as of 2017. In 2018, Nigeria - a Country endowed with abundance of natural and human resources overtake India as the world's poverty capital, with around 88 million people living in extreme poverty, compared with India's 74 million, who are also blessed with greater advantage in skilled workforce in Information Technological Innovations, even a Nuclear Power Nation. However, according to the World Poverty Clock, the latest statistics of Nigerians living in extreme poverty was pegged at (70,677, 758) representing 33 per cent of the population. The above demographics coupled with financial strengths of these two nations could be seen as a dangerous signals arising from the wanton financial crimes, high level electronic frauds and economic recklessness that have dominated their respective National Livelihood in the last three decades or more! The growth of cyber-crime – particularly in these two countries ranges from Hacking, Distributed Denial of Service Attacks, Phishing, Spamming, Trojans, Service Denial Attacks, Identity theft, Premium Online Dating Scams and Account Takeover– and these incidents and several other challenges (like poor awareness campaign, unskilled personnel, poor infrastructure etc) have threatened the existential relevance of financial institutions, especially regarding how they protect their assets and prevent their customers from becoming victims of cyber frauds. These criminal activities have remained pervasive due to the borderless nature of the internet banking transaction and the continuous growth of the information super highway with different innovative service offerings by banks and other financial institutions. This study will adopts mixed research methods with the aid of descriptive and inferential analysis because human nature is heavily involved, which comprised exploratory factor analysis (EFA) and confirmatory factor analysis (CFA) for the

quantitative data analysis, whilst thematic analysis was used for the qualitative data analysis. The theoretical framework was informed by Routine Activity Theory (RAT) and Fraud Management Lifecycle Theory (FMLT) which will assist the study in maintaining the balance required in the competing and complementary actions within the Fraud Management Lifecycle.

TABLE OF CONTENTS

CHAPTER ONE

1.0 Introduction

The term Electronic Payments has evolved from the days of European Union Transfer of 18th Century using the Telegraph, through the birth of TCP/IP Protocols in the early 1980s and the Ultimate turning point of some years later - 1989 precisely, when Sir Tim Berners-Lee invented the World Wide Web Protocol for the Internet - an hypermedia initiative for global information sharing! This developments have led to the rapid and innovative myriads of services that banks have to offer their numerous customers over the course of time. Recently, the advancement in Internet Security and Speed has also enable Financial Institutions to emerge as a Start-Up Companies, Offering traditional banking services that are hither to the exclusive rights of orthodox banks and other novelty value add services electronically using the information super highway platform. These common e-payment channels from both Banks and Financial Institutions now include Payment Cards (Debit or Credit with different levels of capabilities and premium services), Online Web Portals, Point of Sales (POS) Terminals, Automated Teller Machines (ATM), Mobile Phones Apps (electronic wallets), Tokenized Digital Transactions, Unstructured Supplementary Service Data (USSD),

Automated Clearing House (ACH), Direct Debit/Deposit, Digital Ledgers and Real Time Gross Settlement (RTGS) System.

Interestingly, as these service offerings are are cropping up, so are the challenges of keeping them secured from potential risks posed by criminal elements in our society - who often used the loopholes in the systems and human vulnerabilities (like Identity Theft, Social Engineering, Password Compromise, Spamming, Trojans, Malware Attacks, Ransom-ware Attacks, Worms Attacks, IP and MAC Address Spoofing, Card Trapping, Pharming, Cloning, BIN Attack, Skimming, Phishing, Carding and Counterfeiting) to defraud and steal from users of these platforms their hard-earned money. According to Olaleye et. Al., 2019, asserted that simple consumers are not the only targets of electronic payment crimes, other targets include the merchants, retailers, banking institutions, organizations that use individuals' data to transact businesses and even the government. No possible target is spared by these criminals.

Nigeria and India ranked First and Second respectively on the global index of Countries that people got swindle or ripped-off of their money without you being aware that you are been scammed! The digital financial systems of Nigeria and India are bedeviled with the myriads activities of unscrupulous elements, especially from the teeming youth population of these two countries, to insider dealings of officials of banking and financial institutions, corrupt government officials and bad governance and irresponsible political leadership, the list of these criminal and corrupt elements goes on and so is the methods of perpetrating and internalizing these nefarious crimes are novelty day in, day out.

Crimes as rightly asserted in humanistic social sciences are deviations from the general norms, sociocultural or religious standards that are prevailing in the Society or the world as a global village and as necessitated by the incidence of Internet and pervasiveness of technological innovations and the new normal ways of conducting business engagements of all kinds. According to an online survey conducted by Numbeo.com, 2021, Nigeria's crime index was pegged at 63.89&, while that of India was at 44.59%. Both Countries reports from Numbeo.com also showed that Nigeria was at 84.89% in her Corruption and Bribery Index, while India is following at 70.49% respectively.

The upsurge in fraudulent practices in all aspect of national life all over the world has become a source of concern and that of Nigerian banking sector has been embarrassing in recent times (Okpala & Enwefa, 2017). The major factors responsible for the high rate of fraud include the advent and extensive growth in computer technology and globalized economies supporting e-fraud, poor financial and regulatory framework, week internal control system and societal attitude to achievement at all cost.

With the emergence of information super highway, it is common knowledge that the worldwide adoption of Information and Communication Technological Innovations has immensely altered and enhanced human interaction and our way of life in the past three decades or more. Thus, with this paradigm shift the world is now a global marketplace as a result of the application of Information and Communication Technology (ICT) in business and cross-border trade activities with decentralized ledger on SWIFT Networks as an enabling infrastructure and distributed ledger in more recent times as an enabler

for smart contracts and block chains transaction. However, the advent of Electronic Commerce (e-Commerce) as a result of the rapid and pervasive development of the internet and its antecedence in robust service offerings has brought with it, a number of legal and compliance issues, cultural and socioeconomic issues, privacy inversion and insecurity concerns of varying degrees. Information and Communication Technology (ICT) is the use of scientific tools and techniques for developing, documenting and communicating information when needed especially as it concerns solving problems and providing needed services in the various areas of human endeavors. It is a term that generally covers the harnessing of electronic technology for the information needs of a business at all levels.

India, is the largest democracy in the World with a GDP per capital of $7,200 as of 2017, while Nigeria - the Most Populous Black Nation in the World has a GDP per capital is $5,900 as of 2017. In 2018, Nigeria - a Country endowed with abundance of natural and human resources overtake India as the world's poverty capital, with around 88 million people living in extreme poverty, compared with India's 74 million, who are also blessed with greater advantage in skilled workforce in Information Technological Innovations, even a Nuclear Power Nation. However, according to the World Poverty Clock, the latest statistics of Nigerians living in extreme poverty was pegged at (70,677, 758) representing 33 per cent of the population. The above demographics coupled with financial strengths of these two nations could be seen as a dangerous signals arising from the wanton financial crimes, high level electronic frauds and economic recklessness that have dominated their respective National Livelihood in the last three decades or more!

The growth of cyber-crime – particularly in these two countries ranges from Hacking, Distributed Denial of Service Attacks, Phishing, Spamming, Trojans, Service Denial Attacks, Identity theft, Premium Online Dating Scams and Account Takeover– and these incidents and several other challenges(like poor awareness campaign, unskilled personnel, poor infrastructure etc) have threatened the existential relevance of financial institutions, especially regarding how they protect their assets and prevent their customers from becoming victims of cyber frauds. These criminal activities have remained pervasive due to the borderless nature of the internet banking transaction and the continuous growth of the information super highway with different innovative service offerings by banks and other financial institutions.

With the global use of progressively more sophisticated internet and information technology (Papazoglou, 2003), electronic banking is developing as a key channel for banking businesses (Wei et al., 2012). Globally, remote banking is regarded as a characteristic of the new economy, which involves electronic transactions between banks and their customers (Banstola, 2007). Electronic banking, generally referred to as ebanking, is the latest delivery channel for the banking system (Keivani et al., 2012). The term “e-banking” has been discussed in several ways by many researchers from diverse backgrounds, mostly because electronic banking involves quite a lot of banking activities through which customers can inquire for financial information and implement transactions by means of a digital television, telephone, mobile phone or computer (Hoehle, Scornavacca & Huff, 2012). Perkins and Annan (2013) describe electronic banking as the rendering of

services and dissemination of information by banks to customers through various delivery channels that can be accessed with a personal computer or other electronic devices.

The causative factors leading to high rates of electronic and cyber financial crimes in these two countries, especially amongst the teeming youthful population could be as results of various abnormalities prevalent in our society - which may not be limited to political instability, bad governance, broken homes, peer pressure, wrong perceptions on moral virtues, unemployment and poverty to mention a few. However, this research work will be dedicated to explore emerging perceptions from the youth of these two naturally endowed Countries - Nigeria being the Most Populous Black Nation in the World and India, the largest democracy in the World.

According to the Wisdom (2012), Information and Communication Technology, the most significant factor in the forthcoming development of the banking industry, enhances banks' ability to produce sophisticated products, to have superior market structures, to diversify their markets and to expand globally. Furthermore, Darlington (1999) states that over the past three decades, customers' needs have changed significantly: customers are demanding simplicity in their daily banking services together with maximum security and safety.

Thus, the traditional banking system, which consists of physical branches, is now being threatened by information and communication technologies characterized by automated systems of interaction with

customers (mobile banking, call centers, automated teller machines (ATMs), online banking), that include relatively minimal costs and permit customers to select from the alternative delivery channels (Keivani et al., 2012). Therefore, electronic banking has become a great business; the transformation from traditional banking to electronic banking has been a "Leap" change (Yazdanifard, WanYusoff, Behora, & Abu, 2011; Wang & Huang, 2011).

Globally, the electronic banking system addresses several emerging trends and so are the challenges with these emerging markets are also enormous: it is very convenient and easy for electronic banking users to manage and access their bank accounts at any time and from anywhere in the world (Brar, Sharma & Khurmi, 2012). The banking sector has been strengthened by this development in recent years, since electronic banking saves vast amounts of resources in areas such as investments into ATMs, staff training, opening of branches and other operational costs (Chaturvedi & Meena, 2016), which are the positive impacts for investors' funds, however the possibility that a threat exit or a risk might occurred has not been totally addressed. The internet has improved users' experience of electronic banking operations dramatically (Abu-Shanab & Matalqa, 2015). Banking transactions can now be performed any place, anytime in the world through any bank delivery channel: ATMs, POS, Smart TV, personal computers, telephones are among the channels a customer might consider (Hoehle, Scornavacca & Huff, 2012). These diverse channels for mobile banking operations and transactional activities are what make the occurrence of cyber crime and electronic frauds a possibility today. And Nigeria and India are the most corrupt

countries in the world crime index, especially in the areas of cyber crime and electronic fraud.

1.1 Background of the Research Problem

According to Rajdeepa & Nandhitha, (2015), fraudulent electronic activities are increasing and becoming sophisticated, severely threatening and menacing the trust and security of electronic banking services; Mahdi, Rezaul & Rahman, (2010). E-banking fraud has turned into a thoughtful and serious phenomenon to the financial fraud and crime management in the banking industry across the entire globe.

These current electronic fraud opportunities are often tremendously difficult to mitigate due to their technological complexity; hence, banks may devote substantial resources endeavoring to prevent and detect them Kranacher, Riley & Wells, (2011). Banks encounter challenges in preventing and detecting fraud, and these challenges can often be aggravated by the organizational frameworks, political frameworks, regulatory frameworks and newly invented technology approaches that are in place. Nevertheless, even the issuing of momentous regulatory frameworks and the regulatory supports of a given economy or nation cannot be predicted to eliminate or minimize the occurrence of fraud in the banking sector Hoffman, (2002). However, in the very beginning of electronic banking systems, the scale of fraud was very insignificant because the banking industry was one of the most strictly regulated sectors, which treats prevention of fraud as a duty Mahdi, Rezaul & Rahman, (2010); Shannak, (2013) all asserted.

On the contrary, banking represents the mediator of the economy; fraudulent acts have brought enormous losses that are affecting all the performing activities Sahin &Duman, (2010). Equally, banking development, from traditional banking to electronic banking, is not only challenging in terms of managing bank risk, but also with international and national irregularities Saranya & Gunasri, (2013); Chaturvedi & Meena, (2016); AbuShanab & Matalqa, (2015) all concluded.

For the purpose of this dissertation, the causative factors or the reasons perpetrators of these heinous crimes advanced for engaging in these criminal activities are based on the following premise; firstly, that the Developed and Advanced Countries 'plundered' the Developing Nations and also termed these Countries as such, even a more derogatory term 'Third World' Countries during the Colonial Era as a result of their scramble for foreign lands occupation and expansion of their imperialist rules, the resources of these plundered Countries were used to develop the European nations and the Americas. Consequentially, the youth of these 'poor' nations are now fighting back by taking what was stolen from them! This is the narratives from Nigeria Apprehended Perpetrators mostly!

Secondly, that the Advanced Economies of the World has refused to provide social-security for the poor masses of the developing and poor nations, by allowing wanton treasury loots and providing safe havens for their Corrupt Political Leaders to stashed these loots in their banks and financial institutions abroad. The proceeds of these loots are used to developed the foreign nations economies, education, research and development leading to cutting-edge innovations and inventions, all to

the detriments of the poor masses of these developing nations' quality of life and degradation characterized by abject poverty! This position was shared by both the youth of Nigeria and India respectively.

Thirdly, this is very peculiar to India, the over-population of India as a Nation - which has earned her the largest democracy in the world is now to be seen as a curse per se! Skillful Workforce, especially in ICT was supposed to be the greatest advantage India should over any countries. However, the underemployment rates is always on the negative side, as worker and employees don't get remunerations that could encourage quality of life and standard of living! Most Companies in the world have their major design and manufacturing plants, sales and customer service support infrastructures and offices in India. The Employers of labor taking the undue advantages of the 'cheap' and readily available workforce, always engaged in sharp practices that engendered underemployment and impoverished conditions. The resultant response is that, cyber crimes and electronic frauds are order of the day - as a precarious means to survival.

From the three above claims that spurred the perpetrators of cyber crimes to actions are many other factors which are enabling conditions for such dastardly heinous to be committed, these include: Poor Infrastructural Systems and the Right Personnel to Manned such Systems; Unhappy Employee who may leaked the security details to hackers for financial gains or vengeful purposes; Carelessness on the part of staff - fallen to social engineering schemes and the facts that Cyber Crimes Legal Frameworks are still in it's nascent stage. It should also be noted that 99% of Cyber Crimes and Electronic Frauds are Caused by human error, while 1% are as a result of System Failures!

1.2 Aim of the Study

The research of Nwankwo (2013), a study of internet banking fraud in Nigerian banking sector, indicates that fraud in the Nigerian banking sector negatively affects bank performance, profitability, operational efficiency, foreign direct investments, credibility and reputation. It also causes a psychological and emotional burden on the victims of fraud, criticisms in the public arena and a bad national image. However, it is obvious that, today, no nation in the global economy can sustain business transactions without e--banking. Neha Sindhu, 2021, asserted that to commit a cybercrime a person needs to be having a good knowledge about the computers and internet. Many a times, cybercrime is committed by the very educated people as they have the accurate knowledge about the same. And at times it becomes very hard to trace them. Collecting evidence in a cybercrime is very difficult as the crime committed is in the virtual world this is coupled with Geographical Challenges - Since the crime can be done globally without being physically present at the place. The distance does not matter in cybercrimes. A person sitting in Indian can target a person sitting in Australia.

Therefore, the aims of this research work is to study the emerging causative factors of cyber-crimes and electronic frauds as advanced in recent times by the teeming youthful populations of these two countries and ultimately proffer solutions on how to minimize the instances of cybercrimes, through recommendations inferred from the findings of this research work.

In between the special relationship with borrowers and depositors; banks need to protect the confidence and trust of their various clients (Wei et al., 2012). The failure of banks to satisfactorily perform their role resulted from the numerous risks they are exposed to which are not appropriately controlled (Papazoglou, 2003). One of these risks which are progressively becoming a cause of burden is the banking risk related to electronic fraud (Sruthi & Prasanna, 2016). Furthermore, fraud, which literally means an intentional act of deception that makes society suffer damage, either by monetary or physical asset losses, is now a global menace to the entire banking industry (Ramamoorti, Morrison & Koletar 2013).

However, e-banking fraud has created an aggressive presence in the banking sector and therefore, security cognizance is required in order to bring behavioral transformation, minimize employees' vulnerability and guard against the prospective risk of fraud; and to create strong detection and prevention of fraud using electronic technology, adoption of fraud awareness and other new sophisticated anti-fraud approaches. Hence, to cover these gaps there is a need to examine the natures, contributing factors, preventive and detective mechanisms of e-banking fraud.

1.3 Research Questions

For the purpose of this research work, the following research questions have been designed to further address the research aims:

1. What are the perceived factors that have considerable influence on the increase in e-banking fraud in Nigeria and India in recent times?
2. What are the e-banking fraud risks that are of high concern in the Strategic and Survival Model of Nigerian and Indian banking sector?
3. What are the current significant mechanisms for e-banking fraud detection in the Nigerian banking industry?
4. What are the current significant mechanisms for e-banking fraud prevention in the Nigerian banking industry?
5. What are the mechanisms for control of the liberalized market diversity as occasion by Internet of Things Channels in the Banking Activities and Operations?

1.4 Scope of the Research

This research work's scope will be built around the postulations made by scores of Nigerian and Indian Youth that are engaged in the heinous activities of varying degrees that culminates into Cybercrimes and e-frauds. Attempts will be made to verify these claims, whether is it a noble course, a self-serving vigilante position or criminals are only to justify their acts by lacing it with economic and political errors of the past. Therefore, the scope of this research work will be constrained to the problem statements stated above as the causative factors leading to increase rates in the incidence of cybercrime and electronic frauds as related to Nigeria and India respectively.

1.5 Rationale for the Research

Bamidele (2019), reported that the Nigerian Banking Industry lost N15.15Billion to cyber-crime and forgeries in 2018 alone! This amount

was astronomically higher than the N2.37Billion recorded in the year 2017 with 539%. According to Nigeria Deposit Insurance Commission (NDIC), the rising cases of fraud in the Banking System are attributable to the surge in Internet and Technological Innovation based channels and other smart instruments that are available to bankers and customer base at large. These increase in financial crimes are becoming more sophisticated day in – day out, as advanced computing techniques such as hacking, cyber tools availability in the black markets and other I.T related products and usages are now a common thing, which warranted fraudulent transfers and withdrawals, unauthorized credits accessibilities, money laundering and obtaining money by tricks (scamming) and lots more.

Therefore, the current research aim is to examine e-banking fraud detection and prevention mechanisms in Nigerian banking industry in order to provide information on the challenges of e-banking fraud incidences in the Nigerian banking industry, as well as dialogue on what the banks are doing to prevent and detect e-banking frauds. It provides useful information for foreign organizations considering participation in the Nigerian economy. This study also gives insights on how to advance Nigerians' access to global investment funds.

1.6 Significance of the Research

Since the campaign and fight against Cybercrimes of any sort is a global collective efforts and the need to assist policy makers and aid robust and hassle-free international trades, as occasioned by the advancement of internet technological innovations by the emergence of multiple payments channels, therefore this research has significance for theories and empirical applications in the areas of policy making and financial

institutions new normal ways of protecting investors' funds and deposits of the savers which in this case are their numerous customers.

Theoretically, the submission of prevailing theories of frauds, such as routine activity theory (RAT) (Cohen & Felson 1979; Williams, 2016) and fraud management lifecycle theory (FMLT) to the Nigerian and Indian e-banking fraud prevention and detection context will generate more information about whether these theories can be applied worldwide or whether they depend on cultural or local structures or nullified these claims as advanced by these miscreants in our society.

The research can likewise be projected to expose some of the prerogatives that are claimed in the academic and theoretical literature regarding the understanding of electronic frauds in the financial context and its connotations. Given the application of present theories along with other information from the research concerning the Nigerian and Indian banking sector, this can be regarded as significant research from this viewpoint.

Moreover, the findings of the current study will be of interest for legal, regulatory and law enforcement institutions and policymakers within the executive and legislative arms of the Nigerian government; executive directors of Nigerian financial institutions; and all professional accounting and banking bodies. Also, corporate financial institutions will be able to design better control systems to curb fraudulent practices within their operations.

The study will identify exposure to e-banking fraud and appropriate prevention, detection and investigation approaches which will enhance national economic development of Nigeria and India, as the banking sector constitutes the backbone of these countries economic activities.

Finally, even though several studies have been conducted on e-banking fraud in various parts of the world, particularly in the Europe, United States of America and else where, no broad study has been done to juxtaposed two leading Countries in the World that are regarded as the 'corruption capitals of the world'; and where there are existence of information, they are usually narrowed down to a geographical region. It is therefore expected that this study will contribute significantly to the literature of the existing body of knowledge on e-banking fraud, national rebirth through awareness and campaign against cybercrimes and on the developing economy with a national focus and direction.

CHAPTER TWO: LITERATURE REVIEW

2.0 Introduction

The purpose and focus of this chapter is to present the several literature and carried out a review on some of these literature as it affect this dissertation. The thesis focuses mainly on an examination of the causes of e-banking frauds in Nigerian and Indian Financial Institutions and the Banks in the emerging criminal trends. The chapter discusses the contextualization of the Nigerian and Indian banking system, history of Nigeria and India banking systems and constructs of electronic banking, it also elucidates the impact of e-banking fraud, e-banking attacks and techniques and the contributing factors to increase of these frauds as a results of multi-channel source of financial operations. The discussion also included ebanking fraud detection and prevention mechanisms while ending with a summary.

2.1 Contextualization of The Nigerian and Indian Banking Systems

The Nigerian banking sector is one of the momentous sectors that are contributing to the development of the economy in Nigerian. Over the decades, banking system in Nigeria has achieved incredible growth and development in activities and structures. This section focuses on

contextualizing of the Nigerian banking sector, which comprises its history, evolution and structure of the Nigerian banking system.

While in India, the context in which banks and financial institutions operates are pinned on the notion that it should enhance economic growth and Indian Mixed-Market Economy, although it's apparent that the capitalists reign supreme! The masses are bound to suffer untold hardship if they are not well protected and included into to the borrowing circles and how to use the money.

2.1.1 The History of Nigeria Banking System

The history of the Nigerian banking industry dated back to the colonialism epoch. The colonial banks were established by the colonial government to accomplish its commercial purpose. African Banking Corporation and British West Africa bank were established in 1892 as the leading banking industries in Nigerian. Thereafter, they were amalgamated and formed present First Bank of Nigeria (Ezeoha, 2007).

In 1925, the Barclays Bank was established through the merger of Anglo-Egyptian Bank and National Bank of South Africa, CBN, (2014). The British and French Bank for Commerce and Industry started business operation in 1948 which later morphed into the existing United Bank for Africa after reform. The first local bank was established in 1929 which called Industrial and commercial bank but collapsed in 1930. However, after the collapse of the first indigenous bank, the Nigeria Farmers and Commercial bank were established in 1947 for agricultural growth and development. Followed by the Continental Bank, which came into inception in 1949. Okoh & Okoh, (2014). The Central Bank of Nigeria (CBN) is an autonomous bank that controls and supervises the monetary

and fiscal policies for the Nigerian government as well as oversees the Nigerian banking system, Central Bank of Nigeria, (2009).

The Central Bank of Nigeria is the central bank and apex monetary authority of Nigeria established by the CBN Act of 1958 and commenced operations on July 1, 1959 (CBN, 2021). The central bank of Nigeria is the regulatory authority of the banking sector in Nigeria. It is generally known as the leading monetary authority and the central issue of legal tender in Nigeria (CBN, 2014).

Amongst its core functions, the central bank of Nigeria encourages monetary constancy, price stability, banking industry, dependability and of course, financial and banking adviser to the Government. Besides this, the Bank also enhances the development and advancement of banking institutions. Enabling laws enacted in 1991 offered the Bank more pliancy in licensing, overseeing and regulating the banking industry and other finance systems, and in a recent time, e-naira was introduced to the economy with an App and powered by an etherum network of a decentralized block chain systems, Central Bank of Nigeria, (2021).

However, since 1959 when the Central Bank of Nigeria (CBN) established has been playing its role as the apex of Nigerian banking authority. Despite the issuance of legal tender, Central Bank of Nigeria performs significant impacts in regulating the economy in Nigeria and modifying the structure of the Nigerian banking system, which include disciplinary actions against erring banks executives that are found wanting in the management of their depositors' and investors' funds.

2.17.1b The History of India Banking System

The first that was established in India was the "Bank of Hindustan", established in 1770 and located in the then Indian capital, Calcutta.

However, this bank was able to work and ceased operations in 1832. During the Pre-Independence period over 600 banks had been registered in the country, but only a few managed to survive, Byjus, (2021)

Following the path of Bank of Hindustan, various other banks were established in India. They were: The General Bank of India (1786-1791); Oudh Commercial Bank (1881-1958); Bank of Bengal (1809); Bank of Bombay (1840); Bank of Madras (1843), During the British rule in India, The East India Company had established three banks: Bank of Bengal, Bank of Bombay and Bank of Madras and called them the Presidential Banks. These three banks were later merged into one single bank in 1921, which was called the “Imperial Bank of India.” The Imperial Bank of India was later nationalized in 1955 and was named The State Bank of India, which is currently the largest Public sector Bank.

Following the Pre-Independence period was the Post-Independence period, which observed some significant changes in the banking industry scenario and has till date developed a lot. At the time when India got independence, all the major banks of the country were led privately which was a cause of concern as the people belonging to rural areas were still dependent on money lenders for financial assistance, largely to their unbanked status and absence of facilities, not as a result of illiteracy.

As part of Indian Government’s efforts to solve this problem, the Government of those periods decided to nationalize the Banks. These existing banks after so many debates and compromise were nationalized under the Banking Regulation Act, 1949. Whereas, the Reserve Bank of

India was nationalized in 1949 as the Regulatory and Apex Bank. Following it, was the formation of State Bank of India in 1955 and the other 14 banks were nationalized between the time duration of 1969 to 1991. These were the banks whose national deposits were more than 50 crores.

There were various reasons why the Government chose to nationalize the banks. Given below is the impact of Nationalizing Banks in India:

This lead to an increase in funds and thereby increasing the economic condition of the country; Increased efficiency helped in boosting the rural and agricultural sector of the country as it opened up a major employment opportunity for the people. The Government used the profits gained by the Banks for the betterment of the people. Of course the competition and sharp practices decreased to barest minimum, which resulted in increased work efficiency.

This post Independence phase was the one that led to major developments in the banking sector of India and also in the evolution of the banking sector till this present time and Indian Banking Sector has gone through evolutionary phases and the environment is ever dynamic.

Similarities between Nigeria and India Bank History and Development

From the foregoing, it is obvious that both Nigeria and India have almost identical historical charts viz-a-viz:

1) Historical Period: Pre and Post Independence Era
2) Modern Times Major Reforms that lead to Security on Deposits
3) Management and Board Restructuring that enhances Transparency and Effective Utilization of both Investors and Depositors Funds which leads to efficient service delivery

4) The Evolution of Modern Banking Operational Activities
5) And of course, the challenges of insecurity is ever-present in both Countries.

2.1.2 The Structural Reform of Nigeria Banking System

The Nigerian banking system has experienced main current banking reforms that have had a substantial impact on the Nigerian economy. The first Nigerian banking system reform took place in 2004 while the subsequent banking system reform was performed in 2010 (Sanusi, 2011).

The 2004 banking system reform focused on the combination of banks by means of merger and acquisition, which replaced deposit money banks to N25 billion minimum capital base from N2 billion and minimized the number of banks to 25 from 89 in 2005 and further to 24 Sanusi, (2011). The aim of this reform was to strength and position the banks play crucial roles in bringing advancement and expansion across the segments of the national economy. While, the Asset Management Corporation of Nigeria (AMCON) was introduced in 2010, subsequent by the announcement of its empowering Act through the National Assembly. It is significant purpose was to address the challenges of nonperforming loans in the Nigeria banking sector Kolapo, Ayeni, & Oke, 2012; Sanusi, (2011).

Corresponding to the AMCON mandate, AMCON currently takeover of the nonperforming loan of certain banks valued over N1.7 trillion, which supposed to boost their soundness and safety as well as increase their liquidity. With the involvement of the AMCON, the ratio of non-performing loan in the Nigerian banking industry to gross credit has

significantly low from 34.4% to 4.95% as at December 2011, Agbada, & Osuji, (2013).

Furthermore, the central bank of Nigeria and all the commercial banks or deposit money banks in Nigeria signed an MOU to finance the AMCON in order to accomplish its mandate. The central bank of Nigeria contributes N50 billion every twelve months to AMCON while, each of the participated deposit money banks pays 0.3 percent of their total assets per annum to the sinking fund. Therefore, the resolution cost to the taxpayers in Nigeria is significantly diminished, Kolapo, Ayeni & Oke, (2012).

Moreover, in 2011, the Nigeria Incentive Risk Sharing System for Agricultural Lending (NIRSAL) was introduced and incorporated in 2013 by the central bank of Nigeria (CBN). The NIRSAL was incorporated to build credit facility and capacity of the banking industry to engage and provide loans for agriculture by producing technical support and minimizing counterpart threats facing banking institutions, Anyanwu, (2010). In 2008, due to the challenges caused by fragmentation and weaknesses of the financial sector, the central bank of Nigeria introduced a guideline named “The Project Alpha Initiative” to reform banking sector and other financial system in general. The reforms designed to stop the inherent fragmentation and weaknesses of the financial system, banking system, integrating the different, piecemeal and ad-hoc reforms and releasing of the huge strength of the economy, Sanusi, (2011).

To address the identified crises, the central bank in 2010 revisited the Universal Banking Model by guiding banking industries to concentrate on their fundamental banking activities which they licensed for under

the current guideline, licensed banks were approved to perform banking activities of their license category AJAYI, et al. (2018).

However, the licenses of the Nigerian banking system have been grouped into three categories in relation to their activities, namely:

1. Commercial Banking (Deposit Money Banks) License
2. Merchant Banking License
3. Specialized/Development Banking License

As at 31st December 2016, the Nigerian banking industry made-up of 28 banks, which comprised of 22 deposit money banks (DMBs) that was previously known as commercial banks, 5 merchant banks and 1 non-interest-bearing bank, CBN, (2017).

However, the Nigerian deposit money banks, which comprise of 22 banks of 3978 branches all over Nigeria hold 78% of the capital reserves, total net assets and also, share over 83% of total profitability in the banking sector, while the remaining 22% of the capital reserve and total net asset, including 17% of the total profitability in the banking sector are shared by the other 6 banks (5 merchant banks and 1 non-interest-bearing bank; CBN, (2017). In addition, there are other institutions in the Nigerian financial system that will not be investigated in this study include Bureaux-De-Change, Development, Financial Institution, Discount House, Finance Company and Primary Mortgage Banks Sanusi, (2011).

Furthermore, in 2014 introduction of Bank Verification Number (BVN), globally, biometric technology has been adopted to analyse human characteristics as an improved form of verification, authentication and certification for real-time security methods; Blass & Oved, (2003). In the face of cumulative occurrences of compromise orthodox security

systems (PIN and password), the need for sophisticated security on access to personal and sensitive information in the Banking industry becomes inevitable. Therefore, the Central Bank of Nigeria through the Banker' Committee and in cooperation with all banks (Deposit Money Banks (DMB) and Nigeria Interbank-Settlement System (NIBSS)) in Nigeria on February 14, 2014 introduced a Centralized Biometric Identification System for the banking sector marked Bank Verification Number (BVN); CBN, (2014).

The BVN project was introduced due to growing incidents of compromise on conservative security systems (PIN and password) and an increase demand for sophisticated security for sensitive information in the Nigerian Banking System.

However, the aim of this project (BVN) is to prevent bank customers from identity theft and other financial frauds emanating in the Nigerian banking industry; Orji, (2015). This research study will endeavor to analyse the present mode of operation in the Nigerian banking industry evaluating its impacts since the date of introduction in the Nigerian Electronic Banking System.

2.1.2b The Structural Reform of India Banking System

India has a long history of both public and private banking. Modern banking in India began in the 18th century, with the founding of the English Agency House in Calcutta and Bombay. In the first half of the 19th century, three Presidency banks were founded. After the 1860 introduction of limited liability, private banks began to appear, and foreign banks entered the market. The beginning of the 20th century saw the introduction of joint stock banks. In 1935, the presidency banks

were merged together to form the Imperial Bank of India, which was subsequently renamed the State Bank of India. Also that year, India's central bank, the Reserve Bank of India (RBI), began operation. Following independence, the RBI was given broad regulatory authority over commercial banks in India. In 1959, the State Bank of India acquired the state-owned banks of eight former princely states. Thus, by July 1969, approximately 31 percent of scheduled bank branches throughout India were government controlled, as part of the State Bank of India.

The post-war development strategy was in many ways a socialist one, and the Indian government felt that banks in private hands did not lend enough to those who needed it most. In July 1969, the government nationalized all banks whose nationwide deposits were greater than Rs. 500 million, resulting in the nationalization of 54 percent more of the branches in India, and bringing the total number of branches under government control to 84 percent.

Prakesh Tandon, a former chairman of the Punjab National Bank (nationalized in 1969) describes the rationale for nationalization as follows: 'Many bank failures and crises over two centuries, and the damage they did under 'laissez faire' conditions; the needs of planned growth and equitable distribution of credit, which in privately owned banks was concentrated mainly on the controlling industrial houses and influential borrowers; the needs of growing small scale industry and farming regarding finance, equipment and inputs; from all these there emerged an inexorable demand for banking legislation, some government control and a central banking authority, adding up, in the final analysis, to social control and nationalization.

After nationalization, the breadth and scope of the Indian banking sector expanded at a rate perhaps unmatched by any other country. Indian banking has been remarkably successful at achieving mass participation. Between the time of the 1969 nationalizations and the present, over 58,000 bank branches were opened in India; these new branches, as of March 2003, had mobilized over 9 trillion Rupees in deposits, which represent the overwhelming majority of deposits in Indian banks. This rapid expansion is attributable to a policy which required banks to open four branches in unbanked locations for every branch opened in banked locations.

Between 1969 and 1980, the number of private branches grew more quickly than public banks, and on April 1, 1980, they accounted for approximately 17.5 percent of bank branches in India.

In April of 1980, the government undertook a second round of nationalization, placing under government control the six private banks whose nationwide deposits were above Rs. 2 billion, or a further 8 percent of bank branches, leaving approximately 10 percent of bank branches in private hands. The share of private bank branches stayed fairly constant between 1980 to 2000.

Nationalized banks remained corporate entities, retaining most of their staff, with the exception of the board of directors, who were replaced by appointees of the central government. The political appointments included representatives from the government, industry, agriculture, as well as the public. (Equity holders in the national bank were reimbursed at approximately par).

Since 1980, there has been no further nationalization, and indeed the trend appears to be reversing itself, as nationalized banks are issuing

shares to the public, in what amounts to a step towards privatization. The considerable accomplishments of the Indian banking sector notwithstanding, advocates for privatization argue that privatization will lead to several substantial improvements. Recently, the Indian banking sector has witnessed the introduction of several “new private banks,” either newly founded, or created by previously extant financial institutions. The new private banks have grown quickly in the past few years, and one has grown to be the second largest bank in India. India has also seen the entry of over two dozen foreign banks since the commencement of financial reforms. While we believe both of these types of banks deserve study, our focus here is on the older private sector, and nationalized banks, since they represent the overwhelming majority of banking activity in India.

The Indian banking sector has historically suffered from high inter mediation costs, due in no small part to the staffing at public sector banks: as of March 2002, there were 1.17 crores of deposits per employee in nationalized banks, compared to 2.05 crores per employee in private sector banks. As with other government-run enterprises, corruption is a problem for public sector banks: in 1999, there were 1,916 cases which attracted attention from the Central Vigilance Commission. While not all of these represent crimes, the investigations themselves may have a harmful effect, if bank officers fear that approving any risky loan will inevitably lead to scrutiny. Advocates for privatization also criticize public sector banking as unresponsive to credit needs.

In the rest of this research work, recent evidence on banking in India will be used to shed light on the relative costs and benefits of nationalized

banks. Throughout this exercise, it is important to bear in mind that the Indian banking sector is going through something like a transformation. Thus, it is potentially a dangerous time to evaluate its performance using historical data. Nevertheless, data from the past is all we have, and we believe things are not changing so quickly that the lessons learned are not useful for both countries under study in this research.

2.1.3 Evolution of Electronic Banking in India

In traditional banking customers has to visit bank branches to avail banking services. Now with the ATMs, Internet banking, Mobile banking and Information Technology-enabled services are replacing the traditional method of service. In the recent days banks are concentrating on value-based service through E-banking.

Electronic banking (e-banking) is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels (Daniel, 1999; Sathye, 1999).

Kamakodi et al. (2008) expressed that an extensive gap exists in human service in Indian banking while IT-based facilities are beyond the expectations. Qureshi T M, Zafar M K and Khan M B (2008) evaluated the customer acceptance of online banking study concludes that majority of customers are accepting online banking culture because of favourable factors and usefulness, security and privacy. Uppal R K (2010) expressed in his research, ATMs is the most effective while mobile banking does not hold a strong position in public sector banks, Mobile banking customers are also the highest in E-Banks which have a positive impact

on net profit and business per employee. Mishra (2011) delivered a useful advice to safeguard the safety of internet-based transactions (IBT).

The customer of the banks should not reply to any SMS, calls or Emails, requesting for password and not to connect on any link for banks website. E-Banking has arisen from such an advanced improvement. Zamdi et al (2013), studying 56 countries over 2008-12, calculate that USD 983 billion were added to their cumulative real GDP because of increased card usage. Among the emerging economies, India at a lower level of 0.047%. Dhananjay B and Suresh Chandra B (2015) expressed that retail electronic payment system has progressed in the recent years. The creation of NCPI set the stage for the development of Electronic payments. In this ratio of electronic clearing grew from one percent to three percent. Mukhopadhyay (2016) in their study of benefits from cashless society found that as more payments are directly credited to the account, cashless payments increase significantly. Dr. Karunagupta, Mr. Ravindraarya, (2017) focused on emerging trends in the banking sector in India, he focused on the banking sector with reference to digitalization. The digitalization of banking system leads to a strong foundation in of economy and to ready to become cashless economy to transform the Indian banking industry.

With the passage of time, Concept of E-Banking has got consideration in Indian context. E-Banking services have been effectively implemented by many public and private sector banks as it is profitable for Consumers as well as banks. The Role of information and technologies has been exceptional in endorsement of e-banking. Many financial innovations like ATMs, credit cards, RTGS, debit cards, mobile banking etc. have

completely changed the face of Indian banking. But still there is a need to have more innovative solutions as even now also e-banking is faces many challenges like , i.e., Risks regarding security, privacy, trust factor, lack of knowledge among consumers in relation to e-banking, unsupported infrastructure, Low level of computer literacy among existing staff, etc are acting as obstruction in the implementation of e-banking facilities. Government of India in synchronization with many public banks & financial Institutions are making an attempt to create an E-banking which is more safe, reliable and protected. This paper also highlights the opportunities that are available in India for the development of e- banking. Key opportunities can stated in terms of untapped rural markets, competitive advantage held to Banks, increasing internet users, efforts initiated by government of India, etc. In contrast to overseas banks, online services presented by domestic banks still have an extended way to move. One fact to be admitted is that supportive and efficient infrastructure can make Indian Banks reach masses. This paper fundamentally analyses and presents the sketch of E-Banking in India. Studies in the past have discovered that Internet Banking is accepted by Indian consumers and the growth is certainly overwhelming now, however, it comes with an heavy price - internet fraudsters and scammer, which this paper is trying to look into.

2.1.3 Evolution of Electronic Banking in Nigeria

In the few years, past, Nigerian financial institution, particularly banking industry incorporated electronic banking, through the help of development of information technology. The Allstate Trust bank was the first to introduce e-payment in 1996 through the approval of the Central

Bank of Nigeria to introduce a close system, electronic purse called Electronic Smart Card Account (ESCA) (Imala, 2002; NIBSS, 2015). The introduction of Pay card, followed in 1997 by Diamond Bank with the authorization in February 1998, this e-money product card open platform of Smartcard Nigeria Plc Which established by a group of 19 banks to manage and produce cards known as “Value card” and used by the member banks. Between 1999 and 2002, many banks launched their websites with the aim of starting electronic banking. In November 1999, another group of 20 banks in the Gem card Nigeria limited got the Central bank of Nigeria approval to introduce the “Smart pay” scheme. As from 2002, many banks have been given the approval by the central bank of Nigeria to introduce telephone banking, international money transfer and electronic banking through a limited level (Imiefoh, 2012; Chiemeke,Evwiekpaefe & Chete, 2006; Ezeoha 2005).

A lot of sophisticated on-line banking products were, thereafter, introduced to enhance better delivery and customer satisfaction. According to Central Bank of Nigeria 2003, “Automated Teller Machine; Personal Computer banking; Cards, Telephone Banking and On-line Banking is now available in Nigerian banking system”. Correspondingly, the study of the range of electronic banking approval and implementation by Nigerian financial institutions, the Central Bank of Nigeria (CBN) (2002) disclosed that out of the 89 licensed banks that were available in the nation, 17 were operating online banking, 24 were operating telephone banking, while 7 had started an Automated Teller Machine system, and 13 were operating other types of electronic banking.

As of 2002, it indicates that the average Nigerian bank was operating at least one form of electronic banking; thus, indicating that electronic banking was yet to operate at full range, regardless of its extensively acclaimed aids in compared to traditional banking firms (Ezeoha, 2005). Therefore, Nigerian banks today are extremely into new on-line delivery channels for electronic banking services and products with the aims of better performance in servicing and satisfying customers. The Nigerian banking industry has advanced from traditional services to electronic banking (Salu, 2004; Oghenerukevbe, 2008). Gorman (2006) agreed that banks gained a hundred and seven times of total cost as soon as electronic banking was adopted. It's all time accessibility makes it suitable for the banks' customers. Nigeria as any developing nation is not up till now to be seen at this stage and therefore cannot be found with similar levels of banking services like Western societies or developed countries. For instance, more than an average of populace in Nigeria, is not banked and transaction electronically. (Kanu and Okorafor, (2013); Igbaekemen, Abbah and Geidanm (2014).

Nigerian banks have in the recent past through reorganization transmuted from manual systems to automated systems. Ogbuji, Onuoha, and Izogo, (2012) in the research titled "Analysis of The Negative Effects of the Automated Teller Machine as a Channel for Delivering Banking Services in Nigeria" paper-based payment instruments have been replaced with an automated means of payment in Nigeria, thereby enabling the use of electronic banking transactions. The current adoption of mobile telephone system in Nigeria has enhanced the use of personal computers and internet service facilities to

facilitate the progressive use of electronic banking and to enhance cashless era. The low rate of electronic banking services in Nigeria is emanated from the high proportion of illiterates and electronic banking fraudsters' activities in the country (Owolabi, 2011). Also, asserted by Uchenna and Agbo, (2013) that participating of the customers in this new process of electronic banking in Nigeria is far from being achieved as a result of internet fraud and lack of adequate regulatory framework for prevention and detection.

Conversely, increasingly over the years, Nigerian banks have observed a lot of institutional reforms and regulatory. Just of recent, The Central Bank of Nigeria introduced reforms by looking at decreasing the number of banks in the nation and building the emerging banks to be much more dependable and stronger. This occurred through great challenges faced by the banks in Nigeria such as: corruption, inadequate capital base and asset quality, loss in public confidence, fraudulent practice (Fatokun, 2016). Therefore, with the aim to compete with the global financial economy and to advance the quality of their performance delivery, Nigerian banks must invest enormously on security to escape from the menace of the fraud which is currently ravaging the Internet Banking Operational Activities as occasioned by so called Yahoo-Yahoo Boys and Girls in the Nigeria Parlance.

2.2 Concept of E-Banking Fraud

Numerous definitions of fraud have been advanced in the crime literature. Wells (2014) defined fraud as unlawful gain through deception. Taylor (2011) argued, in line with Wells, that fraud is stealing, disguising and obtaining personal gain from another person or a group

of persons through deception. Curt's (2013) noted that fraud contains the acquisition of property or monetary advantage by way of deception, either concealment or misrepresentation. Boniface (1991), agreeing with the above three authors, described fraud as any deliberate act of illegal deceit, scam or forgery by a group of persons or a person with the aim of modifying facts to gain unjustified personal economic benefit.

According to Graycar and Smith (2002), frauds usually encompass the transaction, falsification or forgery of financial documents and unlawful endorsement.

KPMG (2000) observed that fraud occurs when a person or a group of persons of authority and responsibility refuse standard and violate the rules for the benefit of self-interest at the expense of others. Mirjana Pejic-Bach (2010), opined that fraud is misrepresentation of financial records by an individual or group of individuals among employees in the management of an entity or third parties.

In 1888, the United States Supreme Court accepted that fraud happens when there is a misrepresentation of a material fact by the defendant and the complainant sensibly believes it to be true. Entities, either as individuals or organizations, commit fraud to get a monetary advantage (Silverstone & Sheetz, 2004). Hence, fraud is criminal offences using deception for personal gain to the disadvantage or loss of another person. It comprises activities such as deception, concealment theft, money laundering, bribery, forgery, corruption, embezzlement, conspiracy, misappropriation, collusion, and extortion of material facts (CIMA, 2009).

Furthermore, from the above definitions, fraud can be described as a deception and a false channel for converting another person's (legal

owner) financial and non-financial property and assets for personal interest illegally. It can also be explained as a misrepresentation of financial statement which is intentionally done by internal or external stakeholders of an organization for personal motives. Bank fraud, then, involves the deceitful use of one's position without or within the bank for self-enrichment by intentionally misappropriating the bank's financial means, properties, or other resources held by the bank and collecting funds from bank accounts of customers - Taylor, 2011.

Now what is e-fraud? According to Graham, 2008, electronic fraud is a fraudulent act associated with an automated system by which someone aims to gain fraudulent benefit. The USA Department of Justice described the electronic fraud in the internet perspective as "a fraud system that adopts internet components such as emails, Web sites to existent fraudulent solicitations to potential victims, Web sites, to perform fraudulent transactions, to transmit the proceeds of fraud to banks or to others connected with the scheme" Finch, 2010.

The differences in the definitions of e-fraud are attachable to certain factors such as the varied contexts in which e-fraud has been found to occur. Therefore, electronic banking fraud can be elucidated by the researcher as theft, robbery, forgery and altering of another person's financial assets illegally for self-motivated ends with the help of the internet.

Electronic banking fraud can also be illuminated as a deception and dishonest way of converting another person's monetary advantage for personal benefit at the expense of others with the use of electronic devices and the internet.

2.3 The Panache of Perpetrating Banking Frauds

Again, there are myriads of literature with distinctive styles of frauds. This view has been debated amongst scholars. Hamilton, Justin and Odinioha (2012) in the study titled, "styles of fraud are usually not exhaustive as fraudsters are forever devising new methods."

Therefore, as societies and businesses are expanding as progressive techniques of committing frauds are sophisticated and classy (Pedneault, Sheetz & Rudewicz, 2012).

The growth of businesses and rapid increased of the fraud perpetration are as a result of the development and expansion of the communication and information technology (Silverstone and Sheetz 2007).

Furthermore, Udoayang and James (2004) opined that fraud could be seen in two ways, viz. **bite and nibble** frauds. When an individual taken assets and disappears in order to not be detected is known as bite fraud. This style of fraud usually involves stolen of large assets or huge amount of money and can be easily detected. To escape being detected and tracked down, the fraudster breaks out into a protected colony. **Bite** fraud can occur in the form of electronic frauds particularly, stealing of hardware devices or back-up devices of a computer system. While, an individual or fraudster involves in taking assets in piecemeal or small unit in order to not be detected easily is called **nibble** fraud. This style of fraud is very difficult to be detected at an early stage, hence, this kind of fraud occurs every day and is common in electronic banking frauds,

particularly, fraud through ATM, PoS, Credit Card and Web Banking Fraud.

Moreover, Alao (2016) grouped fraud styles into two, internal fraud and external fraud. When fraud is perpetrated by the individual employee or group of employees of an organization or a bank using computer, point-of-sales, automated teller machine and internet inform of phishing, vishing and counterfeited or forged smart card is recognized as internal fraud. While, fraud committed with the use of bank financial records, customer's financial information and electronic devices such as ATM, internet, mobile app, mobile phone, pocket picking machine by the outsiders, such as service providers, bank customers, suppliers and unknown party is called external fraud (Hansen et al 1996; Sydney, 1996; Adewumi, 1986). Iwuagwu (2000) argued that, fraud perpetration can involve combination of both internal and external which known as outsider-employee fraud. This kind of fraud is difficulty to detect because the insider-fraudster is supplier of financial information needed and bank security information carrier to the outsider fraudster who is an operator of fraudulent acts.

Additionally, Association of Certified Fraud Examiners, (2015) argued that fraud against a business organization can be perpetrated either externally by vendors, customers and other related parties such as individual or managers, employees, officers, and owners of the organization. The author categorize frauds into three basic categories which are: external frauds, internal frauds and frauds against individuals. External frauds are kind of frauds committed by outsiders or third-parties by compromising electronic bank account through personal information about the victims.

This fraud could happen through pharming, phishing and vishing. While, internal frauds also known as occupational frauds, can be explained as a means of using one's profession or occupation for self or personal gain through intentional misuse or misappropriation of the company's resources. This kind of fraud happens when the executives, managers and other employees perpetrate frauds against their employer.

Iwuagwu (2000) further argued that, fraudsters are progressing in the use of technologies and innovative approaches for concealment and perpetration of internal fraud schemes.

While, fraud against individuals is a type of fraud in which many perpetrators have designed systems to defraud individuals such as identity theft systems, phishing systems, advanced fee crimes are just a few of the methods the fraudsters have discovered to defraud unsuspecting victims.

On the same vein, Adeyemo, (2012) opined that, fraud has been categorized in diverse ways and using various methods such as management and employee frauds, customer and non- customer frauds and stakeholder and non-stakeholder frauds. Management Frauds are electronic fraud perpetrated by the top management of the organization. These frauds can be committed through electronic financial statement and the group of sufferers of these kinds of frauds are creditors and investors (Association of Certified Fraud Examiners, 2015). This electronic banking fraud can be perpetrated through the creating of more investment from potential and current shareholder of the organization, Doctor of Financial statement or window dressing of account statement and can occur by painting the bank in better light in the eyesight of the regulatory authorities using electronic systems.

Kevia & Huange, (2011) explained that management fraud as the falsification of financial statements for the benefit of the person perpetrating the fraud. This involves false transaction, bogus trades, backdating of executive security or stock trade options and wrong use of corporate asset for personal benefits and violation of tax rules and regulations for personal gain using the internet and electronic devices. While, Association of Certified Fraud Examiners (2012) concord that management frauds happen through timing differences, fictitious revenues, improper asset valuation, inadequate disclosure and concealed liabilities and expenses. Employees' Fraud is generally known as non-management fraud. It is a kind of fraud committed by the non-management staffs or employees of the organization through forgery of customers' signatures, stealing of customer's passwords, PIN codes and electronic cheque for illegal withdrawal of money from the customers' accounts, creating and operating of fictitious electronic bank account, fund diversion, lending fictitious borrowers and other related computer's fraud or internet frauds, Adeyemo, 2012.

Furthermore, customers and Non- customers' frauds occurred through the act of performing the primary functions of money deposit Banks, which connects capital deficit customers with the capital surplus customers in the money market (Association of Certified Fraud Examiners, 2012). In the process of this, bankers come in connecting or interacting with both non-customers and customers and this leads to the risk of frauds.

These types of frauds may be through counterfeit securities, opening of the fictitious electronic bank account, forged electronic cheque, fraudulent electronic money transfer because of a request made sole

and solemnly through email, telephone, fax, telex, and other electronic means, and skimming card data, Regha, 2015.

While, stakeholders' and non- stakeholders' frauds is the kind of fraud perpetrated through the collaboration of insiders and outsiders, employees and non-employees, staffs and non-staffs of the organization. Before this type of fraud to succeed, there must be an insider or internal fraudster that will be providing financial information while, the outsider fraudsters or external fraudsters will be carrying out the instruction given Adewunmi (1986). However, majority of banking functions in Nigeria are now electronically base activities including transaction of business such as funds, registration of new customers, collection of customers' personal data and preparation of financial statements, particularly in this era of cashless system, then, all types of fraud mentioned above are now electronic banking related frauds and there is need to discover the best way for detecting and perfecting of these menaces.

Chartered Institute of Management Accountants, (2009) differentiated frauds into several types which are also applicable to Nigeria economy. Frauds include the following: Frauds from any individual versus client; customers; consumers and others inform of misrepresentation of the quality of stocks or goods. Employee frauds versus employers inform of payroll frauds; thefts of cash; falsifying expense claims; false accounting and thefts of assets.

In addition, frauds by the organization or businesses versus consumers; investors and employees inform of falsification of financial statement; selling of fake goods as original ones; not paying tax. Frauds by the company or individual versus government in the form of grant frauds;

tax evasion; and social security gain claim frauds. Frauds by professional criminals versus big companies in the form of mortgage frauds; advance fee frauds; money laundering; counterfeiting and corporate identity frauds. Electronic frauds by a group of individual or an organization with the use of computers and information technology through the help of internet to perpetrate frauds inform of spamming; phishing; social engineering frauds; hacking; and copyright.

2.4 Impact of Fraud on Internal and External Stakeholders

E-banking fraud has become a global and provocative issue that produces debate among quite a few authors, for example Usman and Shah (2013), Tan and Rasiah (2011), Saleh (2013), Pandey (2010) and Oghenerukevbe (2008) stated that electronic banking fraud is a worldwide problem and is persistently too costly both to the banking sector and to customers. Until the mid-1990s, the banking industry in most parts of the globe was reliable and dependable (Dzomira, 2015). The new millennium started with an overabundance of activities that have contributed enormously to the academic field and the economy in general, especially electronic banking adoption by the financial institutions. Nevertheless, this e-banking adoption has become a global debate in the academic arena and the financial sector is not exempted (Barker et al., 2008).

Researchers in this phenomenon are still developing and formulating different theories for the electronic banking context (Mhamane & Lobo, 2012). Since the introduction of technology, the banking industry has experienced a paradigm change in the phenomenon (Dzomira, 2015a).

However, with the development of technology, e-banking frauds have similarly increased.

Most statistical bases specify that e-fraud is on the increase, while local forms of fraud are usually in decline (Levi & Williams, 2013; Ablon et al., 2014). The Eurostat 2010 Information and Communication Technology survey undeniably confirmed that ebanking frauds have become the most rampant type of acquisitive fraud in both developed and underdeveloped economies (Anderson et al., 2012). However, the impacts of ebanking fraud were grouped into monetary and non-monetary impacts.

2.4.1 Monetary Impact of Fraud

E-banking fraud is a global phenomenon (Alao, 2016). Fraudulent activities have affected a lot of businesses in the banking sector (Rubasundram, 2015). The findings of the empirical study done by Anderson et al. (2012) offer details of e-fraud perpetrated across the globe in the banking sector, showing that globally, banks have lost billions of dollars to indirect and direct losses. Therefore, e-banking fraud losses continue to cause great problems for several industries, despite significant developments in fraud detection mechanisms. IIA, AICPA, and ACFE (2015), concurred that all electronic banking is susceptible to the menace of e-banking fraud. In reaction to the above, this is a time for the banking sector to give a zero tolerance for fraud; hence there is need for e-banking fraud detection and prevention.

Wilhem (2004) calculated annual losses through fraud for different industries in the United States of America to comprise $67 billion in insurance, $1.2 billion in banking, $150 billion in telecommunication, $40 billion in money laundering and $6.7 billion in e-banking. Also, the

UK office of National Statistics reported in 2015 that the number of bank accounts being opened through fictitious or stolen identities had nearly doubled from the previous year, with over 23,600 instances reported in 2014 compared to 12,500 cases in 2015. This means, e-banking fraud is a universal problem.

Meanwhile, electronic banking fraud in the United Kingdom had increased from £40.9 million to £60.4 million. These losses occurred through the assistance of electronic transactions and are significant challenges to financial institutions in performing their role in the economy (Office of National Statistics, 2015). In 2014, The German cybercrime watchdog, the Federal Office for Information Security, disclosed the stealing of 16 million email addresses and passwords (ENISA, 2014). Also, in 2014, three major worldwide e-banking frauds, together with the biggest ever documented, caused by the theft of customer records and counterfeiting of above two billion credit cards from large US retailers which caused liquidation of some banking industry and other were left in a state of insolvency (Perlroth & Gelles, 2014; Finkle & Hosenball, 2014). This indicates that, bankruptcy is one of the impacts of e-fraud and also, a lot of fraud incidences occurred are as a result of loss of customer's financial data or identity fraud Generally, fraud activities eventually lead to bank failures. Financial Fraud Action UK (FFA UK) (2016) in their report between January to June 2016 Fraud Update: Payment Cards, Remote Banking and Cheque", reported £13.1 million loss in the United Kingdom to telephone banking frauds in the first half of 2016. In the third report of the European Central Bank of Nigeria (2014) on card fraud, the fraudulent transactions committed in 2012 within the "Single Euro Payments Area (SEPA)" totalled €1.33

billion, which serves as an increase of 14.8% from 2011. It was uncovered that 60% of the value of the reported fraud resulted from telephone and internet payments, 23% represented payment at point-of-sale (POS) terminals and fraudulent transactions, and 17% was from automated teller machines (ATMs). This shows that, all e-banking's channels of transactions are susceptible to frauds.

NIBSS (2015) that there was a significant increase of 78% in the volume of fraudulent incidents in 2014. The author's findings showed the vast amounts of N485, 194,350 (£1,239,690) and N6, 215,987,323 (£15,882,085) that were lost to fraudsters in 2013 and 2014 with 822 and 1461 cases respectively. NDIC (2016) reported N857 million (£2.2 million) actual loss sustained in electronic banking fraud in Nigeria, representing 27% of the total actual loss of the banking industry in 2016. Therefore, this confirms that, monetary loss is one of the significant impacts of e-banking fraud.

Moreover, regarding electronic payment system attacks, Financial Fraud Action UK (2015) reported that fraud losses on UK-issued cards in 2015 amounted to £567.5 million, an increase of 18% from £479 million in 2014. Saudi, Ismail and Tamil (2007), in their study titled "Phishing: Challenges and Issues in Malaysia", showed that in 2004 and 2005, the United States suffered losses of approximately $929 million from phishing frauds, the United Kingdom lost £12.2 million and £23.2 million in 2004 and 2005 respectively from phishing, and the loss suffered in Malaysia was RM18, 000 in 2003. Financial Fraud Action (2015) reported 1,028 cases of phone fraud in 2014 and vishing frauds costing £23.9 million in the United Kingdom in 2014, compared with £7 million

reported in 2013. Apparently, vishing and phishing have negative impacts on the e-banking stakeholders.

US Payments Forum (2017) disclosed 16,594 victims and $517,653 loss to pharming attacks in 2015. Norse (2014), the Javelin study in USA, estimated losses over $4.9 billion from account takeover fraud in 2012. Meanwhile, Financial Fraud Action UK (FFA UK) (2016), in the report titled “Fraud the Facts 2016”, reported actual loss of £29.4 million in UK financial industries through account takeover attack. Obviously, pharming and account impersonation are part of the major challenges facing e-banking activities.

In addition, Everyone API (2014), in the study “Fraud Mitigation and Identity Verification for Card Not Present Transactions” disclosed that businesses suffer losses of over $11,000,000,000 dollars yearly. The percentage of income lost to card-not-present fraud is increasing, rising from 0.51% in 2013 to 0.68% in 2014. Losses to merchants through phone, web, and mail order are mainly from card-not-present financial transactions. Likewise, Pandy (2016) declared in the study titled “Mitigating Fraud in the Card-Not-Present Environment” that card-not-present fraud resulted in 25% of global fraud losses and 45% of card loss in the US in 2015. And also, Dzomira (2015) study of “Cyber-banking Risk Mitigation” the Banking Industry in South Africa” reported R168.1 million and R189.2 million losses due to card-not-present fraud in 2014 and 2015.

Therefore, there is a need to begin to develop strategies to mitigate card-not-present fraud, as several developing and developed nations have experienced significant spikes in this type of fraud.

Financial Fraud Action UK (FFA UK) (2016) reported a £39.24 million loss for skimming device fraud. According to RSA (2010), this increase is a result of an increase in usage of advanced and sophisticated tools by the fraudsters to target internet banking users through the automated pickpocket machine to pick card data and malware which targets vulnerabilities in the user's computer rather than the bank's own devices, which are hard to attack. Furthermore, the recent upsurge in fraud provides growing evidence that networks of malware and hijacked computers serves as most momentous threats in relation to present-day identity theft.

2.4.2 Non-Monetary Impacts

Manyika and Roxburgh, 2011 argued that the banking sector and customers suffer not only money loss, but also non-monetary loss due to the incidence of frauds. Fraud has a negative impact on operating efficiencies, reliability of services, companies' reputations, investors' confidence, employee morale, and can also lead to potential fines levied by regulatory bodies (BITS, 2003). Unfortunately, electronic banking causes huge investment losses, substantial legal charges, loss of assurance in capital investment, and imprisonment of important individuals (IIA, AICPA & ACFE, 2015). In addition, Norse (2014) supported the view that electronic banking fraud can lead to loss of consumer trust, damage brand reputation, cause financial damages, and endanger compliance with financial institutions' regulations.

Generally, in conclusion, there is a need for the collective accord of regulators and banks to enact policies and implement measures to protect and prevent the banking system from e-fraud threats. Therefore,

the importance of appraisal of electronic banking fraud prevention and detection cannot be overemphasized. Hence there is a need for incessant improvement in safety and security to avert frauds and alleviate the risks suffered by banks, customers and other industries, which have resulted in loss of confidence in electronic banking systems.

2.5 E-Banking Attacks and Techniques

There are several major information types targeted by e-fraudsters to defraud an individual or an organization: personal data, educational information, health information, credential information, payment card data, financial information, others and unknown through hacking or malware, insider leaks, payment cards, fraud loss or theft and unintended disclosures.

Also, Park (2015), in a study titled “Follow the Data: Dissecting Breaches and Debunking Myth” supported the view that malware or hacking are employed to compromise any kind of records through phishing, unauthorized access to servers, vulnerability manipulation, compromising of databases and servers and unauthorized access to debit and credit cards. Restaurants and retailers were sufferers of payment card fraud through skimming devices, use of POS RAM scrapers of collecting payment card information, and frequent fraudulent transactions through stolen payment card data Moreover, unintended disclosures occurred because of accidental posting of personal identification data, education data and health data online, and negligent data leakage by third parties and contractors. Insiders such as employees are also involved in fraud; they usually target financial information, personal identification data, and health and payment card

data. They use these for fraudulent tax claims, to defraud customers' accounts, for identity theft and for selling customers' data to outsiders with the aims of defrauding those customers' accounts or committing other crimes. Loss and theft also compromise personal identification data, education data, health data, and financial data and make them vulnerable to fraud (Anderson et al., 2012). This happens through theft or loss of portable and removable devices (laptops, backup drives, USB keys and others); physical or hard copies of the records (bills, files, receipts and others); and stationary devices (office-use computers and other specialized business equipment).

Figure 2.1: Information Stolen and Methods of Fraud

In addition, Park (2015) stated that there are unknown methods that can cause online fraud incidents in banks, which can also compromise payment cards, financial data, personal identification information, education data and health data. The author's analysis across the industry between 2005 and 2015 in a Bayesian network showed that online fraud consisted of 25.0% malware or hacking, 24.0% portable device loss, 17.4% unintended disclosure, 12.0% insider leak, 11.6% physical loss, 5.4% stationary device loss, 1.4% payment card fraud and 3.2% unknown. Therefore, there is a need to take cognizance of the above to have effective prevention and detection of electronic banking fraud in financial institutions.

Additionally, the United Computer Emergency Readiness Team (US-CERT) (2015) supported the view that unauthorized access in the situation of electronic banking implies that an individual or group of individuals

access a bank's or a customer's system without permission. This can result in the theft or loss of account information, personal identification information and account passwords, and the transfer of vast amounts of money through the same system into an unknown account. Another method is when unauthorized software is installed in the victim's computer system, for example, malicious code, infecting systems with viruses, recording of keyboard strokes, and stolen data.

Moore, Clayton and Anderson (2009) concluded that there are various categories of attacks of electronic banking, but all may involve either stealing authentication identities from the victim or altering the victim's reasonable transactions. Moore and Clayton (2009), and Wang, Rashid and Chuang (2011) categorized attacks as a means of denying the victim access to their bank, or else watching their e-transactions. However, the aims and objectives of hackers are different. Hackers may decide to exploit vulnerabilities in targeted operating systems or gain unauthorized access to a website to deny customer services (Brar, Sharma & Khurmi, 2012). Attackers or hackers have several ways they use to gain access to the targeted system. However, the challenge facing information systems today is takeover within the system of computers and communication (Omariba, Moses, and Wanyembi, 2012). Therefore, information service providers and financial institutions need to guard against diverse types of electronic attacks to accomplish safe and sound communications in the networks of information systems.

Furthermore, researchers have categorized the diverse types of attacks against electronic banking in several ways. Vrincianu and Popa (2010) reported that the main types of attacks on the security of electronic banking are illegitimate use, denial of service, repudiation and disclosure

of information. Dalton and Colombi (2006) suggested a hierarchy of causes which involved three main categories: credential theft, device compromise and illegitimate access. Peotta, Holtz, David, Deus and Sousa (2011) adopted an attack tree model to represent the major attacks and how they associate with each other; for example, phishing attacks, and social engineering, malware to gain control of system devices, and malware and fake web pages for credential theft from an authentic user.

Omariba, Moses and Wanyembi (2012) classified the different attacks that electronic banking can suffer into the following types: port scanners, social engineering attacks, phishing, Trojans, pharming, denial of service, PIN hacking, super user exploits and server bugs. Conversely, Brar, Sharma and Khurmi (2012) grouped attacks into three major categories: local, remote and hybrid attacks. Local attacks occur on the user's device: when the bank website is opened, the uniform resource locator (URL) in the address bar is not spoofed, and the yellow secure sockets layer (SSL) padlock exposes the correct certificate information; but only an overlapped fake password prompt is maliciously set on.

One common type of local attack is shoulder surfing, which is usually related to observing and detecting the personal identification number for a bank card, before stealing the physical bank card either by pickpocketing or by force (Brar, Sharma & Khurmi, 2012).

Remote attacks do not modify the user's device but aim to redirect or intercept the traffic of a session. Phishing, vishing and cloned voice-banking systems are some of the types of remote attacks (Brar, Sharma & Khurmi, 2012). Bo and Surya (2003), in a study of reputation services in electronic markets, stated that Trojans are programs that compromise

a computer without the knowledge of the user. Lewis (2011) posited that the most globally documented malware in e-banking fraud is recognized as being the Zeus Trojan. Likewise, Bo and Surya (2003) also estimated that the Zeus Trojan was accounted for about 90% of the e-banking fraud across the globe since it had been placed into the financial market. Zeus has developed into almost a variety of forms of Trojan.

Finally, hybrid attacks are a combination of both local and remote attacks. A Trojan is the best example of a hybrid; it will be executed on the vulnerable system, examining all saved bookmarks and exchanging any useful online service URL with a counterfeit one (Omariba, Moses & Wanyembi, 2012). The Trojan also modifies the browser settings to disallow the address bar from displaying or overlap it with a forged pop-up window to prevent the user from seeing the modified URL (local attack). The more sophisticated the approach taken against an attacker, the more attackers also redirect domains and change the host file to predefine the Internet Protocol address (Brar, Sharma and Khurmi, 2012) (see Figure 2.2).

Figure 2.2: E-Banking Account Compromise

However, the followings are the most common attacks used by the fraudsters to commit e-banking frauds. These are discussed below. First, electronic Payment System frauds: These are the manipulation of account information through electronic payment devices such as a debit or credit card for direct payment Hoang, Hu, Bertok (2003). However, Financial Fraud Action UK (2016) reported fraud losses through UK-

issued cards in 2015 amounted to £567.5 million, an increase of 18% from £479 million in 2014. Correspondingly, KPMG (2016) KPMG Forensic Services report of investigation carried out on "Top Five Fraud Trends in Nigeria's Commercial Banks in 2016" shows that, Nigeria suffered actual loss valued N485, 194,350 and N6,215,987,323 of electronic payment frauds in 2013 and 2014 respectively.

Second, phishing is the fraudulent perpetration of sending electronic mail or pull-down (pop-up) web pages claiming to be from legitimate enterprises so as to convince people or entities to provide sensitive or personal account and business information such as account information, credit card numbers, passwords and memorable words (Brar, Sharma and Khurmi, 2012). Phishing occurs when the fraudsters set up a fake copy which includes all the code of the web site targeted to impersonate on a server they control.

Next, the fraudsters may send an email of convincing messages to the numerous number of email addresses, to deceive the recipient of the email and to mislead them into the spoofed web site by revealing their log in information Hoang, Hu, Bertok (2003).

Jakobsson (2005) opined that phishing is a popular method of stealing authentic identifications of the victims. Abu-Shanab and Matalqa (2015) described phishing as an attack premeditated to influence the victim to give away their electronic banking information to an unauthorized party. The followings are some of the phishing techniques used to steal the financial information and identification data of the electronic banking customers, which are Trojan, Shoulder surfing, Social engineering and key loggers (Symantec Security Response, 2005). Phishing web sites are the most popular attack form of credential stealing in the world,

commonly joint with an email with deceptions to have access to the user's websites (Hooks, Kaplan, Schultz and Ponemon, 1994). Bossler, (2009) opined that phishing websites are totally a social engineering fraud which depend on the user's understanding of system security and problems with the way indicators of security are presented to the users. The attached model below describes in more detail the phishing attack.

Chaturvedi and Meen (2016) suggested that phishing attacks can be carried out through the following methods: Domain Spoofing, URL Modifying and Web Site layout similarities. Saudi, Ismail and Tamil (2007) in their study titled "Phishing: Challenges and Issues in Malaysia" shows that between 2004 and 2005, United States suffered losses approximately $929million from phishing frauds and United Kingdom lost £12.2 million and £23.2 million in 2004 and 2005 respectively through phishing on the web banking while, the loss suffered in Malaysia is RM18, 000 in 2003.

Third, vishing occurs when the hackers, phone the victims and trick them to reveal some secret data through the uses of social engineering. Cloned voices-banking systems happen as a result of many vishing attacks by clone the voice in the banking systems so that it sounds similar as the original banking systems. Fake e-mail is adapted to beseech customers to call a number claiming to be their bank (Dalton, and Colombi, 2006). In the report of the Ombudsman (2015) titled "Calling Time on Telephone Fraud" describes vishing as voice phishing, as the fraudsters' practice of employing the phone to deceive and defraud people. Vishing is another means used by the fraudsters to gain access to victims' account information. The author termed vishing as "no hang-up fraud" which involves giving away of account information,

personal identification number details and online money transfer over the phone. CIFAS, (2010) corroborate the issue in the report titled “Digital Thieves”, text phishing and phone vishing frauds are increasing every day.

Action Fraud (2015) reported 1,028 cases of phone fraud in 2014 and vishing frauds of £23.9 million losses in the United Kingdom reported in 2014 compared with 7 million reported in 2013. Financial Fraud Action UK (FFA UK) (2016) in the report of “January to June 2016 fraud update: Payment cards, remote banking and cheque” reported £13.1 million loss in the United Kingdom to telephone banking frauds in the first half of 2016.

This is done by the use of cloned voice-banking system, voice-over-IP and automated answering systems (Abu-Shanab & Matalqa, 2015).

Fourth, pharming is used for hijacking and stealing the web address of service supplier. This happens when a service user enters a Web address and it transmits to a Web site of fraudsters without the knowledge of the senders. The website will resemble the legitimate website with the intent of capturing confidential information of the sender (Kirda & Kruegel, 2014). Pharming refers to wrong direction of a criminal website through technological means. For example, an electronic banking user, who usually accesses his internet banking website, may be misdirected to an illegal website instead of being directed to his own banking website or legitimate website (Brar, Sharma & Khurmi, 2012).

Pharming is an illegal practice in which malicious software is installed on a user computer system or server, misleading the users to criminal websites without the consent of the users. Pharming can happen in four distinct ways: spoofing, malicious, hijacking and domain name server

(DNS) poisoning (Abu-Shanab and Matalqa, 2015; Brar, Sharma and Khurmi, 2012; Peotta, et al., 2011; Dalton, and Colombi, 2006). Spoofing occurs when the pharming criminal uses slight mistake in the domain name or fake domain name to divert the attention of the user from accessing the intended website to have unintended visiting into pharming criminal's website. For instance, a pharming criminal may redirect the user to www.mydmu.dmu.au.uk instead of www.my.dmu.ac.uk (Abu-Shanab and Matalqa, 2015). Likewise, malicious software (Malware) occurs through Trojans and viruses installed in a personal computer of the user by interrupting and diverting the user's attention to access the criminal website instead of the intended website (Peotta, et al. 2011).

Equally, domain hijacking is a situation when the hacker redirects transmits of the legitimate online traffic to an illegitimate website. This can be done in two ways: Domain slamming is an unauthorized transmission or a domain registration scam in which fraudulent domain name administrators tricks the domain holders to switch from original and legitimate registrar to their fraudulent domain registrar or illegitimate server (AbuShanab and Matalqa, 2015).

Correspondingly, domain expiration is a situation when a domain name is leased for a specific period and the lease agreement procedure is not properly managed until it resulted to wrongly transfer or loss of legitimate ownership (Dalton, and Colombi, 2006). This is usually occurs through mail of notification of expiration sent by fraudsters, not original domain registrar to legitimate domain service users notifying them that their domain registration services are about to expire and the mail contains the means of renewal or purchase engine traffic generator

software which contradict to the original domain service or is the service the recipient of the main has never procured or used and probably does not want (Peotta, et al. 2011). Similarly, Domain Name Server (DNS) poisoning: This is a dangerous pharming which happen when a user enters domain name and the domain name server on the internet protocol address change the domain name and redirects the user to another website or fraudster's website. This poisoning can happen as a result of malicious software (Malware) installed on the server, misconfiguration and network vulnerabilities (Brar, Sharma and Khurmi, 2012). Respectively, Jackson (2009) explained that, 13 root DNS servers are available for the entire internet, which are strictly control and protected. Utmost of the requests are directly transferred from the local DNS server into root DNS server. However, if hackers were to infiltrate any of these root DNS servers, the internet banking would be violently compromised. US Payment Forum (2016) disclosed 16,594 victims and $ 517,653 loss to pharming attack in 2015.

Six, Account takeover occurs when a person or a group of people overthrow another person's account, through capturing of the confidential information of the targeted victim, and then communicating the card issuers by impersonating the legitimate cardholder and requesting for a mail to be forwarded to a forged address. The fraudsters then report for loss of card and enquire for a reissued card to be sent. The fraudsters may then create a new PIN so as to free to use the card until the legitimate cardholder notices the deception when tries to use the card and discovered that the account has been drained (Hoang et al, 2003).

Account Takeover also called Facility Takeover. Fraud happens when a third party impersonates someone by making an application for insurance, credit or other services to hijack a person's existing policies, accounts or other similar services and use them fraudulently (Sharma & Khurmi, 2012). Pandy, (2016) opined that account takeover occurs when a fraudster uses stolen identifications harvested from stolen documents, payment cards and data breaches to create new accounts.

Financial Fraud Action UK (FFA UK) (2016) explained that accounting takeover happens when a fraudster fraudulently uses another person's debit or credit card account, first by collecting accounting and personal information about the targeted victim, then communicate their credit card issuer or bank to pretend as the legitimate card or account.

The fraudsters then plan for funds to be paid out of the bank account, or they can change the legitimate address on the bank account and request for replacement or new cards to be sent which can be then used fraudulently.

However, Norse (2014) the Javelin study estimated losses over $4.9 billion from account takeover fraud 2012 which represent an increase of 69 percent in 2011$4.9 billion. While,

Financial Fraud Action UK (FFA UK) (2016) in the report titled "FRAUD THE FACTS 2016" reported actual loss of £29.4 million in UK financial industries through account takeover attack.

Seven, Card-Not-Present fraud: An illegal use of card information on the internet or through the phone (Anderson et al., 2006). Pandey (2010) Card-not-present happens when payment made for a procurement using a debit card or a credit card at where the card is not physically present to permit the bank or card issuer to authenticate the cardholder at time

of transaction or purchases, such as payments transaction made by phone internet or mail. For instance, Everyone API, (2014) the findings of the study “fraud mitigation and identity verification for card not present transactions”, disclosed that, businesses suffer losses of over $11,000,000,000 dollars yearly. The percentage of income lost to card-notpresent fraud is increasing; rising from 0.51% to 0.68% in 2013 and 2014 respectively.

Losses through phone, Web, mail order to merchants are mainly from card-not- present financial transactions. The author in 2012 concluded that 42% of Americans had been the victims of credit card fraud in the last 5 years. Likewise, Pandy (2016) declared in the study titled “Mitigating Fraud Risk in the Card-Not-Present Environment” that Card-NotPresent fraud resulted to 25 percent of global fraud losses and 45 percent of card loss in U.S. in 2015. Likewise, Chigada and Ngulube (2015) survey on card fraud, banking industry in South Africa” reported R168.1 and R189.2 million fraud losses due to cardnot-present (CNP) in 2014 and 2015. Therefore, there is need to begin developing strategies to mitigate card-not-presented fraud as several developing and developed nations experienced significant spikes of Card-Not-Presented fraud.

Eight, skimming is a fraudulent practice by gathering of payment card information using electronic device. The smart card can be inserted in the point-of-sale (PoS) terminals or automated teller machine (ATM) that allows fraudsters to capture card details including cardholder’s name, card numbers, issued and expired dates, secret code and PIN. The introduction of wireless system has made it possible for fraudster to greatly download stolen information without physically appearances at the terminals (Ford, 2011).

Financial Fraud Action UK (FFA UK) (2016) described skimming as skimming devices attached to the automated teller machine to capture the details from the card's magnetic stripe while a miniature camera records the personal identification number (PIN) being entered FFA UK (2016).

A fabricated magnetic stripe card is then manufactured and used with the legitimate PIN to withdraw or transfer cash at machines within the country and overseas, which have yet to be advanced to PIN and Chip FFA UK (2016). While, Shoulder surfing is when the fraudsters watch the legitimate cardholder inserting and entering their PIN, then steal the card by using pick pocketing or distraction techniques. Financial Fraud Action UK (FFA UK) (2016) reported £39.24 loss to skimming device fraud. Chigada and Ngulube (2015) reported that banking industry in South Africa" disclosed R89.2 and R48.5 million fraud losses due to credit card skimming in 2014 and 2015 Ninth, SIM Swap fraud happens when the phone number of a bank customer is stolen through fraudulent SIM replacement at a Telco outlet/agent. The perpetrator then uses the mobile line to access the account of the victim usually via mobile banking or receives account sensitive details like PIN through PIN reset request (Bahnsen et al., 2013).

Tenthly, traffic injection is a traditional method of attack which uses to modify the financial transactions being made by the user so as to redirect it or vary the amount concerned. Traffic injection is done by manipulating and hacking internet router which the traffic passes or counterfeiting packets. Traffic injection can be done through evil tor nodes, access points, proxy server, hacking internet routers, Trojans and ADSL routers (Brar, Sharma & khurmi, 2012) (see Figure 2.3).

Figure 2.3 Traffic Injection

Park (2015) opined that injection aids, electronic fraudsters to steal electronic banking users' credentials and to inject and manipulate transactions while bypassing or evading two factor authentications. Since many banks use two factor authentication techniques (Sign In – Phone Banking Code and Sign In – Token) for transactions such as token and mobile phones, any unpredicted transaction notice will suddenly ring an alarm to the internet banking customers. This inject deploys a social engineering method when injecting a transaction.

2.6 The Contributing Factors for E-Banking Fraud Increase

With the global use of progressively advanced internet technology, electronic banking is developing as a great medium or network for banking businesses (Chanson & Cheung, 2001). However, electronic banking fraud perpetrations are becoming more sophisticated, unbearable, greatly intimidating the security and trust of electronic banking activities.

Agwu, (2012) viewed electronic banking fraud as an epidemic disease in the banking industry, which has become a great challenge to both management and customers of the industry. E-banking fraud has become a global and provocative issue that produces debate amid quite a few authors like Saleh, (2011); Pandey, (2010) that electronic banking fraud is a worldwide problem and is persistent to be overpriced to both banking sectors and customers.

Corroborating the views, Usman and Shah, (2013) frauds in electronic banking services happen as a product of several concessions in security

extending from inadequate internal controls to feeble substantiation systems. Electronic banking fraud is now a thoughtful matter of financial crime management in all financial institutions. The development and advancement of challenging of electronic banking frauds such as ghost website, phishing scams and malware have coursed a massive loss in the banking industries worldwide (Wei, et al. 2013). Therefore, there is need to examine the causes of electronic banking frauds. Uchenna and Agbo (2013) a lot of factors contribute to the menace of fraud perpetration in Nigeria, which is grouped into: technological challenges and nontechnological challenges. Ojo (2008) and Idowu (2009) also classified the causes of fraud in the banking industries into: the endogenous (institutional) challenges and the exogenous (environmental) challenges. Hence, for the benefit of this study, the factors contribute to the increase of e-banking fraud were grouped into technological factors and non-technological factors which explained below.

2.6.1 Technological Factors

The introduction of Electronic banking has come with its risks and challenges, starting from electronic banking adoption to financial transaction with the new system (Usman & Shah, 2013). The research concluded to several factors that impact the adoption and implementation process of electronic banking such as system security, accessibility, trust and social influence, the cost and time factors embedded in fund transfer, its usefulness and ease of use (Abu-Shanab, Pearson and Setterstrom, 2019). Security is a factor that is frequently emphasized as a critical success factor (CSF) for the success and effectiveness of electronic banking. The deficiency of security will

possibly lead to negative media publicity, financial losses and disciplinary measures by regulators. Security was ranked by some researchers as the significant concern of electronic banking operations (Yan et al, 2009).

Moreover, grounded in an empirical analysis completed on real world transaction datasets, Kovach and Ruggiero, (2011) discovered that a lot of electronic banking accounts were defrauded by only one fraudster, which involved a small amount of money transaction with a total amount of money larger than one account. The author concluded that many frauds occur as a result of increased number of password failures which give opportunities to fraudulent behaviours. Correspondingly, in the survey carried out in Australian banks on electronic banking frauds, the finding showed that almost electronic banking frauds have the following challenges and characteristics, ineffective real time detection, weak forensic evidence, dynamic fraud behaviour, imbalance large datasets and diverse behaviour patterns of customers (Wei, Cao, Ou, & Chen, 2012).

Jassal and Sehgal, (2013) in their study titled “electronic banking security flaws” aimed at finding diverse types of faults in the security of electronic banking that end to loss of money by customers and banks. The authors discussed the reasons of security breaches and the involvement of both banks and customers in giving a chance to crackers and fraudsters to have access into their networks through web-browser installed on their customer’s personal computer which give opportunities to unauthorized persons to have access to their personal identification information and financial information (Nor, Shannab & Pearson, 2008). Usman and Shah, (2013) viewed electronic banking fraud as a global issue which is persistent to prove costly to both banking

sector and its stakeholders. Electronic banking frauds happen because of different concessions in security started from feeble authentication systems with inadequate internal controls.

Electronic banking fraud could be from bank website, such as cross site scripting through malicious and SQL statement entered by attackers into the web page of the bank (Schneier, 2011). Omar et al. (2011), argued that most stakeholders willing to use electronic banking services because of its convenience, cost effectiveness, speed and easy accessibility, but the finding reveals that ATM machine problems; electronic frauds and insecurity. European Central Bank (2014) reported that card fraud payment is one of the major means of fraud such as counterfeit card, card not received, lost and stolen cards.

The author further elucidated that the contemporary mobile devices with their operating system were not intentionally produced with the security of financial payment, the transmission of personal data and sensitive payment through the use of radio technology leaks mobile payment to risks, unlike traditional payments, mobile payments expose include extra actor in the signal transmission such as mobile network operators and also, the general public may not have adequate awareness of the associated information security risks attach to use of mobile devices and internet desktops or laptop for payment at home.

Correspondingly, Adedipe (2016) in the study internet fraud, findings show that, the external fraud is fundamentally direct outcome of hackers' activities which include unauthorized access to electronic bank account information which are accomplished through pharming attacks, phishing attacks, session hijack, skimming attack, eavesdropping hijack,

brute force attacks. These are emanated through bank staff and customers' ignorance and unawareness of common social engineering techniques, negligence in displaying PIN code and accounting information, and carelessness disposal of computer devices and related software.

Deloitte (2015) in the study of "India Banking Fraud Survey" discovered that there is increase in the electronic fraud occurrence in the banking sector because of lack of the tools and technology to discover the potential red flags. Likewise, Regha (2015) concord that difficulties in preventing electronic banking frauds could be influence by the following factors which involve: ineffective monitoring of electronic banking channels such as ATM terminals, internet banking, telephone banking, personal computer banking and card teller banking, non-existence of camera such as CCTV at e-banking transaction terminals, absence or inadequate of system base solution to trace and to report suspicious transactions and compromised accounts, lack of compliance to Know-your-customer and best practice procedures of e-banking management, no segregation of transaction limits, failure of incorporating string validation test of security, ineffective encryption key management, inadequate control to restricted environment and availability of ex-staff with active login pin to e-banking management system data base.

Equally, Odediran (2014) the findings in the study titled "holistic approach to electronic channels fraud management" shown that, the factors that influence the rising cases of electronic banking frauds in Nigeria are Ignorance of cardholders on card usage security, Inadequate monitoring of electronic payment terminals and lack of adequate

management of electronic bank production services. Gates and Jacob (2009) have pointed that the factor contributes to increase of e-banking fraud is the mismanagement of technology in the banking industry which comprises use of technology for illegal activities, sharing of confidential data, banking access for over-payments to sellers. European Central Bank (2014) in the survey of cards fraud, further elucidated that the contemporary mobile devices with their operating system were not intentionally produced with the security of financial payment, the transmission of personal data and sensitive payment using radio technology leaks mobile payment to risks. Banking services and other financial industries experience losses annually through fraud incidences such as internet banking frauds, cheques and cards frauds (Adams, 2010).

Therefore, these obviously signify that fraudsters are exploiting electronic banking channels. Moreover, Brunner et al. (2004) in their survey, found that the location of Automated Teller Machine (ATM) is a high determining factor for fraud perpetrating at Automated Telle Machine point. From this study, above 75% of the respondents confirmed that the location of Automated Teller Machine (ATM) in isolated places without surveillance security such as Closed-circuit television (CCTV) , Video Surveillance and Security officer subsidize to the fraud occurrence at ATM point. Therefore, Automated Teller Machine (ATM) within the premises banks is more secured and, it is noticeable that the location of Automated Teller Machine in attractive environment or location does not support it prone for fraud.

Correspondingly, Diebold (2002) reported that the significant form of Automated Teller Machine(ATM) fraud is personal identification number or information (PIN) theft which is performed through several means; shoulder surfing, skimming, camera, key pad recorder and other related means. This study explicates that the major type of perpetrating fraud during the Automated Teller Machine(ATM) is PIN theft which is commonly happening when there is overcrowding of the users at Automated Teller Machine points.

In the same vein, in the investigations of Bernett (2000), and Oko and Oruh (2012) found that 24 hours' access to the Automated Teller Machine or point of sales (POS) devices is a "double edge sword" it has both disadvantage and advantage.

Therefore, it is easy to construe that automated teller machine (ATM) fraud incidents occurred most in the day time. Also, no dispute, there are some incidences of fraud at night, but most automated teller machine users usually make transactions in the day hence, preventing fraud incidences at night paramount. In addition, Bernett (2000) reported that some banks have no provision for reporting of fraud incidences and there is no enough orientation for the customers on how to operate e-banking devices such as automated teller machine, POS and the similar, neither provision of Fair and Accurate Credits Transactions Act (FACTA) or Automated Teller Machine Manuals for the ATM users.

This also corroborated with Roberds, (1998) discovered from historical lesson learnt where insufficient security measures caused fraud in retail payment systems. This was backed up by example of cloning that led to losses of almost $600 million from the store's value card encryption. Hence there is need for incessant improvement in safety and security to

avert frauds and alleviate the risks suffered by banks, customers and other industries which have resulted to lose of confidence in electronic banking systems (Giles, 2010). Moreover, presently some enhancement development in preventing fraud of electronic banking channels have been experienced. Financial Fraud Action (2011) testified to the actual fraud losses of 10% on credit/debit cards and 24% fraud losses on internet banking lower than the previous years in the UK. This has been accredited to growth and development of electronic banking safety by the use of non-technical and technical approaches. Globally, to protect and safeguard electronic bank accounts and other financial information on their websites, banks spend substantial technology resources in terms of hardware, software, licensing fees, consulting fees and personal hours on providing an infrastructure that will protect electronic banking from fraudsters (FFA UK, 2016).

Moreover, technological factors, universally, the costs of managing e-banking fraud risk and the number of electronic banking fraud incidents are always increasing due to the sophisticated techniques used by electronic banking criminals (CIFAS, 2009). Symantec Security Respons (2005) found that internationally, on average, 116 e-fraud attacks occurred each day in 2012 through social engineering and customized malware, obtaining unauthorized contact with sensitive information, as against 82 attacks per day in 2011.

Likewise, Avinash Ingole and Thool (2013) agreed that, phishing, card skimming, Trojans, spyware and adware, website cloning, cyber stalking, lack of sophisticated antivirus software and weak passwords contribute to the rapid increase of electronic banking fraud. Therefore, the

importance of examination of electronic banking fraud prevention and detection cannot be over emphasized, hence this study.

2.6.2 Non-Technological Factor

Regardless of religion, ethnicity, culture and other factors, there are individuals that are still being motivated to perpetrate electronic frauds. Irrespective of technology, The American Institute of Certified Public Accountants (AICPA), and the Association of Certified Fraud Examination (ACFE), (2015) found that the financial pressure to make means is paramount to some individuals, opportunity and rationalization which are the main reasons why fraud happens. In the authors' research found that, 72 percent seek for personal gain while other 40 percent do not recognise their fraudulent actions as a motive for illegal behaviour.

Usman and Shah (2013) discovered that inadequate staff education, customer education and internal control are other areas which need to be addressed to minimise electronic banking fraud. Grounded on an empirical analysis completed on real world transaction datasets. Dynamic fraud behaviour, fraudsters constantly advance in the techniques to overthrow electronic banking protection. Imbalanced large datasets, huge amount of money and time spend on electronic banking fraudulent transactions per day still, the process of detecting frauds becomes a difficult challenge (Wei, et al 2012). Lastly, diverse behaviour patterns of customers, electronic banking customers perform different transactions in diverse ways for various purposes. This is a challenge as it results to variety of genuine customer transactions that would be imitated by fraudsters who change their behaviour regularly to

contend with advances in fraud detection, thus makes it hard to characterize fraud behaviour from genuine behaviour. BIS, (2012) viewed the cause of electronic banking fraud beyond electronics. The finding of these authors indicates that exploited staffs, lack of training, low compliance level and competition are the major reasons for electronic banking frauds. Therefore, there is need for banks to observe the rising graph of electronic banking frauds seriously and make sure that there is no slackness in internal control mechanism.

In conjunction with the above, Choplin and Stark, (2013) in an investigation conducted, the finding was that, the banking customers are vulnerable to electronic banking frauds both lack of education and demographics have impacts on consumers' vulnerability.

Abou-Robieh, (2005) reaffirmed this, to prevent payment card fraud, consumer education on personal information protection is essential. Zimucha, et al (2012); Masocha, Chiliya and Zindiya, (2011) discovered that the causes of electronic banking frauds are insecurity, limited internet access, cultural barriers and poor legislation. While, Agboola and Salawu (2008) concurred with this, security is paramount issue of the effectiveness of electronic banking services. El-Guindy (2008) asserted that most banks are investing on development of electronic banking, but not on its security. Although Nigeria financial institutions have invested a lot on information technology infrastructures, most banks and e-businesses in Nigerian still lack cognizance of the significant of security in electronic banking. Therefore, there is a need to examine electronic banking frauds prevention and detection in more detail.

Roberds, (1998) ascertained that, opportunities or motives for electronic banking frauds rise in the situations when there is a transaction of enormous amounts, when there is unidentified transacted and, in a situation, when the parts to claim the payment suffer the cost of fraudulent transactions, thus the need for effective electronic fraud prevention and detection. CBN Annual Report, (2010) disclosed that, almost of electronic banking frauds occurred in 2010 are because of an inadequate internal control system. Odediran (2014) believed that, the internal fraud which is often committed by bank staff comprises mailing of wrong financial information, card and PIN code hacking, account records suppression and collusion with external fraudsters as a result of inadequate internal control and management oversight.

While, Sullivan, (2014) argued that, financial institutions bear huge losses yearly through electronic frauds such as card fraud, Automated Teller Machine frauds, misused of private passwords and negligent of the customers to their private transaction data. This signifies that fraudsters are taking advantages of electronic banking system. Then there is a need for substantial strategies for prevention and detection of fraud.

Kinkela and Harris (2014), in other hand, committing of fraud involve team-up of bank staffs with the security agents in both national and international networking. Surprisingly, the outcome of above author's research work revealed that internal staffs that have direct access to the records and personal data of stakeholders and the system of the bank are teaming-up with the fraudsters. Thus, standard procedures of recruitment and adequate training of the staff will contribute enormously in the prevention and detection of electronic banking frauds.

Nkemdilio, Bonaventure and Kingsley, (2013) discovered that perceived job insecurity and inequality had great contribution to employees' fraudulent intent. This is consistent with one of the elements "perceived pressure" in the Fraud Triangle Theory. Therefore, this finding proves beyond technology, it means their other causes that could lead to electronic banking fraud; hence there is need for detection and prevention strategies. In other hands, another critical success factor is organizational learning in the framework of fraud vulnerabilities from the perspective of historical lessons learnt.

Furthermore, Ganesan and Vivekanandan, (2009) warned that the manner of opening an internet account on the internet and transaction security on the internet must be paramount to both internet bank account holders and the bank managements. This also corroborated by Roberds, (1998) discovered from historical lesson learnt where insufficient security measures caused fraud in retail payment systems. This was backed up by example of cloning that led to losses of almost $600 million from the store's value card encryption.

Chartered Institute of Management Accountants (2008) showed lighter to the occurrence of electronic banking fraud that electronic banking frauds occur because of need or greed. The author buttresses the point that 63% of fraud cases cited in 2007 were as a result of greed or people's needs. Other causes are challenges from gambling and debts.

CIMA (2008) opined, Temperament and personality also play a vital role in the occurrence of fraud. Some good people with good aims and agenda or principles can equally find themselves in the bad company and beginning to have a taste for the quick and fast better life, which

lures them to the fraud. Chartered Institute of Management Accountants, (2008) looks at the perspective of pressure or motivation which is one of the elements of Cressey in the Fraud Triangle. KPMG (2006) concluded that, fraud is certain to occur in an organization where there is a feeble internal control system, possibility of detection and slight panic of exposure, uncertain policies regarding satisfactory behaviour.

These authors are in support with the opportunity as an element of fraud triangle theory as also, research has revealed that some workers are completely honest, some are completely dishonest, but there are many that are influenced by opportunity. In corroborate with above, CIMA (2008) and KPMG, (20006) agreed that fraud can still be committed through the concept of reasoning of some people, some people may perceive fraud that is necessary to be committed particularly when done for business, when some perceive fraud that is harmless because the affected organization or victim is big enough to mesmerize the impact and also many people may see perpetrating certain fraud that is justified because the organization or victim deserved it or because those perpetrators have already been mistreated by the company's management or company. From the above, these researchers argued that rationalization as one of the elements of the fraud triangle is also a vital cause of fraud, even without respecting the nature or kind of the fraud either electronic banking fraud or non-electronic banking frauds. Therefore, to commit any fraud, especially, electronic frauds there must be an element of rationalization in the mind of the perpetrators.

Shah, Brayanza and Morabito (2007) believed that, incompetency and lack of knowledge of the customers have caused losses and the failure of some banks and customers.

Therefore, there is a need to teach customers the cause and prevention of electronic banking. Chartered Institute of Marketing (2008) posted that the causes of electronic banking frauds associated with human perspectives which have to do with motivation of

the prospective fraud perpetrators, the conditions of rationalize the prospective fraud, opportunities to perpetrate frauds, perceived appropriateness for the targeted fraud, technical ability and capability of the perpetrators, expected risk of discovery after the fraud has been committed, expectations and actual consequences of discovery.

The AICPA and ACFE (2015), the ineffectiveness of online security results to electronic banking frauds, financial losses as well as a result of inadequate disciplinary measures by regulatory body, lack of customer due diligence which means failure to identify beneficial account owners and company owner and also, other professionals such as accountants, lawyers, police and estate agency fail to play their roles when a fraudster set up unidentified company to hide behind, purchase property, this transaction usually needs the services of these professionals. As electronic banking frauds are influential issues to the word security and desire to be meticulously controlled.

Deloitte (2015) in the study of “India Banking Fraud Survey” observed that there is high frequency of electronic fraud occurrence in the banking industry because of absent of oversight by the top management on movement from the present programme, pressure from business to meet unreasonable target and collusion between the external parties

and internal parties (employees). The above authors concluded that, the most challenging issues of fraud increase, are inadequate customers and staff awareness, unable to integrate data from different sources and lack of research in this field, hence this study to assist in maintaining security and protecting stakeholders from sustaining loss and losing confidence in electronic banking.

Furthermore, the endogenous factors are other factors to consider which also known as the institutional factors, are those factors that can be traced to the internal environment of the banking industry. The endogenous factors are feeble internal control and accounting system, weak customers relation procedure, pay no attention to know your customers rule, ineffective information technology system management, poor management of data base system, poor condition of service and salaries, frustrations from personnel strategies and policies, lack of incentive and promotion, unfulfilled promises by the management, irregular call-over, failure to report fraud incident, insufficient infrastructure, poor generic traits and scanty training, Staff enrolment centred on sentiments, and lack of constant re-training (Ojo, 2008; Adeyemo, 2012;Uchenna and agbo, 2013).

Usman and Shah (2013) stated that frauds in electronic banking services happen as a product of several concessions in security, extending from inadequate internal controls to feeble substantiation systems. Hence there is a need for appraising the factors contributing to the increase in e-banking fraud. Also, the CBN Annual Report of 2010 disclosed that almost all the electronic banking frauds that occurred in that year were the result of inadequate internal control systems.

Equally, Calderon and Green (1994) examined 114 actual incidences of corporate frauds issued by the Internal Auditors between 1986 and 1990. The authors concluded that improper segregation of duties, lack of proper records, and poor internal controls were responsible for almost all fraud incidences. Correspondingly, Jeffords, Marchant and Bridendall (1992) investigated 910 incidences presented by the Internal Auditors between 1981 and 1989 to appraise the exact fraud issues quoted in the Tredway Commission Report. Almost 63% of the 910 incidences were categorized as internal control frauds.

In addition, customers-staff collusion, according to Kinkela and Harris (2014), committing of fraud involves team-up of bank staff with security agents in both national and international networking. Surprisingly, the above authors' research work revealed that internal staff who have direct access to the records and personal data of stakeholders and the systems of the bank are teaming up with fraudsters. Deloitte, in the study "India Banking Fraud Survey" (2015) observed that there is a high frequency of online fraud occurrence in the banking industry because of the lack of staff integrity which gives chance to pressure from business and personal to meet unreasonable targets and collusion between the external parties and internal parties (employees).

Additionally, the study of Usman and Shah (2013) "Internet Banking security" disclosed that 45% of the fraud incidences reported in 2012 included the involvement of managerial and professional staff.

Additionally, ineffective procedure of fraud reporting, AusCERT (2006), in a survey of Australian Computer Crime and Security (ACCS), concluded that the respondents from the organizations that had experience of electronic banking fraud had agreed not to report fraud incidents to

anybody outside of their organization as this would cause damage to the company reputation, did not really know the impacts and capabilities of law enforcement agencies, and believed that if all the frauds were reported the fraudsters would not be caught as a result of lack of regulations and records (AusCERT, 2006).

Besides, negative impressions of bank stakeholders to law enforcement agency, Muscat et al., (2002), this shows that organizations have different negative impressions to law enforcement agencies and this challenge creates a chance for fraud occurrence; there is thus a call for prosecution as a tool for fraud prevention as positioned by fraud management life-cycle theory and as guardianship in routine activity theory.

Correspondingly, individual customers may choose not to report the maltreatment they suffer from fraudsters for certain reasons such as unawareness of the impacts of law enforcement agencies and a feeling of taking responsibility for all loses involved (Yar, 2005).

Similarly, Zimucha et al. (2012) and Masocha, Chiliya and Zindiya (2011) discovered that the causes of electronic banking frauds are insecurity, limited internet access, cultural barriers and poor legislation. The study of El-Guindy (2008) supported the view that most banks are investing in the development of electronic banking, but not in its security. Sullivan (2014) argued that financial institutions suffer huge losses yearly through online frauds such as card fraud, automated teller machine frauds, misuse of private passwords and negligence of customers of their private transaction data. This signifies that fraudsters are taking advantage of the electronic banking system. Thus, there is a need for substantial strategies for prevention and detection of fraud.

Dorminey et al. (2010) stated in line with Donald Cressey, 1953, that the fraud perpetrators use their position of trust to find an illegal solution to a monetary challenge and believe that nobody will see them, or they are unlikely to be caught, this is known as perceived opportunity. Lister (2007) elucidated opportunity as the "fuel that keeps the fire going", which means that however high the degree of motivation, a fraud perpetrator cannot commit fraud without having the opportunity. Taylor (2011) supported this view with examples of opportunities such as poor management of turnover, improper segregation of duties, and ineffective organizational structure. Soltani (2013) consented that position is an opportunity for someone who is a fraudster or trust violator to commit fraud. He also opined that there is a link between power to conceal fraud and opportunity to commit fraud.

Wolfe and Hermanson (2004) described opportunity as a weakness in the internal control of an organization which allows employees to commit fraud. Albrecht, Albrecht and Albrecht (2008) mentioned the lack of audit trail, ineffectiveness of internal controls, weakness of the board of directors, lack of effective anti-fraud disciplinary policy, and other factors as perceived opportunities to commit fraud. Tessier (2013) agreed with the rationalization that almost all trust violators see themselves as honest people who are found in a bad position. This enables them to assess the crime as an acceptable thing to do for them. Authors have explained further that many fraudsters have the idea that what they are doing is illegal or completely wrong at that moment, but they just deceive themselves by thinking that it is illegal. Rae and Subramaniam (2008) also opined that rationalization is an act of

justification of trust violation because of lack of integrity or immoral thought in the lives of employees.

Albrecht, Albrecht and Albrecht (2008) used examples to describe the rationalization by which some organizations' managers or executives violate the rules and standards of financial statements by increasing the stock price arbitrarily or doctoring financial statements to favour their personal interest and still believe that it is for the benefit of the company. Given the nature of the Nigerian economy in relation to fraudulent incidents and lawless attitudes, this theory is most useful for discussing the causes of banking frauds in Nigeria. However, the fraud triangle theory is an inadequate model for detecting e-banking fraud. As is said by critics, the rationalization and pressure cannot be observed; also, it is not technologically oriented and is focused solely on the perpetrator.

Kassem and Higson (2012) argued that the factors of e-banking fraud increase have direct relationships with individual capacity and personality traits. As Soltani (2014) clarified, opportunity gives way to incentive or pressure for fraud, while rationalization leads trust violators to perpetrate fraud; but the fraud perpetrator must have the capacity – good knowledge of the internet and information technology – to identify opportunity and be able to exploit it to commit fraud. Additionally, Dorminey et al. (2012) list the crucial traits that need to be considered for committing fraud, particularly in a large organization: a person's position or function with the combination of ego, intelligence, and ability to handle stress may influence them with the capability to exploit or create an opportunity for fraud. Therefore, potential fraudster who is

the position of authority in the organisation and knowledge the weaknesses of internal controls and able to take advantage of them through his position, authority and function.

Wolfe and Hermanson (2004) concurred that the largest frauds are committed by highly intelligent, creative and experienced people with strong power over the company's controls and management, and with sound knowledge of the company's vulnerability analyses and assessments. Kassem and Higson (2012) conceded that committing fraud and handling the fraud for a lengthy period is stressful. Therefore, a successful e-banking fraudster are the people in the elevated position in the organization who has confident, perfect and effective in dealing with the internet, hacking information, and stress; and be in a position of authority to perpetrate frauds. However exogenous factors are the factors within the external environment of the organization which are job insecurity, family pressure, group pressure, societal expectations, individual financial burden, individual greediness, national economic recession, poor leadership culture, lack of security, inadequate infrastructure amenities and political instability. In the study of Regha (2015) concluded that ignorance of electronic banking and unawareness of tricks of fraudsters, many electronic banking customers have fallen into victims of the fraudsters. CIMA (2008) and KPMG (2006) found that the ineffectiveness of online security results in electronic banking fraud.

Monetary losses occur as well as a result of inadequate disciplinary measures by regulatory bodies; lack of customer due diligence (which means failure to identify beneficial account owners and company owners); and other professionals such as accountants, lawyers, police and estate agencies failing to play their roles when a fraudster sets up an

unidentified company to hide behind to purchase property (such transactions usually need the services of these professionals). Bhasin (2016) argued that frauds commonly occur in the banking industry when procedural and safeguards controls are insufficient, thus allowing the system to become vulnerable to the fraudsters or perpetrators.

2.7 E-Banking Fraud Detection and Prevention Mechanisms

It is universally accepted that banking industries cannot absolutely escape from the menace of fraud (Subramanian, 2014). There are always some people who are motivated to violate the rules or commit fraud, and an available opportunity can make people in an organization perpetrate fraud (MacGibbon, 2005). Therefore, there should be standard, adequate and flexible detection and prevention techniques which will be continuously changing to meet up with diverse changing fraud risks. Therefore, this section discusses the currently available detection and prevention mechanisms. They are discuss as following. First, internal control mechanism, Bhasin (2016) has described, SarbanesOxley dictates that enterprises are strictly devoted to internal controls. However, the most systematic Sarbanes-Oxley compliance strength cannot offer complete security against the occurrence of fraud. Proactive establishments will add extra controls, as well as thorough approval of segregation of duties and procedures.

Second, education, awareness and training mechanism, Bhasin (2016) in a study titled “Combatting Bank Frauds by Integration of Technology” stated that employees must understand the impact of the menace of fraud in the business. The employees need to identify the impact of deceptive behaviour and where and how to document it. Furthermore,

treasury officers need to be properly trained and legally informed on how to use the enterprise's fraud protection technologies and tools. Third, Bank Verification Mechanism, Bhasin (2016), George and Jacob (2015) stated that one of the most significant insecurity problems organizations encounter is fraud committed by dependable insiders and customers. Human resources department and cash control unity must perform background verification on prospective employees and customers, and honest testing is required from the organization itself.

Fourth, Rules and Regulations Mechanism, Wells (2005), in the study "New Approaches to Fraud Deterrence", found that fraud risk management policies and procedures are appropriate and significant for prevention, fraud detection and investigation, and there is a need for reporting policies, resolutions and procedures to be communicated to organizations' employees. The author further suggested regulatory compliance, so as to ensure that suitable procedures and policies relating to company obligations for applicable and ethical conduct are in place, and to familiarize staff with the company's standards and criteria for ethical conduct. Bhasin (2016) stated that many establishments fire the staff that perpetrate fraud but circumvent prosecuting them for fear of spoiling the company's image. A zero-tolerance policy plays a significant role in minimizing the menace of fraudulent incidences. Similarly, company management should instantaneously take evidence or proof of suspected fraud to the law enforcement agencies.

Fifth, technological mechanism, there are various technological mechanisms used to prevent and detect e-banking frauds. Bhasin (2016), in a study titled "Combatting Bank Frauds by Integration of Technology", conducted via a questionnaire-based survey with 345 bank staff in

Malaysia, listed the current tools for detecting e-banking fraud, such as automated analysis tools, data visualization tools, behavioural analysis, deep learning and internal audit functions. Bhasin (2015), in an investigation into the "Menace of Frauds in the Indian Banking Industry", found that the innovative detection and prevention technology employed by some banks, including Data Glyphs, Two-Dimensional Barcodes, Biometrics, Cheque Image Processing, Data Analytics and Data Mining, contributed to addressing the problems of fraud detection and prevention. Therefore, banks need to discover and implement an appropriate sophisticated technique against fraud incidences.

Avinashingole and Thool (2013) posited that banks have different incentives and technologies for preventing and detecting frauds in e-banking services. However, it is mandatory for every banking industry to have adequate rates of incentive and technology to protect customers from the menace of card payment fraud, compromised accounts, and identity doubtful. George and Jacob (2015) presented a risk scoring model as one of the best prevention tools. This model is centred on the current statistical data on card holders, related with the historical data. The outdated method of authenticating via passwords and usernames is not going to be functional and effective in the contemporary system, which needs the support of unconventional technology. Therefore, George and Jacob (2015) concluded that electronic banking fraud prevention and control should be focused on fraud prevention software, smart card authentication, one-time passwords and biometric authentication. The authors further testified that biometric technology provides a better authentication technique and improves security.

In the present day, in the banking sector, several technologies have been adopted to fight fraudulent activities, for example one-time passwords (OTPs). This is an indispensable technique, involving the display of a time-determine code which an e-banking customer needs to insert into the payment or deposit devices of the banking system (Johnson, 2008).

USB Tokens, PINsentry, cards and smart cards are other security instruments used by banks to verify e-banking customers through their custody of any of these security devices. The challenge is that all these current security instruments cause one problem or another. For instance, USB tokens initially need another hardware device and cannot serve its purpose if access is restricted or the available computer has no USB ports (Council FFIE, 2011; Longo & Stapleton, 2002).

Sixth, transaction monitoring is another technique that has been formed for a variation of bank card fraud deterrence approaches. This technique investigates the receiver and sender of a transaction, compared with previous acknowledged fraud incidents. Any resemblance marks will result in the data being declined or transferred to a call centre for physical authentication. This development involves no extra hardware for the customers as all examinations are performed in the setting. However, this approach comes along with certain challenges, as there will be an escape or loophole in the technique when a fresh fraudulent incident arises that has yet to be identified. Moreover, occasionally legitimate transactions may be transferred to call centres, causing inconvenience to the users or customers.

Seventh, two-layered passwords constitute a universal technique of fraud prevention for verifying customers before letting them gain access

to electronic banking systems. For verification to be successfully completed, customers are usually required to have separate internet banking passwords and usernames. Nevertheless, the regular use of a password for different prevention services leads to an increase in the vulnerability of electronic banking customers. Therefore, further methods of security are mainly for identity authentication (Moskovitch et al., 2009). However, Vandommele (2010) concluded that the conventional approach of authentication with password and username is inadequate and unsatisfactory.

Eighth, Biometric Approaches, is considered a progressive means of prevention and detection of fraud, due to the various distinctive characteristics of electronic banking users involved in recognition, verification and discovery. Vandommele (2010) discusses the various features of biometric technique: distinctiveness, universality, intransience, intransigence, performance, circumvention, satisfactoriness and adequacy. Sarma and Singh (2010) also emphasized the resemblance characteristics of biometric technology that should be given great concern in its analysis and evaluation.

Ninth, Keystroke Dynamics is a method of analyzing the user's approach to entering or typing personal information, passwords or accounting data in an e-banking channel by observing the keyboard input data, endeavouring to recognize this data as the usual beat system in the process of typing (Monrose, 2000). The keystroke approach is an innovative technique which was employed by the United States armed forces to differentiate friends from adversaries through Morse code and communication during the Second World War (Bartholomew, 2008).

Over the years, there have been a number of studies on the relevance and reliability of keystroke dynamics through changing input process and algorithm procedures. Patil and Renke (2016) conducted experiments on keystroke dynamic technique via passwords ranging between six and eight characters. Revett et al. (2005) investigated keystrokes using a passphrase of a regular number of 14 digits entered by every e-banking user. The authors calculated a resemblance measurement to form a decision chart and used this to evaluate the rules based on irregular sets. The surveys aimed to discover illegitimate and legitimate logins derived from the key-typing style of the e-banking users. These researchers' findings show (data tests showed 95% accuracy achieved) that the first and last characters, including the typing speed, are the major indicators for determining legitimate and illegitimate logins (Revett, Magalhaes & Santos, 2005).

In addition, research conducted on conciliation between the standard password and lengthy text input using passphrases techniques showed a 0.5% false acceptance rate and a 3.1% false rejection rate (Boechat et al., 2006). The algorithm in this investigation merely involved keystroke latency. However, Gunathilake et al. (2013) state that compared with other present techniques, keystroke dynamics are a highly efficient and prolific approach to validating internet schemes. The keystroke dynamic system is gainful for software, since it improves electronic system access protection; consequently, this makes it also appropriate for reinforcement of the internal security of banks and particularly of electronic banking systems (Revett et al., 2005).

Correspondingly, some scholars have argued that among the various biometric systems, the keystroke dynamic network is the best and most

appropriate method due to its costeffective implementation and performance: it requires only software, and a keyboard and gives reasonable and adequate results over and above the higher rate of transparency it offers (Choras and Mroczkowski 2007). Revett (2009) opined that some banks have implemented keystroke dynamics as a main authentication tool while others have used keystroke dynamics software as a supplementary authentication method. Anthenware technology is a type of online security system protection software which works by understanding and learning the distinction between keystroke behaviours (Bergadano, Gunetti & Picardi, 2002). For instance, Ecuador Bank installed Authenware software to measure keystroke patterns and internet behaviour.

Tenth, bio-password is a type of security keystroke biometric software that operates through a neural algorithm for examination of data and the provision of Crossover Error Rate (COER) to the users. If it provides 3% COER, this means the software has the capacity to register users instantaneously, steadily and noiselessly. Additionally, Shanmugapriya and Padmavathy (2009) investigated the intrusion of the waiting time between pressing an input key and obtaining a result differentiating legitimate e-banking users in order to differentiate the legitimate e-banking users from illegitimate users through the use of a multilayer neural network approach. The neural network approach is a forecast model using historical events to envisage the result of a future event. The outcome proved that adopting neural network for differentiation resulted in a better outcome than any other statistical techniques.

Eleventh, Bhattacharyya et al. (2009) concluded that biometric authentication enhances the components of identification, non-

repudiation and authentication in security information. Consequently, this technology has a fundamental role to play in e-banking fraud reduction. Biometric systems provide a way forward by considering individuals' distinctive features as a means of identification. Even though recent development and improvement of biometric technologies, which include fingerprints, keystroke dynamics and iris recognition, appear promising, Murdoch and Anderson (2010) pointed out that authentication techniques for e-banking fraud prevention must be economically viable and technologically reliable. Many researchers, though, have proved the suitability and accuracy of biometric authentication for prevention of electronic banking fraud. Also, some organizations have implemented behavioural biometrics to enhance their security.

Twelfth, bank verification number (BVN) is a mechanism used to reduce the potential harm of fraud, every business organization, particularly the banking industry, must invest not only in advanced technology but also in policies and people for detecting and preventing attacks as promptly as possible. This has led the Nigerian Central Bank to introduce another policing method: The Bank Verification Number (BVN). Globally, biometric technology has been adopted to analyse human characteristics as an improved form of verification, authentication and certification for real-time security methods (Blass & Oved, 2003). In the face of cumulative occurrences of compromising, of orthodox security systems (PIN and password), the need for sophisticated security for access to personal and sensitive information in the banking industry has become inevitable.

Therefore, on 14 February 2014, the Central Bank of Nigeria, through the Bankers' Committee and in cooperation with all Nigerian Deposit Money Banks (DMB) and the Nigeria Inter-Bank Settlement System (NIBSS)), introduced a centralized biometric identification system for the banking sector, called the Bank Verification Number (BVN) (CBN, 2014). However, the aim of this project (BVN) is to protect bank customers from identity theft and other financial frauds emanating in the Nigerian banking industry (Orji, 2014). The current research will analyse the present mode of operation in the Nigerian banking industry, assessing the impact of the BVN since the date of introduction into the Nigerian electronic banking system.

Finally, ASSOCHAM (2015) in the investigation carried out on "Current fraud trends in the financial sector" found that the adoption of the following methods would enhance the rate of electronic bank fraud detection in the financial institutions. The methods of fraud risk management were adopted which are, whistle-blowing and tip-offs, suspicions transaction reporting, internal audit, data analytics, by accident, by law enforcement, corporate security (physical and IT), investigative media and rotation of personnel. The author further explained that, fraud detective oversight must be in place such as, surveillance and monitoring systems (escalation and investigation, data management, program and controls testing), analyzing identified red flags, regulatory and internal reporting, internal audit, independent review and investigations. While, Deloitte, (2015) opined that to accomplish effective detection of electronic fraud, there must be included of tool for electronic detection, forensic imaging, data anomaly discovery and information management tool which also supports banks

and legal counsel for analyses and control complex information on the fraud cases.

2.8 Summary

This chapter has elucidated the most pertinent and suitable secondary information recognized by the researcher in the literature on the aspects of e-banking fraud prevention and detection which also included contextualising of the Nigerian banking sector which comprises its history, evolution and structure of the Nigerian banking system and historical background of e-banking services in Nigeria such as internet banking, mobile banking, telephone banking, ATM and other channels of banking and e-payment. However, under the current guideline, licensed banks were approved to perform banking activities of their licensed category which grouped into three categories in relation to their activities, namely: Commercial Banking (Deposit Money Banks) License, Merchant Banking License and Specialized/Development Banking License. The chapter has also elucidated the impacts of e-banking fraud which are monetary and non-monetary impacts. While, personal data, educational information, health information, credential information, payment card data, financial information, others and unknown through hacking or malware, insider leaks, payment cards, fraud loss or theft and unintended disclosures are major information types targeted by e-fraudsters to defraud an individual or an organization.

In addition, the factors contribute to the increase of e-banking fraud were classified into technological factors and non-technological factors. And the prevention and detection mechanism were categorized into

internal control, education, awareness, training, verification, rules and regulations, technological techniques, transaction monitoring strategy, two-layer password, application of biometric approach and keystroke,

CHAPTER THREE: THEORETICAL FRAMEWORK

3.0 Research Methodology

This chapter covers the research design, source of data, population of the study, sample size and sampling technique, model specification, theoretical framework (Routine Activity Theory and Fraud Life-cycle Management Theory), measurement of variables and data analysis technique.

3.1 Research Design

Primary Source of Data gathering through Questionnaire to be filled by respondents and Ex-post facto research design will be used in the course

of this research. The basis for this choice of design is because the study intends to use data that are in existence (Secondary data) already and there will be no effort to control or manipulate these existing data, while the Primary Data is a deliberate attempt used to review and evaluate the current assertions on the incidence of Electronic and Banking Fraud that the "Motivated Offenders" are advancing as the basis for their various heinous criminal activities. The works of some authors on incidence of frauds in the banking and other sectors will be used as the source of data on which ex-post facto design will be applied.

3.2 Sources of Data

The study will rely on both primary and secondary data. A thorough investigation of the previous literature was carried out using sources extracted from various academic databases. Ex-post facto design analysis based on an integrative literature review methodology was conducted to synthesize various research contributions and analyzed relevant information related to causes of fraud and the efforts put in place by the managers of people's investments and fund deposits, While the questionnaire are distributed to people working in the Banking and Financial Sector of the Economy.

3.3 Population

As stated in chapter 2, the Nigerian banking industry made-up of 28 banks, which comprised of 22 deposit money banks (DMBs) that was previously known as commercial banks, 5 merchant banks and 1 non-interest-bearing bank (CBN, 2018). However, the Nigerian deposit

money banks, is comprised of 22 banks of 3978 branches all over Nigeria. Hold 78% of the capital reserves, total net assets and also, share over 83% of total profitability in the banking sector, while the remaining 22% of the capital reserve and total net asset, including 17% of the total profitability in the banking sector are shared by the other 6 banks (5 merchant banks and 1 non-interest-bearing bank) (Bank Supervision Report, 2016).

Therefore, the population for this study is mainly entire staff and customers of Deposit Money Banks (MDBs) in Nigeria, which formerly referred to as Nigerian Commercial Banks (NCBs). The choice of the Deposit Money bank based on its highest number of banks (22 banks) and its highest number of branches (3978 branches) all over Nigeria and hold 78% of the total capital that are available in Nigeria. Though, Omotayo, and Kulatunga (2015) observed that, in most case, interviewing the entire population is very difficult, due to inadequate time, limited accessibility, lack of enough funds and other inconveniences. Thus, in this situation, for economic reasons, it will be very easy to interview a subgroup of the population, which means a "sample".

To get appropriate general conclusions the right or appropriate sample must be selected, hence the sample for this study was selected from 22 deposit money banks which consist of 3979 branches all over Nigeria. It included staff from senior level to the managerial level and customers that have been the victims of electronic banking system within the bank premises. Sampling enables accessing of every subject of the sample and using the result of the sample collected to make a general conclusion on the intended population.

Figure 4.2: Population, Elements, Sample and Subject

The population for this research is made up of these categories: directors, managers, accounting practitioners and senior staff in internet commerce departments, information technology departments and risk management departments that are working in the head offices of Nigerian deposit money banks. It also included bank customers within the bank premises; customers within the bank premises being considered as victims of e-banking frauds. The categories of the population considered were found to be appropriate because of their heavy participation and involvement in internet banking and online commerce.

The participants from the departments were chosen based on their knowledge and level of experience in the subject matter, which would enhance the reliability of the responses for the research instrument based on the research hypotheses.

3.4 Sampling Techniques

Each time a fraud incident occurs, there is a victim and a perpetrator. It would have been better to gather opinions and views from fraud perpetrators to get a better picture of their motivations for committing frauds. However, looking for fraudsters to interview or to administer questionnaires to, would have been a complicated issue. The fraudsters would undoubtedly be less likely to give straightforward and truthful information on their motivations and activities.

Therefore, collection of the information about e-banking fraud prevention and detection in banking industry required people that are well-informed, educated and conversant with e-banking fraud incidences in the banking sector. In the same vein, Paler-Calmorin (2007) opined that the use of a mechanism for fraud detection and prevention is decided at the directorial, structural or administrative level of the organization. Also, Krambia-Kapardis (2002) argued that when investigating corporate losses from fraud, it is important to choose suitable participants in the institution to be investigated; failing to do this may result in a low response rate. The selection of whom to speak with, when, where, about what, and why, places limitations on the conclusions drawn and the degree of confidence others can have about the outcome (Miles & Hubermann, 1994).

Concisely, with the above reasons and the nature of e-banking fraud prevention and detection, purposive sampling, which also known as a judgement sampling technique was employed for selection of both respondents of quantitative research and participants in qualitative research. Hence this study sampled accounting practitioners, professional bankers, directors and managers, because this research is actually focused on the decisionmaking process, which is the major managerial responsibility of the chief financial officers, chief accountants, directors and managers; including the heads of internet banking, heads of fraud investigation, heads of information systems and technology, heads of operational risk management, heads of internal audit units, heads of security personnel, heads of forensic audit, heads of financial crime team members, and others.

These staff are in the best position to provide the needed information. Also, customers from the banking premises where selected for the second face of the questionnaire. The selection of the customers was based on those who had previously been the victims of fraud. This would certainly contribute to enhance the reliability of the data obtained.

3.5 Sampling and Sample Size

Works on the sampling method state that a specific sample frame is important for random sampling. According to Tran and Perry (2003), non-probability sampling is employed in research when it is the only feasible and viable option to adopt in the aspect of restrictions in selecting probability sampling; therefore, the choice of non-probability sampling requires solid assumptions on the nature and proportion of the sample for its validity. For both the qualitative research and quantitative research questions used to examine electronic banking fraud detection and prevention in Nigerian banks, 10 deposit money banks (MDB) in Lagos and Abuja out of 22 deposit money banks in Nigeria (CBN, 2017) were selected as a unit of the population, using a purposive sampling technique. Directed by the above arguments, only ten deposit money banks in Nigeria (given anonymous titles: Bank A, Bank B, Bank C, Bank D, Bank E, Bank F, Bank G, Bank H, Bank I and Bank J) were chosen as the representative sample from the sample frame.

Firstly, the rationale for selecting ten deposit money banks in Nigeria from the 22 banks with 3979 branches (CBN, 2017) that were available in the Nigerian banking sector was that, the selected 10 deposit money banks in Lagos State and Abuja Federal Capital Territory (FCT) had 2902 branches which made- up 73% of all bank branches over the 36 states of

Nigeria, while the other deposit money banks had only 1077 branches, making up 27% of the total (CBN, 2017). The selected banks were appropriate because of their heavy participation and involvement in electronic banking and commerce.

Secondly, the choice of Lagos as the main place of this study was to do with the number of head offices of deposit money banks in Lagos. Out of 22 banks in Nigeria, 21 head offices were in Lagos while the remaining one located in Abuja. Thus, the choice of these banks based on the number of the branches owned by each of the banks, geographical location and their proximity to one another were also considered. Ten banks that have the highest number of branches all over the country were selected (CBN, 2017). Precisely, the head offices of 9 banks were selected while only 1 bank in Abuja which is the second bank with the highest branches in Nigeria also selected. Therefore, the selected banks are the banks that have the greatest numbers of branch offices and staff across the country; this gave opportunities to capture the needed information on the subject matter from every nook and cranny of the country.

Information generated through qualitative and quantitative research was adopted for this study. This study employs the idea posited by Creswell et al. (2003) on the method for chronological exploratory strategy; that is, the quantitative and qualitative approach (QUAN QUAL approach), as this method gives opportunity to collect data through faceto-face qualitative interviews after the responses have been collected from the quantitative survey. The qualitative interviews were adopted to investigate further the results obtained from the questionnaire data. This supported interview carried out with ten

selected top managers from the selected Nigerian deposit money banks through a purposive sampling technique, with at least one head for each of the following departments: Application and Database Security Management, Frauds and Risks Management, and Fraud Control and Monitoring Management. The participants who had answered the questionnaire were excluded from participating in the interviews to escape positive bias. The main reasons for the use of qualitative interviews were to enhance the understanding and to elucidate the quantitative results.

Moreover, for the quantitative research, representative samples were sourced from two groups with two different classes of questionnaires. The first group comprised the representative of banks' staff as experts in banking business. A sample size of 383 was initially determined out of estimated 113,200 bank staff in Nigeria. While, the second group comprised the representative of banks' customers as victims of e-banking fraud with a sample size of 384 out of the estimated 22 million bank customers in Nigeria was also originally determined with the use of an online electronic sample calculator for a 5% confidence interval and 95% confidence. However, there are two classifications of sample size generally recommended in factor analysis (EFA and CFA). The first group agreed that the complete number of samples (N) is significant, while the second agreed that the subject-to-variable ratio (p) is imperative (Velicer, Eaton & Fava 2000; Velicer & Fava, 1998; Arrindell & van der Ende, 1985, and MacCallum, et al., 1997). A minimum sample of 100 is appropriate, that it is, the sample size should not less than 100 samples for factor analysis, even though the variable size is not up to 20 (Gorsuch, 1974; Psylch & Hatvher 2013; Arrindell & Van der Ende, 1985). , Hatcher (1994)

and David Garson, 2008) also suggested 100 samples as minimum sample size for a factor analysis while, Hutcheson and Sofroniou (1999) acclaimed at least 100 – 200 samples as a moderate sample size.

In addition, many scholars have used a ratio 10:1 of subjects-to-variables in their studies (Orakci & Toraman, 2018; David Garson, 2008; Nunnally, 1978, Marascuilor & Levin, 1983). A ratio between 3:1 and 6:1 of subjects-to-variables is acceptable if the minimum variables-to-factors ratio 3 to 1. But, the absolute lowest sample size must not be less 100 samples for EFA and CFA (Kline, 2004; Comry & Lee, 2013; Fabriger et al., 1999). Ferguson & Cox (1993), and Marsh and Hocev (1985) opined that sample size use in any large study must, not less than 100 samples. Therefore, having considered the types of analyses employed (EFA and CFA), the level of accuracy and precision required, population heterogeneity and homogeneity, sampling technique employed (purposive sampling technique) and availability of resources and targeted respondents (bank staff at management level and e-bank fraud victims among the customers within the bank premises). The researcher decided to limit the sample size of the study to 200 samples for each group of staff respondents and customer respondents which their ratios of subjectto-variables range between 5:1 and 10:1.

Hence, the sampling method was to survey all potential respondents and to get their permission for the research's engagement. As it turned out, 169 of the 200 determined questionnaires were returned for the quantitative research on the banks' staff, while 165 out of the determined 200 questionnaires were returned for the quantitative study of the bank's customers. Also, all ten top managers contacted face to face with semi-structured interviews agreed to participate and gave

their useful responses. The response rate that would be confirmed as suitable and appropriate representation was anticipated to be between 40% and 50% (Blumberg, Cooper & Schindler, 2005). The qualitative survey gained a 100% response rate, while the quantitative study of the banks' staff achieved an 85% response rate and the survey of the banks' customers gained 78% response rate.

Consequently, a high and appropriate response rate was accomplished through selfadministration of a simple questionnaire, adequate follow-up, short length of interviews, advance notification of respondents and positive interest of the participants in the research.

3.5 Model Specification

3.6 Theorectical Framework

This section deliberates on the related studies to the phenomenon with the associated theories adopted so as to show light to the appropriate theories employed in this study.

While, concluded with the discussion of routine activity theory (RAT) and fraud management lifecycle theory (FMLT) as the theoretical framework underpinning of this study.

3.6.1 Related Studies of E-banking Fraud Prevention and Detection

There are a small number of studies on fraud prevention and detection in electronic banking (Phua, Smith & Gayler, 2012; Dzomira, 2015). Most of them are fraud prevention, such as (Robert et al, 2009; Roberds 1998;

Vandommele 2010; Bhattacharyya 2009; Murdoch & Anderson, 2010; Tan, 2003) which adopted efficient and effective security control to prevent counterfeit transactions perpetrated by fraudsters and to enhance integrity and honesty transactions. Alimolaei, 2015; Peotta et al. (2011); Kovach and Ruggiero, 2011; Bignell, 2006; Dandash, et al. (2008); Edge et al. (2007); Hertzum, Jrgensen, and Nrgaard (2004,); Leung, Yan and Fong, (2005); Aggelis (2006); Wei et al. (2013) and Edge et al. (2007) investigated on detection of internet banking fraud based on critical success factors and online banking security measure. Furthermore, related studies on eletronic banking fraud prevention and detection, a number of research studies on only credit card fraud prevention and detection have been conducted (Alfuraih, Sui & McLeod 2002; Dheepa & Dhanapal, 2009; Mahdi, Rezaul & Rahman, 2010). A lot of the studies on the detection and prevention of credit card fraud have been done by using Neural Networks, Rule-Based Association System, Neuro-Adaptive Approach, HMM, BLAST-SSAHA Hybridization and other statistical modelling (Kou, et al. 2004; Leung, Yan & Fong, 2004; Srivastava, et al. 2008, Neill & Moore, 2004). However, almost methods and theoretical frameworks of prevention and detection of credit card frauds used to identify spending forms which based on the only historical transactions are not suitable for the active banking industry as a result of various e-banking customers' transactions and the incomplete previous data obtainable from individual customers.

Notwithstanding, Chiezy and Onu (2013) appraised the effects of fraudulent activities on the growth and development of banks through data from 24 Nigerian commercial banks, between 2001 and 2011 (secondary source of data). The association between fraud incidents and

other variables were appraised using multiple regression analysis and Pearson product moment correlation.

Moreover, some scholars based their studies on computer intrusion detection and prevention. For instance, these studies mainly examined the prevention and detection of anomaly and misuse of computer systems within the organization by monitoring program behaviour, multiple classifier model and Neutral networks model (Beghdad, 2008; Ghosh et al, 2007; Eskin & Stolfo, 2007; Teoh det al. 2004; Giacinto, Roli & Didaci,2003). Therefore, since forensic financial investigators declared that detection and prevention of computer fraud is all about the users of computer systems, prevention and detection techniques of intrusion which are the attributes of electronic banking activities. Thus, the theoretical framework used could be applied to the e-banking fraud prevention and detection.

In addition, Mhamane and Lobo (2012) study investigated prevention and detection of online banking fraud with the adoption Hidden Markov Model (HMM) algorithm and Fraud Management Lifecycle Theory while, Wada and Odulaja (2012), Bossler and Holt (2009), Reyns, (2013), Wilhelm, (2004) and Leukfeldt, (2014) conducted qualitative studies on cybercrimes and internet banking fraud with the use of routine activity theory (RAT) and fraud management lifecycle theory (FMLT). The finding holds that the combination of the absence of a capable guardian with a suitable target and a motivated offender in a convergence of space and time has an influence on the victimization of malware and phishing. Precisely, Wilhelm (2004), Jamieson, Stephens and Winchester, (2007) Newton; Nenga and Osiemo, (2013) investigated for fraud management and control with the use of fraud management lifecycle and their

findings exposed that the proper interrelationship of distinct groups and components of these stages would result to successfully control and perfect management of fraud in the organizations. Hence, the theoretical framework of Fraud Management Lifecycle Theory was considered also useful and appropriate for this study.

Likewise, Jansen and Leukfeldt (2016) researched on "phishing and malware Attacks on online banking customers in the Netherlands", the qualitative analysis of the factors of victimization with data collected from 30 victims of malware and phishing in their bank accounts through semi-structured interview and using routing activity theory as a theoretical framework. The finding showed that victimizations of malware and phishing attacks were marginally influenced by suitable targets. In the same vein, Hutchings and Hayes (2009) investigated quantitative research on "routine activity theory and phishing victimisation". The study investigated 104 victims of deceptive email through the interview. The findings revealed that probable victims who perform routine activities through online banking and other computer activities are more vulnerable to be defrauded by motivated offenders. In a nutshell, the theory of routine activities has been extensively used in the extant literatures, among other things, robbery (Tseloni, et al. 2004), sexual crimes (Tewksbury and Mustaine, 2001), cybercrime and online frauds (Newman & Clarke, 2003; Eck & Clarke, 2003; Wilsem, 2013; Holt & Bossler, 2008; Bossler et al., 2012; Pratt, Haltfreter & Reising, 2010, Williams et al, 2013; Reyns & Henson 2013). Likewise, Yar, (2005); Delvema, (2015) Choo, (2011); Willson and Fulmar (2014) and Bossler and Holt, 2003 discussed the cybercrime with application of mixed method and routine activities theory.

Therefore, the theoretical framework of routine activity theory was also considered suitable and appropriate for this study.

Furthermore, the routine activity approach has been used by several studies of cybercrime (Ngo and Paternoster, 2011; Duffield & Grabosky, 2001; Hutchings & Hayes, 2009; Reyns, Henson & Fisher, 2011; Van Wilsem, 2011). Therefore, the theory applies to this phenomenon. On the other hand, Pratt, Holtfreter and Reisig (2010) view through the suggestion of routine activity theory that those involved in e-banking is more likely to be victims of fraud. Karmen, (2010) opined that the victim of e-banking fraud is naturally involved in a lawful transaction and legitimate online business at the time of attack and oppression. Because of this, merely engaging in transacting business or transferring money (e-payment or e-commerce) from e-banking websites provide a high-fraud motive, compared to individuals or entities that do not transact business or pay money via e-banking.

However, out of the various channels of electronic banking, only online banking through phishing and malware and card payment fraud prevention has ever received concerns of the researchers, therefore, there is a need for examination of e-banking fraud prevention and detection with the use of routine activity theory (ROT) and fraud management lifecycle theory (FMLT). Hence, this study.

3.6.2 Theoretical Framework of the Study

Over the past three decades, many theories have been developed to elucidate the nature of fraud. The two principal theories of criminology and management were adopted as theoretical frameworks that

underpins this study, which are the routine activity theory (RAT) and fraud management lifecycle theory (FMLT).

3.6.2.1 Routine Activity Theory (RAT)

A routine activity theory is a significant theory of environmental criminology and a placebased clarification of fraud theory, where the behavioural forms and the interrelationship of people in the place and in time influence where and when fraud occurs. This theory assert axiomatically that when suitable targets and motivated offenders meet without capable guardians, fraud will probably materialize (Miller, 2013). In an equal manner, the absence of any of these listed three circumstances might be sufficient enough to prevent a fraud from Occurring. Positioned within the comprehensive context of environmental criminology, routine activity theory proposes that reducing opportunities for fraudulent activities plays a significant role in minimizing the pervasiveness of fraud (Williams, 2016). However, routine activity theory is, in a nutshell, an effort to identify fraudulent activities and their methods through clarification of vicissitudes in movements in the fraud rate (Cohen & Felson, 1979). It therefore offers a setting of orientation for material and modified fraud analysis and simplifies the application and implementation of actual practices and policies aimed at changing the essential elements that make the presence of fraud probable, thus averting it (Tilley, 2009)

Figure 3.1 Routine Activity Model - The Physical Convergence In Space and Time

The routine activity approach was introduced in the United States by Cohen and Felson (1979). This approach has proved its helpfulness in accounting and banking for a variation of fraudulent activities (Bradford, 2013). The routine activity theory was developed to examine the vicissitudes in the crime rate after World War II (Kennedy & Forde, 1990; Cohen & Felson, 1979). From the societal perspective, routine activity theory specifies that variations in combined routine activities can generate opportunities for fraud.

Furthermore, from the individual perspective, empirical researchers have emphasized the position of the individual or entity's routine activities in generating fraud opportunities (Fisher, Daigle & Cullen 2010). However, the routine activity theory proves that there is an opportunity for the occurrence of fraudulent activities in a place and time when the motivated offenders come together and there is availability of suitable targets with absence of capable guardianship. The proposal of a routine activity theory (proximity and acquaintance to target attractiveness, motivated offender, with absence of capable guardianship) has become the main elucidation of what brings individuals to fraud or being defrauded. Moreover, the continued acceptance of the theory in clarifying direct-contact fraud incidence has prompted researchers to adopt the theory to describe opportunities for fraud taking place at a distance (Holtfreter, et al., 2010; Marcum, Higgins & Ricketts, 2010).

The theories have mainly concentrated on fraudsters that meet their targets in a place (Tillyer & Eck, 2009). However, some frauds do not require direct and physical contact at a place. This has encouraged philosophers to determine whether the routine activities approach is restricted to place-based fraud (Tillyer & Eck, 2009). In addition, the struggle of the first researchers to adapt the routine activity approach to frauds in which fraudsters and their victims do not meet in the same space and time have generated assorted, but inspiring results (Marcum, Higgins & Ricketts 2010; Holt & Bossler, 2009). These studies have concentrated on e-banking fraud, such as computer virus contagion and phishing harassment, and suggest that more studies are required for categorizing cyber routine activities that possibly place cyber operators at higher risks of diverse cyber fraud and adapting the theories to describe distance-based fraud. The current research work discussed both phenomena through appraising e-banking fraud, prevention and detection from a routine activities perspective.

Correspondingly, in the context of e-banking fraud, routine activity theory (RAT) is an environmental theory, a time-and-place-based elucidation of crime, where connection of individuals and behavioural patterns of a place and time influence where and when frauds occur (Williams, 2016). The routine activity theory suggests that there is likelihood of fraud when there is the absence of a capable guardian and the availability of attractive targets and motivated offenders (Marcum, Higgins & Ricketts, 2010). Conversely, the absence of one of these elements might be able to stop e-fraud from occurring. Therefore, this theory is adopted by this study.

In this case, routine activity measures a diversity of hypothetical fraud environments, such as places and time spent on the internet. The following twelve routine activities are related to online identity fraud, which is classified into activities and locations of internet access that measure a variety of cyber activities and location access. The first group is cyber activities such as purchasing, banking, auction, selling, email and social networking. The second group is location of internet access, which includes bank, home, public, university, mobile, café and work; some locations are more dangerous than others, such as computers in public places and cafes that have many users, which can increase virus infection (Wilcox, Madensen & Tillyer, 2007). However, if these approaches of internet activities remain unguarded, this will probably uncover attractive internet targets to motivate electronic fraudsters. The routine activity theory describes fraudulent activities through three important bases that meet in time and space in the sequence of daily events: (a) Capable guardian; (b) Suitable target; (c) Motivated offender.

3.6.2.1.1 Capable Guardian

Cohen, Lawrence E.; Kluegel, James R.; Land, Kenneth C. (1981), explained in this theory that the absence of a capable guardian; that is, of someone or something that can intercede to prevent a fraud from happening. The presence of a capable guardian will not permit the possible fraud to be committed, while the absence of a capable guardian will give room for the fraud to be committed. A capable guardian includes anyone within an environment or working as a guard of property or persons, such as security guards and police. They are

honestly capable guardians and are usually absent when frauds are happening (Felson & Rachel, 2010). However, a literature review of the capable guardian of routine activity theory has described guardianship as the symbolic or physical presence of a person or group of persons that acts either unintentionally or intentionally to prevent a potential fraudulent activity (Hollis-Peel, et al., 2011). For instance, closed-circuit television (CCTV), which is placed by people, but is a presence at the place of fraud that is not physically seen (Hollis-Peel et al., 2011). Felson (1995), in an effort to relate routine activity theory to Hirschi's social control theory (1969), polishes the image of the guardian by differentiating the place manager from the intimate handler. The place manager guardian is recognized as those individuals or persons who have guided and controlling responsibilities at a certain place; for instance, bus drivers, doormen, and the like.

The intimate handler may be a parent or family member who attempts, through condemnation and disagreement with the motivated offender's behaviour, to deter the actions that disrupt the rules. Thus, in extending at the notion of the capable guardian, Felson (1995) considered the four factors of Hirschi's theory which commitment, attachment, belief, and involvement. The author abridges these factors into one: "handler". Furthermore, analyzing the idea that somebody could deter an offender through his/her presence in a place, or that a person could discourage a probable offender due to his relationship with him (Cohen & Felson, 1979), shows that control is an essential element in the fraud rate, and also that success of a place manager is based on the degree of relationship and responsibility he/she has with the possible offender.

Consequently, in the context of e-banking fraud, capable guardianship can be reflexive physical guardianship: operating only one electronic system, using antivirus and email spam filtering, safekeeping of credit/debit cards, token card, PIN sentry and secured browsing. It can be active personal guardianship through the changing of passwords, security settings, memorable words, PIN codes and secret questions (Wilcox et al., 2007). Moreover, it can also be avoided personal guardianship: reducing time spent on the internet such as during online purchasing and online banking and logging out of email and electronic banking on time when finishing. If these online activities are well guarded, motivated electronic fraudsters may be deterred from suitable online targets to perpetrate electronic banking frauds. Capable guardians include law enforcement, the owner of the property (the account holder), banks and other financial institutions, Computer Emergency Response Teams (CERTs) or any other agency or individual that is capable of discouraging the offenders (Yar, 2005). It may also be social-informal guardians such as systems security staff; inhouse network administrators; and technological or physical guardians such as intrusion detection systems, virus scanning software, and firewalls (Denning, 2000).

As e-banking is often faced with attacks related more to characteristics of human nature than technical activities, a proficient guardian can be fashioned by feeding the customers with awareness and information rather than safety software. In addition, the Australian Crime and Security investigation posited that awareness may be missing. It was concluded in 2006 that even though 98% of responding companies considered antivirus and firewall software, only 15% of respondents

agreed that they had got satisfactory training and skill through security and protection awareness (AusCERT, 2006).

In the same vein, the highest influence on e-banking fraud attacks was attributed to lack of qualitative staff education and adequate training in protection and security procedures and practices (AusCERT, 2006). Growing the public and collective awareness of possible fraud victimisation improves their capacity to become capable guardians. Grabosky and Smith (2001) stated the significant principle for preventing electronic fraud is the demand for the necessity of awareness of the potential victims to the menaces of fraud. Smith and Akman (2008) appraised the 2007 campaign conducted by the Australasian Consumer Fraud Taskforce (ACFT), which was organized by 19 government departments and agencies for customer protection against fraud and related incidences and found that it was exceedingly effective in floating customer awareness. The campaign involved the circulation of flyers and posters, radio advertisements, media releases and television appearances, and included articles in magazines and newspapers (Smith & Akman, 2008).

Therefore, the researchers also suggested that website cautions on internet browsing and banking websites, email filters, hints for identification of authentic and legitimate websites, and provision of procedures for suspected online fraud or hoax email reporting on banking websites will serve as capable guardians. However, it seems as if the banking sector is not happy to be responsible for the role of capable guardian. Correspondingly, the Parliamentary Joint Committee on the Australian Crime Commission's (2004) investigation of cybercrime observed that a suggestion by the Association of Australian Bankers

emphasized the customers' responsibility for personal-protection or self-safety from fraud rather than the banking industry's responsibility for protection and security of their customers. Therefore, while financial institutions will habitually recompense sufferers for their monetary losses, they are unwilling to take the issue any further. Lynch (2005) contended that there is no monetary incentive for the banking industry to prevent electronic fraud.

Nevertheless, recently there have been improvements in banking industries through using two-factor and three-factor identifications, whereby customers are required to use multiple techniques, such as a digital token and password (Smith, 2007). Reyns (2013), Wilsem (2013) and ENISA (2012) have tested the application of the routine activity approach and the policy hypothesis of the adoption of passive physical guardianship and active personal guardianship in online crime and cyber victimization. Their findings show that the application of the routine activity approach reduces cybercrime and online identity theft.

3.6.2.1.2 Motivated Offender

This describes someone whose motive is to perpetrate fraud and who is capable of doing so (Cohen & Felson, 1979). It is possibly a young man or woman as crime has no gender preferences, deprived of steady employment, a school dropout, as well as intelligent, canny and clever (Gottfredson & Hirschi, 1990). Even though in the original formulation of this theory by Cohen and Felson (1979) the term **"motivated offender"** was used, in later studies such as Felson & Rachel, 2010. The authors have avoided using the term **"motivated"** to describe the offender: what they considered relevant was not the motivation or the temperament to

perpetrate a fraud, but rather the physical influences which made it probable for a potential fraudster or someone to be involved in perpetrating fraud.

Thus, what this tactic underwrote was an enunciation required to distract attention from the perpetrators in order to recognize and understand the fraud (Felson, 1995), nevertheless, though it is essential to take note of other characteristics of fraud in order to prevent and understand it (Felson & Clarke, 1998), this does not mean forgetting the standpoint of the fraudster (Felson, 2008); the very explanation of the suitable target is through the acknowledge and understanding of the importance and capacities of the fraudster in relation to essential characteristics of the possible targets of fraud.

The sources of this perception can be discovered in the study of Cornish and Clarke (1986), which intersects with the approach of Felson (1995) in beginning from a point of rational decision and in laying emphasis on fraud prevention and elucidation of the environment in which the fraudster performs. The rational choice proposition is when fraudsters make decisions after they have assessed the availability of opportunities of perpetrating fraud successfully, the anticipated benefit attached to it and the danger of being caught. The motivated offender may be temperamentally inclined to perpetrate fraud; that is, the person evaluates the diverse options available to accomplish targeted objectives, whether lawful or unlawful, and eventually chooses to start committing frauds.

The motivated offender can be influenced by circumstances or conditional factors. Nevertheless, the Cohen and Felson approach has been dependable and constant with the impression of a rational

offender who takes the benefit of opportunities. At this point, the issue of opportunity has a significant role from the perspective of routine activities.

In fact, deviations in society's routine activities, the ineffectiveness and unreadiness of guardians, or the increase in obtainability of suitable targets may strengthen the probability of fraud if these elements meet in space and time and consequently create opportunities. In addition, another most significant and commanding concept in routine activity theory is indeed that opportunity is wrong or not evenly distributed in society, and therefore there are a restricted number of obtainable targets that the fraudsters may find suitable (Tillyer & Eck, 2009).

3.6.2.1.3 Suitable Target

This is the property, a person or any object that may be attractive to an offender. The likelihood that a target is more suitable or less suitable is a function of twelve attributes, designated from the perspective of the offender by the acronyms "CRAVED", which defines levels of obtainability, and "VIVA" which describes levels of risk and challenge (Felson, 2008). The acronym "CRAVED" represents **C**oncealable, **R**emovable, **A**vailable, **V**aluable, **E**njoyable and **D**isposable (Clarke 1999) while, "VIVA" means **V**alue, **I**nertia, **V**isibility and **A**ccessibility (Sutton, 2009). Sutton (2009) compared the two acronyms and established that they deal with distinguishable attributes. Likewise, the author argues that the elements of VIVA describe the characteristics that draw attention, while the CRAVED elements relate to characteristics that make the attractive object available for fraudsters (Anderson, 2006).

This current study is about the victim's characteristics that motivate fraudsters to perpetrate frauds; hence it adopts the VIVA acronym.

The first letter of the acronym, "Value", means that the fraudsters are targeting an individual with a huge amount of money in their bank account. This has been proved by Harrell and Lynn (2013) study of cybercrime, which describes the correlation between the identity theft attack and the individual with a higher income. The "Inertia" simply means the weight, volume and size of the online item, or data that influence the technical specification, portability and accessibility of the target (Yar, 2005). Therefore, a small amount of money is more easily stolen on electronic channels than a huge amount of money. "Visibility" is operationalized as electronic banking activities. Studies to cybercrime show that activities such as e-purchasing, e-fund transfer, e-payment, online auctioning, social media and wrong disposal of computer system and its devices make targets become visible and suitable for fraudsters (Duffield & Grabosky, 2001; Holt & Bossler, 2009; Pratt, Holtfreter, & Reisig, 2010; Hutchings & Hayes, 2009).

Additionally, "Accessibility" is the factor such as a virus, weak software, lack of antivirus, weak password and so on that provides a way for the fraudsters to attack the targeted customers (Duffield & Grabosky, 2001). Accessibility is referred to as the ability and capability of the fraudsters to reach the target, perpetrate the fraud and get away with it (Felson, 1979); for example, unauthorized access to cyberspace through vulnerable encryption devices and weak passwords. The routine activity approach has been used by several studies of cybercrime (Ngo and Paternoster, 2011; Duffield & Grabosky, 2001; Hutchings & Hayes, 2009; Reyns, Henson & Fisher, 2011; Van Wilsem, 2011).

Therefore, the theory applies to this phenomenon. On the other hand, Pratt, Holtfreter and Reisig (2010) view through the suggestion of routine activity theory that those involved in e-banking are more likely to be victims of fraud. Karmen, (2010) opined that the victims of e-banking fraud are naturally involved in a lawful transaction and legitimate online business at the time of attack and oppression. Because of this, merely engaging in transacting business or transferring money (e-payment or e-commerce) from e-banking websites provide a high-fraud motive, compared to individuals or entities that do not transact business or pay money via e-banking. Although it is not illegitimate, the activity of procuring items by the means of e-payments is not the norm. Snyder (2000) posits that the guardianship of online business transactions comes via three procedures: self-regulation and in-house discipline of the online business transaction; organizations and consumer protections; and government regulations. Guardianship does occur in all three procedures from the standpoints of e-fraud prevention and detection; therefore, this theory has really impacted on this phenomenon.

Finally, routine activity theory is one of the main theories used in this study. This section applies routine activity theory to the perception of a target assortment of e-fraudsters in e-banking fraud. In an e-banking fraud, “Suitable Targets” is the banks’ websites and customers’ account information that are involved in the malicious software configuration page to be targeted in e-banking attacks. “Motivated Offender” is the e-fraudster: the planner and the executor of the attack. The “Absence of Capable Guardian” is heightened by cyberspace’s distinctive inconspicuousness and could be described as the absence of security

countermeasures in the banks and on the part of the customers. Consequently, ebanking fraud occurs at the places where these three criteria intersect each other.

In conclusion, the theory of routine activities has been extensively used in extant literatures; among others, robbery (Tseloni, et al., 2004); sexual crimes (Tewksbury and Mustaine, 2001); and cybercrime and online frauds (Pratt, Holtfreter, and Reisig, 2010; Reyns, 2013). Conradt, (2012) has discussed the extrinsic and intrinsic features of cyberspace and deliberated whether it offers a diverse atmosphere of fraud opportunity. Furthermore, the major arguments used to criticize routine activity theory interrogate its efficiency and efficacy, and its political and moral legitimacy, including its propensity to emphasize the victim's blameworthiness. However, these criticisms, which stem mainly from a certain category of authors associated with traditional criminology, respond to criticisms that theories of fraud generally and routine activity theory in particular is the only theories of frauds and the protective models (Cohen & Felson, 1979; Clarke & Felson 1993; Felson, 2008).

Additionally, critics have argued that routine activity theory is based on the rational decision, which makes it applicable only to insignificant crimes with a slighter emotional element, and never to forceful crimes and frauds (Akers, 1998). Additionally, in relation to opportunity, it has been identified that routine activity theory and other fraud theories do not clarify whether spaces can change their capacity to perpetrate fraud or just stand as an attraction for frauds that would have happened anyway.

In conclusion, routine activity theory has faced its most unembellished criticism in the aspect of moral rightfulness. Its critics have shown that

the emphasis on routine activities has revealed an ample absence of interest in the offender, therefore dismembering the aetiology of the challenge. In this case, routine activity theory, though it commences from the principle of the presence of a motivated offender, has not demarcated its connotation and has consequently been unable to demonstrate the basic methodologies of detecting frauds and to answer these questions: “Who are motivated offenders?” “What attributes do motivated offenders have?” and “Why are some people more interested and (motivated) than others to perpetrate frauds?” (Akers, 1998).

3.2.2 The Fraud Management Lifecycle Theory

The fraud management lifecycle is the proactive use of prevention, deterrence, investigation, policy, analysis, detection, mitigation and prosecution of the fraudsters (Wilhelm, 2004). The fraud management lifecycle theory is a network lifecycle where each node or stage in the lifecycle is a combined entity that is formed of interrelated and interdependent actions, operations and functions (Albrecht et al., 2010). The provision of this theory with its components will be adopted in the examination of electronic banking fraud prevention and detection in Nigerian banks. The adoption of this theory results from its methodical approach for combating frauds. In the first place, this theory creates an environment that deters people from perpetrating both online and offline frauds; it embraces the strategies to avoid frauds from happening; and even, if there is occurrence of fraud, and it has provision for purposeful detection strategy, it provides for reprimand and punishment of the criminals.

Moreover, Iminza, Gikiri & Kiragu (2015), in their study "Operational Governance and Occupational Fraud in Commercial Banks in Kenya: A Positivist Approach" proved that the interconnections of the nodes or stages in the fraud management network are the main components of the fraud management lifecycle theory. The theory is significant; it vividly illustrations the stages of fraud management in a chronological manner and demonstrates what institutional procedures and practices should be installed in place for all kinds of frauds to be perfectly and effectively controlled. Furthermore, the theory assumes legal, uniform cultural and technological uses in the prevention and detection of fraud. Therefore, an operation of the Fraud Management Lifecycle begins with an explanation of the lifecycle platforms.

Devoid of this cognizance or consideration, fraud-managing professionals are not likely to relate efficiently with one another both within and without of the organization (Wilhelm, 2004; Jamieson, Stephens & Winchester, 2007; Newton & Osiemo, 2013). The theory posits that the proper interrelationship of diverse groups and components of these stages will result in successful control and perfect management of fraud in the organizations. Therefore, Wilhelm (2004) related the fraud management lifecycle with the need for the management to be responsible for reducing fraud chances and proactive in eliminating fraud opportunities; measuring and identifying fraud; and implementing and monitoring internal control, proper preventive and detective, and other deterrent measures.

Wilhelm (2004) describes the fraud management lifecycle as the accurate interconnectivity of stages of activities such as prosecution, investigation, policy, analysis, mitigation, detection, prevention and

deterrence (see Figure 3.2 below), both internal and external to the business environment, to enhance an environment and culture that elevates ethical behaviour and promotion. This study will identify the effects of interaction of eight significant lifecycle stages in examining electronic banking fraud detection and prevention.

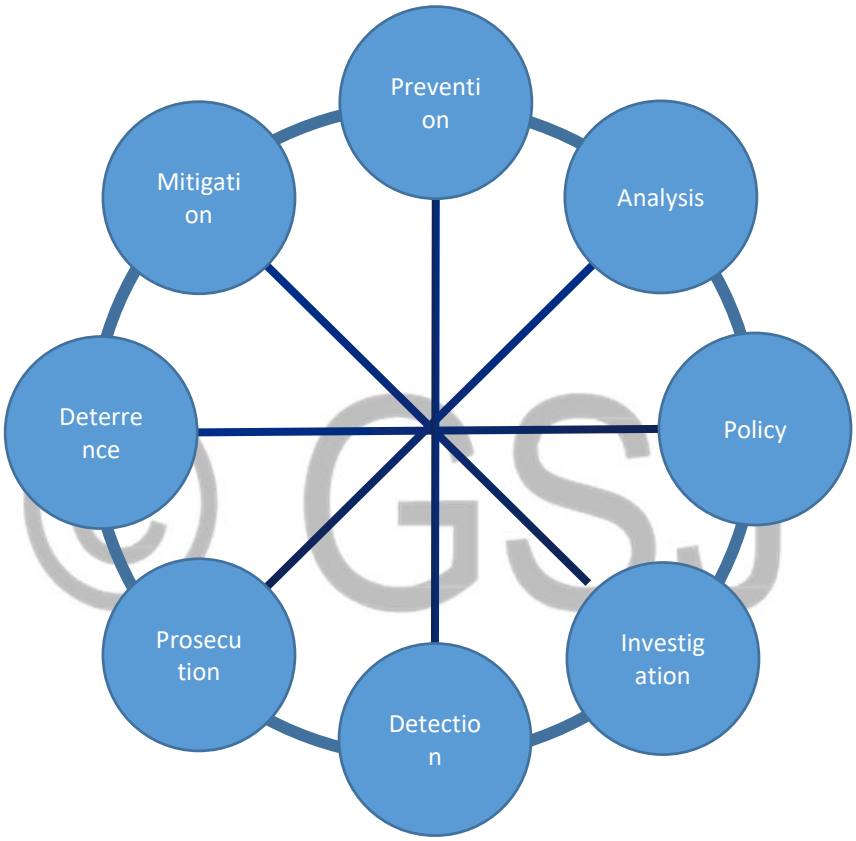

Figure 3.2: The Fraud Management Lifecycle

The operation of the management of the Fraud Management Lifecycle begins with elucidations of its components. One can equitably describe the several lifecycle platforms as numerous disciplines in fraud management. The Fraud Management Lifecycle is consequently a component in lifestyle; that is, a combined entity of interconnected, codependent, and self-governing functions, activities, operations and

actions. These operations may, but need not essentially, happen in a sequential manner.

3.2.2.1 Deterrence

Deterrence is accomplished through creating fear of difficulty and consequences of perpetration, to discourage or turn aside fraudsters from attempting fraudulent activity (Kimani, 2013). Deterrence is characterized by activities and actions targeted at preventing and stopping fraud before it is attempted by making the effort to perpetrate fraud dreadful, unattractive or life-attacking (Ibor, 2016). Deterrence, the leading e-component, is considered by functions, actions, operations and activities envisioned to prevent fraud before it occurs; specifically, to discourage the attempt at committing fraud.

Examples include policy implementation, implementation of laws and regulations, card activation, internet passwords, card pin codes, anti-fraud portals, biometric identification systems, electronic passport verification portals, bank verification numbers (BVN), single points of connection with all bank schemes, data management programs and legal and reputational fraud management (Deloitte, 2015). Therefore, this should include establishing authentication measures and appropriate authorization privileges, physical and logical access maintenance, authentication control processes, customer verification, satisfactory infrastructure security to control appropriate restrictions and boundaries on both external and internal users, data and activities integrity of transactions, information and records.

3.2.2.2 Prevention

This is the second component of the fraud management lifecycle; this comprises functions to avert fraud from happening (Wilhelm, 2004).

Prevention includes activities and actions to stop fraud from occurring (Ibor, 2016). Prevention should be supreme in any e-banking fraud control system. E-banking fraud prevention is the actions and activities to reduce opportunities for e-banking fraud to happen, such as the bank verification number (BVN).

It must be centred on a fraud assessment development that reflects the bank's vulnerability to fraudulent activities within an integrated e-banking approach (Vasiu, 2004). Prevention is the activities to reduce the incidence of electronic fraud, which include core process components, automated controls, deep learning technology, data analytics, employee and customer education, fraud assessment, hotlines mechanisms and real-time monitoring (Chakrabarty, 2013).

3.2.2.3 Detection

This is the activity or action that reveals or uncovers the presence or attempt at fraud, such as statistical monitoring programs that are used to locate and identify fraud subsequent, during and prior to the completion of the fraud perpetration (Wilhelm, 2004). Deloitte (2015) states that detection is a function or an activity exposing or disclosing the existence of fraud and fraud perpetrators which involves special tools and techniques, such as security monitoring software, security monitoring teams (forensic accountants, police forces), inter-agency problem bank meetings, statistical monitoring programs, and national anti-fraud programmes that are used to pinpoint and discover fraud early in, during, and after the finishing point of the fraudulent activity. Chakrabarty (2013) further explained that fraud detection oversight must be in place, for example through surveillance and monitoring systems (escalation and investigation, data management, program and

controls testing), analysing identified red flags, regulatory and internal reporting, internal audits, independent reviews, investigations, fraud management, whistleblowing and tip-offs, suspicious transaction reporting, internal audits, data analytics, by accident, by law enforcement, corporate security (physical and IT), investigative media, and rotation of personnel.

3.2.2.4 Mitigation

This component aims to discontinue fraudsters' activities or to hinder fraud perpetrators from completing or continuing to perpetrate fraud by deactivating banking cards (credit or debit cards), barring their account passcode or PIN, or blocking an account; it can be achieved through message authentication, one-time passwords (OTPs), personal identification numbers, biometric characteristics, payment authentication codes to be sent to customers, customer awareness, customer verification, and account origination (Thamizhchelvy & Geetha, 2012; European Central Bank, 2013). In the following stage, known as analysis, losses that happened regardless of deterrence, detection, and prevention components are known and measured to control the causes of the damage situation by using statistical methods (Wilhelm, 2004).

3.2.2.5 Analysis

Analysis is recognized as the activities to understand and identify losses that happened regardless of the detection, deterrent, mitigation and prevention of e-banking fraud. Analysis must be performed to examine the effects of the fraud management stages of activities on banks and

victim customers. The cost of fraud incidences must be assessed and properly estimated to ascertain exert prioritization of fraud cases. The analysis component collects data concerning performance from other components of the fraud management lifecycle and feedback the outcomes of the performance of each of the components. The analysis gives the performance reporting matrices that permit fraud management to provide calculated, relevant, informed decisions. The procedures of analysis involve examination of causes and the volume of shortages or losses, the reporting and examination of investigation and performance analysis, reporting and evaluation of aggregate and individual detection (rule) performance, the examination and feedback on e-banking fraud prevention and detection, analysis of the impact of the aggregate or individual stages of the fraud management on the increase factors, prevention and detection mechanisms of e-banking fraud.

3.2.2.6 Policy

This is the stage of the fraud management lifecycle theory which deals with the creation, evaluation, communication, and deployment of policies to minimize the occurrence of frauds. Nance and Straub (1988) agreed that information security policies about organizational policies will prevent potential fraudulent acts from being committed.

Hollinger and Clark's (1983) study demonstrates the significance of policy development and organizational control in the prevention of fraud and fraudulent activities in an organization. This theory suggests four key areas of policy improvement that are indispensable in preventing frauds: the full understanding of fraudsters' behaviour, the

dissemination of useful information on organizational policy, broadcasting sanctions, and the implementation and enforcement of sanctions (Wilhelm, 2004).

This also implies that financial institutions need to employ the right, high-integrity, people as staff and have judicious expectations of them. Therefore, the theory postulates the effective and perfect control and management of fraud. Fraudulent behaviour and intentions need to be influenced through the adoption of effective organizational policies and controls targeted at fraudulent awareness for deterrence and the development of controls to detect, prevent and deter fraudulent activities. The policy must strive for balance in deterrence value, sales volume, loss reduction, cost-effectiveness and operational scalability (Wright, 2007). Policy development encompasses continually reassembling the circumstances disassembled in the analysis stage, by gripping the benefit of the knowledge acquired by analysis and merging it with interactive, external and internal environmental factors with the purpose of crafting policies that address the whole intended situations (Wilhelm, 2004).

3.2.2.7 Investigation

This stage involves having sufficient information and enough evidence to end fraudulent incidents, recover stolen assets, and produce evidence that will support the prosecution and conviction of the fraud perpetrators (Wilhelm, 2004; Albrecht et al., 2009). Fraud investigations are concentrated upon three main aspects of activity: law enforcement harmonization, internal investigations, and external investigations. Law enforcement harmonization, as argued by Gottschalk (2010), is the

maintenance and delivery of resources and information to the national, state, provincial and resident law enforcement authorities. Routine and rigorous investigation is required for an effective relationship with law enforcement to enhance effective deterrence of frauds. External investigations are carried out on fraudsters, organized groups, and customers. Meanwhile, internal investigations consist of investigating employees, managements, contractors, vendors, and consultants (Wilhelm, 2004). Electronic surveillance is one of the methods used in this stage of investigation.

3.2.2.8 Prosecution

Wilhelm (2004) argued that "Prosecution" focuses on the judicial and prosecutorial system of authority, along with law enforcement. The main objectives of prosecution in the arena of fraud are to discipline and castigate the fraudsters with the aims of preventing further theft; establishing, maintaining and enhancing the banking sector's reputation; and deterring fraud incidence (Albrecht et al., 2009). The prosecution is the conclusion of both positive and negative outcomes of the fraud management lifecycle stages. Outcomes are negative if the fraud was successfully committed and positive if the fraud was detected and a fraudster was identified, arrested, detained, and charged. This stage also comprises criminal restitution, asset recovery, and conviction with its attendant deterrent value.

Wilhelm (2004) also recommends that the prevention and detection of frauds requires a complete fraud management lifecycle and effective connectivity of its components, which encompass deterrence, detection, prevention, analysis, policy, mitigation, investigation and prosecution.

This means that effective management and control of fraud needs a balancing of the complementary and competing components of the fraud management lifecycle in financial institutions.

Failure to effectively balance the components of this fraud management lifecycle, and failure to adopt appropriate techniques that will ensure perfect integration of its components, may result in poor control and management of fraud in financial institutions.

Therefore, the fraud management lifecycle can be said to be the fraud management, network, in which each of its components represents a node and the lifecycle represents a network, which is seen as a group of entities that is made up of interdependent and interrelated functions, operations, and actions (Wilhelm, 2014).

Moreover, for the fraud management lifecycle to be effective for controlling fraud, there must be an effective, systematic approach and standard coordination of the interconnection of its components. This indicates that, without detection of fraud, prosecution and punishment measures cannot be used to deter perpetration of fraud. An increased detection rate implies that deterrence and preventive techniques have failed. This signifies and confirms the importance of the relationship between these components. The theoretical framework of this study is based on the fraud management lifecycle approach; it will therefore examine the activities of deterrence, detection, prevention, mitigation, policy, analysis, prosecution, and investigation, including their combined interactions and their general impact on prevention and detection of electronic banking fraud in Nigeria.

However, some scholars have argued in their studies that e-banking frauds are not accidental occurrences (Gillett and Uddin, 2005, Bagnoli &

Watts, 2010, Carpenter and Reimers, 2005). Numerous factors contribute to the possibility of their incidence, and the process of the incidence (Langenderfer & Shimp, 2001, ACFE, 2015, Bakre 2007, Zahra, 2005). Conversely, Wesley (2004) argues that the fraud management lifecycle theory is a lifestyle with a system made up of interdependent, interrelated and independent operations, actions and functions. As said earlier, fraud management lifecycle theory comprises eight stages: detection, deterrence, mitigation, prevention, policy, analysis, investigation and prosecution. Contrasting with the fraud triangle theory, Wesley (2004) opined that fraud management theory activities or stages do not essentially occur in a linear flow or sequence. The theory also makes provision for countermeasure of any type of fraud, either e-fraud or non-e-fraud.

Wilhelm (2004) consented with deterrence of frauds, prevention of frauds, detection of frauds, mitigation of frauds, analysis of frauds, fraud policy, investigation of frauds and prosecution of frauds. These platforms of the fraud management cycle must be carefully and successfully incorporated and balanced to get the advantages or the merits of developments in fraud detection and prevention technologies, to prevent the Nigerian economy from suffering shortages of valuable resources and to protect the Nigerian banking sector from fraudulent activities.

3.3 Summary

The relevant and appropriate secondary information acknowledged by the researcher in the literature on the aspects of e-banking fraud were discussed this chapter. The theories of fraud have produced an

understanding of the methods, behaviour and characteristics of fraud and fraudsters. The related studies to the phenomenon with the associated theories adopted serve as guide for the selection of appropriate theories employed as the theoretical framework underpinning this study which are routine activity theory (RAT)
and fraud management lifecycle theory (FMLT).

However, a routine activity theory is a significant theory of environmental criminology and a place-based clarification of fraud theory, in which the behavioural forms and the interrelationships between people in place and in time influence where and when fraud occurs. It advocates that when suitable targets and motivated offenders meet without capable guardians, fraud will probably materialize.

Secondly, the fraud management lifecycle theory is the proactive use of prevention, deterrence, investigation, policy, analysis, detection, mitigation and prosecution of the fraudsters. It is a network lifecycle where each node or stage in the lifecycle is a combined entity that is formed of interrelated and interdependent actions, operations and functions.

The adoption of this theory resulted from its methodical approach for combating fraud. In the first place, this theory creates an environment that deters people from perpetrating both online and offline frauds; it also embraces strategies to prevent frauds from happening; and if there is occurrence of fraud, it has provision for purposeful detection strategy, reprimand and punishment of the criminals.

CHAPTER FOUR

DATA PRESENTATION AND ANALYSIS

4.0 INTRODUCTION

4.1. Research Instruments Design and Testing

Primary data were collected through the means of interviews and questionnaires. The questionnaire survey strategy was employed in this study. Extant literature has identified that the questionnaire is the best and the most appropriate instrument for data collection when employing the survey strategy in this kind of business research (Dionco-Adetayo, 2011; Kothari, 2004). Dionco-Adetayo, (2011) argued that the questionnaire is a technique for collecting information. It is a pro-formulated written set of carefully worded questions and instructions related to a problem for the respondents to answer. Thus, this research used both face-to-face interviews and self-administered questionnaires in order gain understanding of the perspectives of different groups. Consequently, self-administered questionnaire method was adopted in Nigeria, while google docs was deployed to get answers from India, as Dionco-Adetayo (2011) has proved that the self-administration method provides an efficient way of collecting data from many respondents and enhances researcher's understanding through self-observation.

Hence, this method provides quantitative data analysis that supports the deductive approach to the objectives and the research questions of this study.

Furthermore, these questionnaires were in two categories which are questionnaires for the bank staff and questionnaires for the bank customers. The first category was questionnaires for the bank staff, which structured into 5 sections with 97 variables. Section A labeled 'demographic data' has 6 variables. Section B examines 'the current nature of e-banking fraud that are of high concern in Nigerian Banking

Industry and India with 6 variables. Section C, measures 'the factors contributing to the increase of e-banking frauds in Nigerian banks' with 30 variables. Section D measures 'current preventive mechanisms of e-banking fraud in Nigeria banks' with 30 variables. While, section E measures current detective mechanisms of e-banking fraud in Nigeria and India banks with 25 variables (see Table 4.2). While, the second category was questionnaires for the customers within the selected bank's premises which have 2 sections with 30 variables.

Section A labeled 'demographic data' has 3 variables. Section B with 28 variables. It should be noted that response modes and questions in a questionnaire can come in different forms.

4.2 Data Collection Procedure

The researcher seeks for the permission of the respondents through telephone calls and letter of consent sent to the selected banks particularly in Nigeria before the interview and questionnaire administration period, which supported face to face interview with the aid of a tape recorder and taking of notes, and self-administration of questionnaires which took place between on the 14th August and 28th October 2022. These methods gave the researcher a perfect access into the headquarters of the selected banks located in both Lagos state and Abuja. Nevertheless, gaining access to the individual questionnaire respondents and interview participants was very hard, but through management and personal interaction connections with the respondents and participants the aims were achieved.

4.3 Data Preparation and Analysis Procedure

In this research work, preliminary checking of the retrieved questionnaire was carried out to inspect for invalid and valid responses. Although, several authors have argued that quantitative data should be screened, edited, coded, reformed and inputted into a database before it can be analyzed and interpreted (Hair et al, 2010; Crowther & Lancaster, 2009; Sekaran & Bougie, 2010; Hair et al., 2007; Lancaster, 2005). However, there is no specific agreement on which process and pattern it should take.

4.4 Factor Analysis

Factor analysis was employed to answer question 2, which seeks to identify the contemporary perceived factors that have considerable influence on the increase in e-banking fraud in Nigeria; Research question 3 and 4, which seeks to recognize the current mechanisms of prevention and detection of e-banking fraud in Nigeria; and to answer related research questions (see Section 1.3). The purpose of factor analysis is the method simplification of many interrelated measures or components into a small number of representative factors or constructs (Ho, 2006). A researcher may choose to perform factor analysis as either as R- mode or Q-mode. The R-mode deals with the columns, resulting in a minimization in the number of variables of observations, while Q-mode factor analysis deals with the rows, leading to a reduction in the number of observed variations. It is argued by scholars that R-mode factor analysis is more generally accepted, hence many researchers are concerned with minimizing the number or total of variables in any given research situation (Miesch, 1975; Udofia, 2011).

Factor analysis assists a researcher minimizing a large volume of variables. In factor analysis, it is presumed that entire variables are correlated or interrelated to some level or degree. It is thus assumed that variables with comparable or parallel dimensions should be highly correlated while those with different dimensions would have low correlation. Therefore, in the correlation matrix, these low- and high-correlation coefficients become obvious as variables with related dimensions that are interrelated or correlated (Ho, 2006, p 203).

Three main steps are necessary in factor analysis (Raykov & Penev, 2001; Ho, 2006; Udofia, 2011). These are the computation of the correlation matrix, extraction of the initial factor loading, and rotation of extracting factors. In the computation of the correlation matrix, inter-correlation coefficients of variables were computed, which was followed by the extraction of initial factors with the use of SPSS Version 23 software.

There are two main techniques for extracting initial factors: common factor analysis and principal components analysis. The SPSS program further provides an additional six techniques under common factor analysis (Pallant,2001). The principal component analysis (PCA) method was suitable and appropriate for this study, since it is designed for data reduction to attain a small number of constructs or factors to represent the original data set (Holland, 2008).

4.5 Confirmatory Factor Analysis (CFA)

Confirmatory Factor Analysis (CFA) is a multivariate co-relational analysis procedure (Schumacker & Lomax, 2004). It was the most appropriate analysis technique adopted in this study for the quantitative analysis specifically to answer question 2, which seeks to-identify the perceived

factors that have considerable influence on the increase in ebanking fraud in Nigeria and also, research question 3 and 4, which seeks to recognize the current mechanisms of prevention and detection of e-banking fraud in Nigeria; and to answer related research hypotheses. Because CFA is a statistical analysis tool for testing the theoretical relationship between the observed and latent variables. It involves the mixture of factor and regression analyses (Tabachnick & Fidell, 2007). CFA is also known as path analysis technique and is used for multiple correlations and evaluation of relationships, commencing from exploratory analysis to confirmatory analysis (Hair et al., 2010). Structural equation modelling through the structural model estimates multiple simultaneous equations. CFA has been used in similar studies, such as those of Suleiman, et al (2012) and Dimitrios, Dimitrios, and Lazaros (2013). It is, therefore, despite certain limitations, required for theoretical model and hypothesis testing in the current research.

However, to perform CFA, there is a need for a theoretical model with observed variables and unobserved variables. Therefore, to determine the observed variables, latent or unobserved variable computation of exploratory factor analysis (EFA) was required, and then confirmatory factor analysis (CFA) for construct validity (Brown, 2014). Moreover, the outcome of confirmatory factor analysis produced convincing evidence of theoretical construct differentiation and convergent validities. Discriminate validity indicated that there was no high inter-correlation among the diverse indicators of theoretical constructs, while convergent validity meant that there was overlapping or interrelation between various indicators of the theoretical constructs (Schumacker & Lomax, 2004).

Subsequently, hypothetical models were computerized to identify the collaboration between the factors produced by exploratory factor analysis (EFA) and thereafter to determine the extent to which the theoretical model was supported by the sample data using Amos (Schumacker & Lomax, 2004). Moreover, the hypothetical model was modified through the strict observation of fit indexes and significance values: certain factors were removed from the hypothetical model due to their feeble association and correlation with other factors. A modified model with acceptable or excellent fit indexes that significantly and plausible associations among the constructs was fitted and identified as the model.

In this study, identification of the model fit was done by first examining the statistical significance of the parameter estimates of the path, which is commonly appraised by the 0.05 level of significance (Schumacker & Lomax 2004). The next standard considered was an examination of the fit indexes, such as the chi-square (χ2 , Tucker-Lewis index (TLI), comparative fit index (CFI), and root mean square error of approximation (RMSEA). In the Amos fit, measure, there are three estimated techniques that are usually used to compute the χ2 statistic in unmeasured-variable or latent-variable models: maximum likelihood (ML), unweighted least squares (ULS) and generalized least squares (GLS). Each method estimates the model fit and evaluates a best-fitting result. Loehlin (1987) opined that the ULS estimate does not rely on an assumption of normal distribution; therefore, its estimates are inefficient and scale variant, unlike ML and GLS.

Maximum likelihood (ML) evaluations are unbiased, dependable, scale invariant, efficient, normally distributed and scale-free if the measured

variables match with the multivariate normality assumption. Generalized least squares (GLS) valuations have comparable properties to the ML technique under a low rigorous multivariate normality assumption and make available an estimated chi-square test of model fit to the data. However, the researcher has chosen the ML chi-square estimation method for the model analysis in this study.

Model Fit (MF) of the maximum likelihood is used to evaluate the degree to which the sample variance-covariance data fit the structural equation model. The normally used measures of model fit include chi-square (χ2), adjusted goodness-of-fit index (AGFI), goodness-of-fit index (GFI) and root-mean-square residual (RMR) with the Amos program. These measurement techniques are based on variances between the modelimplied variance-covariance matrix and the measured samples; hence, these models fit the criteria. Chi-square (χ2), the adjusted goodness-of-fit index (AGFI), the goodness-offit index (GFI) and the root-mean-square residual (RMR) were adopted as appropriate for this study.

The likelihood ratio chi-square (χ2) statistic is an essential indicator and major statistical measure of the overall goodness-of-fit used in structural equation modelling (Schumacker & Lomax, 2004). When using the chi-square test, the researcher usually aims to reject the null hypothesis and accept its alternative, particularly when there is a statistically significant variance between the “expected” and the “observed”; therefore, the higher the chi-square the better it fits. However, it is otherwise in structural modelling: there the researcher is interested in getting insignificant variances with related degrees of freedom between the predicted and the actual matrices (Wothke, 2000).

In structural modelling, the researcher is interested in accepting or not rejecting the null hypothesis; thus, the lower the chi-square the better the fit of the sample variancecovariance data. The chi-square is sensitive to withdrawals from multivariate normality in measured variables, indicators and intensifies as a main purpose of sample size.

Schumacker and Lomax (2004) posited that the χ2 statistic of model fit may lead to inaccurate decisions concerning analysis of outputs. The chi-square model of the fit measure is delicate to observed sample proportion as the observed sample proportion rises (specifically, equal or greater than 150), the chi-square measure has a propensity to show a significant probability rate. In contrast, as sample proportion declines (specifically, below 100), the chi-square measure displays insignificant probability levels (Blunch, 2012). Hence, χ2 is influenced by sample proportions, due to its computation from $\chi 2 = (n - 1) fq$, where fq is the maximum likelihood fit function.

The goodness-of-fit index (GFI) is determined by the ratio of the addition of the squared variations between the original covariance matrix and replicated matrices to the measured variables. The GFI evaluates the value, variance and covariance in the original covariance matrix that is forecast by the reproduced (implied) covariance matrix based on a factor model (Blunch, 2012). The GFI is an examination of the degree of model fit associated with a single model (no model) (Schumacker & Lomax, 2004; Blunch, 2012; Ho, 2006).

The GFI model fit criterion ranges from 0, signifying no fit, to 1, representing an excellent fit. Specifically, a value close to 0.95 shows a good fit (Schumacker & Lomax, 2004; Blunch, 2012). The adjusted

goodness-of-fit index (AGFI) is attuned from the degrees of freedom (DF) of a specific model compared to a certain number of variables. The AGFI is calculated as 1 – [(R/DF) (1 − GFI)], where R represents the number of single distinct values in the original covariance matrix, p (p + 1) /2, and DF is the number of degrees of freedom in the model. The model fit scale for AGFI runs from 0 (no fit) to 1 (excellent fit). Specifically, an AGFI of 0.95 indicates a good model fit (Schumacker & Lomax, 2004; Blunch, 2012).

The RMR index employs the square root of the mean squared variances between the observed and implied covariance matrices. In other words, it is the square root of the inconsistency between the model covariance matrix and the sample covariance matrix. The root means square error of approximation (RMSEA) evades issues of sample size by investigating the variation between the hypothesized model and the optimally selected population covariance matrix and parameter estimates. The RMSEA is scaled from 0 to 1, with lesser values representing better model fit. A value of 0.05 or less signifies satisfactory model fit (Schumacker & Lomax, 2004; Blunch, 2012). Despite the role of the chi-square of the model fit of unobserved variable models, another five measurement indices have been developed as variants for relating alternative models: The TuckerLewis Index (TLI), normed fit index (NFI), relative fit index (RFI), incremental fit index (IFI) and comparative fit index (CFI). These classically compare a proposed model with an independence model (null model) (Schumacker & Lomax, 2004; Blunch, 2012).The Tucker-Lewis Index (TLI) is used to equate alternative models or a projected model against a null model. The TLI ranges from 0 (no fit) to 1 (excellent fit). Typically, a value close to 0.95 reflects a good model

fit. The value of TLI of this current study was calculated as [X2null/dfnull) – (X2model/dfmodel)] /[(X2null/dfnull) – 1]. The normed fit index (NFI) is used to rescale the chi-square from a no fit (0) to excellent fit (1.0) level (Schumacker & Lomax, 2004). It is measured to assess a constrained model with a completed model by means of baseline null models such as this: (X2null – X2model) /X2 null. The comparative fit index (CFI) is used to measure the development in the non - centrality in proceeding from the least restrictive model of a saturated model.

The relative fit index (RFI) is calculated by the mean of RFI = 1 – [(X2model/dfmodel) /(X2null/dfnull)], while the incremental fit index (IFI) = 1 – [(X2null – X2model) /X2null – dfmodel)]. Schumacker and Lomax (2004) and Blunch (2012) posited that a value close to 0.95 reflects a good model fit. (Note: X2model = the default model, model of the discrepancy; dfmodel = the default model, model of degrees of freedom; X2null = the independence model, model of discrepancy; dfnull = the independence model, model of degrees of freedom). The benchmark for model fit indexes varies in various articles. Hu and Bentler (1999) and Schumacker & Lomax, (2004) elucidated that it is hard to attach a fixed benchmark value to each of the fit indexes because they do not perform correspondingly well in diverse circumstances. Correspondingly, Schumacker and Lomax (2004) stated that there has been much debate on the subjective appropriateness and the independent interpretations of a modelling condition. However, Hu and Bentler (1999) suggested benchmark measures of 0.95 for fit indexes, while a non-significant measure has been suggested for the chi-square (Schumacker & Lomax, 2004). Notwithstanding this, it has been noted that the chi-square benchmark (non-significant) can be prejudiced by the sample size,

particularly if the sample size is above 200. Likewise, Browne and Cudeck (1993) proposed that the benchmark value for the RMSEA index must be less than 0.05, while benchmark values of GFI, AGFI, TLI, NFI and PFI close to 0.95 reflect a good model fit.

4.6 Reliability

Tavokol and Dennick (2011) posited a standard rate of reliability for measuring instruments in sample sizes of over 200 with the use of the Cronbach's Alpha formula. A reliability level of 0.90 and above is accepted as strongly reliable, 0.80 to 0.90 is regarded as highly acceptable, 0.70 to 0.80 is regarded as acceptable, 0.60 to 0.70 is regarded as less acceptable, below 0.60 is regarded as unwanted. Therefore, the Cronbach's Alpha Formula was adopted in this study using the SPSS package; it showed the reliability coefficients of the items related to e-banking fraud prevention and detection in the research questionnaire to be at levels between 0.70 and 0.99.

4.7 Validity

Samples of 200 staff and 200 customers were selected from deposit money banks in Nigeria and India respectively, 100 each, as descriptive and inferential tests of structural equation modelling (SEM) are more reliable with a large sample. Discriminate validity and convergent validity were evaluated through the adoption of exploratory factor analysis (EFA) and confirmatory factor analysis (CFA); all the factor loading was satisfactory for the scope of verifying the concept and the quality of the measurement model. The researcher reviewed the drafted

questionnaire carefully to ensure that the questions were free from ambiguities, lack of clarity and misunderstanding from the researchers' perspective. Additionally, the questionnaires were given to colleagues in the department to review and certain adjustments were made.

Additionally, to fulfil this purpose, the questionnaire adopted for this study passed through pretesting and piloting before finally being used for the data collection. Questionnaires were developed and administered to 25 staff and 10 customers in five of the selected deposit money banks in Lagos between on the 19th and 23rd December 2021 through the due processes stated in section 4.7 of this chapter. The respondents were the internal control managers, internal auditors and accounting managers in the head offices of the selected banks in Nigeria and India alike. In fact, the respondents were selected purposely based on their unique experiences, characteristics, perceptions and possession of the desired information.

CHAPTER FIVE

CONCLUSION, SUMMARY, FINDINGS AND RECOMMENDATIONS

5.1 Conclusion

This research work was carried out particularly to look into the assertions of some youth in Nigeria and India, the context upon which the based their claims (the motivating factors) to be perpetrating criminal activities of diverse sorts - that can be categorized as electronic frauds using banking business channels that are powered by technological innovations as occasioned by the Internet. The cross-border nature of these frauds and the sheer volume of victims and

amount of money been recorded as loss and the untold hardships of the victims aftermath are sources of concern to every saner society.

People grow and developed overtime, but the notion that 'civilization' and advancement of knowledge are one of the driven factors for electronic crimes over the internet could not be totally ascertained nor agreed to as this has led to debates in different fora and its either you speak for or against such notions. However, this research work has concluded that 'technology' is an enabler of opportunities for business growth and development of a society's wealth if well managed, within the right enabling environment, and that the adoption of a technological innovation is not evil in itself, rather it was the ways and manners people who used these innovations will make them appeared to be otherwise. And these wrong assertions are coming from ignorance of the Cyber Space as a system.

The Globalization of Trade, Monetary and Fiscal Governance by the International Organizations (such as World Trade Organization, World Bank, IMF and Paris Club etc) are often if not all the time, dominated by Advance Countries and World Super Powers, which some school of thoughts believed it's at the detriments of developing economies, but in recent times we have all witnessed the emergence of China as a major contender in trade commodities, technological and infrastructural development as export-aid package for third world economies, especially within the African sub-regions - it takes a visionary and committed leadership for a nation like China to emerge from the squabbles of yuan to USD exchange about 2 decades ago and transformed to knowledge (IT Solutions), Infrastructure (Civil and

Structural Engineering) and Argo-Allied export economy, which rival the dominance of the Advanced Western Economies, Europe Inclusive.

On a broader perspective, the Foreign Policy of these western countries tend to project their capitalist instincts on developing nations' economies and its detrimental indices are always propagated by our very own political leaders and businessmen alike. And these elements in our society are but a few inside the whole lots of our population. Therefore, the National Policies of these two very Unique and Strategic democratic Nations in the world must be the ones that engender growth and development at the grassroots, with their youthful population in focus, which this study has been able to reviewed and posit that they are not adequately planned or where there are such policy frameworks, they are not well implemented and monitored for evaluation and measurement of progress or deviation. However, the absence of some of these developmental goals and policy framework does not warrant anyone (including these youth) to be engaged in criminal activities, while attempting to blame it on the Economic Situations of their Countries or trying to blame it on the Advanced Economies. No matter their justification crimes in any form is against the norms and cultural practices in any society.

In exploring the claims of the study population (i.e. the young people involved in online criminal activities - the motivated offenders) during the course of this research, it's also concluded that while attempting to defraud some foreigners of their hard earn money, these motivated offenders also defrauds their own fellow country men and women, not minding who their victims could be! This actual expose the criminal motives of the study population, which longer has no bounds. For the

records, some have even term their illicit activities as ‘yahoo plus’ that is, they have been using some forms of rituals and jujuism as protection from the Authority and hypnotizing their victims. Therefore, the assertions that they are taking vengeance as a result of the economic miseries as occasioned by the Trans-Atlantic Slave Trades and the provision of safe haven for corrupt politicians who stashed our collective wealth abroad do no longer stand and it void.

5.2 Summary

The objective of this study was to provide a contribution to the knowledge and understanding of cyber crimes and electronic frauds as a growing concern amongst the Nigeria and India Youth. The research that has been performed within this study was comprehensive and wide-ranging, and it addressed a broad variety of fraud-related subjects in Nigerian and India Banking Institutions, since it’s on their platform that these cyber crimes and electronic frauds are committed. As these Institutions provided the conduit or an enabling environment for these youngsters dominated crime scene.

However, this study only reproduces a fractional view of fraud in the Nigerian banking industry, only examining the e-banking fraud prevention and detection in the Nigerian and Indian banking sector. There is a profound bedrock of historical, political and social issues that are excluded from the scope of this study, which has engaged only within the e-banking service aspect of nature, contributing factors, challenges, prevention and detection. In view of this, the information discussed in this study provides a significant foundation for discussion of the strategies and mechanisms for preventing and detecting distinct

types of cyber crimes and e-banking fraud in the banking system and other financial institutions within Nigeria and India. Thus, this study elucidates the practical and theoretical contribution made by this study, summarizing the major findings in respect of the research questions; explaining the implications for knowledge, theory, the judiciary and policymakers; revealing policy implications and providing recommendations.

5.3 Findings

5.3.1 Implications of the Findings

The findings and analyses of this study have some significant implications; not only for academic researchers or scholars and accounting practitioners, but also for policymakers in the financial institutions and anti-fraud agencies in both the private and public sectors in Nigeria and India, particularly, given their leadership roles in the stability of their respective sub-regions.

5.3.2 Implications for Theory

This study is the first study to examine the causes of cybercrimes and electronic frauds in the Nigerian and India as a growing concern amongst the youth of these two great Countries. Although. previous studies have focused on banking frauds but were only on online banking fraud and credit card fraud prevention (Williams, 2016; Belan, Mane & Patani, 2014; Kathirvel, 2013). Even though several related studies have been conducted on online banking and credit card fraud in various parts of the world, particularly in the United Kingdom and United States of America, no broad studies like this current study has been done in developing

nations such as Nigeria and near advanced economy nation like India. Peradventure, if any, related study has been conducted in Africa, it was only piecemeal. This is therefore the first study of this nature in the Nigerian context; thus, it has contributed to the theoretical literature and the growing body of knowledge on cybercrimes, e-fraud prevention and detection and also, to the practices of effective e-banking industry.

In Chapter 3, the two theories were combined to discuss cybercrimes and e-frauds prevention and detection. Firstly, the study identified the importance of Routine Activity Theory in the prevention and detection of e-frauds. However, routine activity theory (RAT) commences from the principle of the presence of a motivated offender. It does not demarcate its connotations; consequently, it is incapable of demonstrating the basic methodologies of detecting fraud and of answering basic questions such as “Who are motivated offenders?”, “What attributes do motivated offenders have?” and “Why some people are more interested and (motivated) than others to perpetrate frauds? And also, what are the mechanisms of prevention and detection of fraud?” These questions have been answered by this current study.

Secondly, the findings, submit that the activities of each stage of Fraud Management Lifecycle Theory and their interdependence and consanguinity have a collective and considerable influence on combating e-frauds generally. The eight components of prevention, deterrence, investigation, policy, analysis, detection, mitigation and prosecution are based on the view that individual perpetrator can be dissuaded from perpetrating fraud.

However, the interview and questionnaire respondents confirmed that, at present in the Nigerian and India Cyber Spaces, the activities of fraud

detection and prevention have yet to be balanced with all components of the fraud management life-cycle. The findings indicated that policy and legal, environmental factors intensely influenced the ability of the banking sectors of these two Countries to perform activities in some of the fraud management life-cycle components.

For instance, the findings have disclosed that policy and prosecution have not been effectively handled to prevent and detect e-fraud in Nigeria due to the rampant bribery and corruption in the judicial system, that could really served as deterring factors to serial offenders, and these are also the narratives from India. This involves judges, prosecutors, police, EFCC and has led to a massively increased rate of fraud perpetrators being acquitted. And the youth of these two Nations are seen Political Leaders Siphoning and Embezzling Public Funds in Billions and Court Cases are Prolonged with unending adjournments, there are instances where some of these cases on financial crimes are dismissed based on mere technicalities standings.

Therefore, information policy and legal resources are significant keys to the effectiveness of e-frauds activities as well as the effectiveness of all fraud management units in the banking industry and financial market space.

Conversely, the underlying statement is that unawareness of the fraud management life-cycle and, subsequently, the need to integrate and balance the technological improvements and activities available to each of its components, results in inefficient and ineffective fraud management. Therefore, without this understanding and awareness, fraud management experts in the banking industry are unlikely to

communicate successfully with each other, with their colleagues in other institutions, and within their individual banking businesses.

For example, one of the interview respondents indicated that detection and prevention mechanisms were difficult to implement due to the nature of the laws and technology required. When fraud management experts in the banking industry fail to balance the different components of the fraud management life-cycle effectively and fail to integrate innovative technologies into each component of the life-cycle, this exposes the banks and their customers into fraud losses and the benefits of improvements in fraud detection and prevention technologies are subsumed and muted. Therefore, there is a need for innovative technology, in terms of security infrastructure and technical-know-how, effective awareness and efficient legal practices for mitigating e-banking fraud particularly in the Nigerian banking industry, as the Case and Approach of India is a bit secured with the level of Information Technological Infrastructure available in their System. Also, as discussed earlier, prosecution focuses on the judicial and prosecutorial system of authority along with law enforcement. The main objectives of prosecution in the arena of fraud are to discipline and castigate the fraudsters with the aims of preventing further theft; establishing, maintaining and enhancing the banking sector's reputation; and deterring fraud incidences. The prosecution is the conclusion of both positive and negative outcomes of the fraud management life-cycle stages. Outcomes are negative if the fraud was successfully committed, and positive if the fraud was detected and a fraudster was identified, arrested, detained and charged. This stage is also comprised of criminal

restitution, asset recovery, and conviction with its attendant deterrent value.

Lastly, the current study has added to the theories of fraud by reaffirming the "Seven-Star Model" (see Figure 6.1), (Insert Author) which includes seven prevention and detection mechanisms for e-banking fraud. These are technological mechanisms, fraud monitoring and internal controls, customer complaints and whistle-blowing, surveillance mechanisms, staff-customer awareness and education, legal and judicial controls, and institutional and organizational synergy mechanisms. Therefore, this is a considerable contribution to the theory in the aspect of financial fraud prevention and detection.

5.3.3 Implications for the Judicial System

Due to the challenges emanated by the legal or judicial system, banks find that prosecutions sometimes do not provide compensation for the money and time lost. Nigerian and Indian banking institutions do not find it advantageous to take legal or judicial action when the charges of prosecution are higher than the amount recuperated from the fraud.

The findings of this study have identified that there are feeble legal provisions for prevention and detection of fraud available to the banking industries of these two Countries. The respondents agreed that there were inadequate fraud prosecution procedures, ineffective legislation and law enforcement, inadequate prosecutorial knowledge and unproductive legal procedures, particularly in the Nigerian legal system. Some respondents also said that many fraud cases in the courts remained unresolved for several years; in the process of these delayed cases, some witnesses died (even some where murdered and

perpetrators are not found) or relocated abroad with material evidence, material information was lost, some lost interest in the issue some fraud perpetrators were given an opportunity to bribe their way out. Therefore, these factors affect the deterrence and mitigation power of fraud prosecution, greatly impairing banks' development. Thus, there is need to investigate the impact of the judicial system on the prevention and detective of financial fraud in Nigeria as a whole.

5.3.4 Implications for Policymakers

Obviously, this study has provided other significant contributions to knowledge of theories and empirical applications in the aspect of policy-making in banking institutions.

The study also serves as a source of information on theoretical literature on e-banking fraud prevention and detection in the academic setting. In addition, it provides significant information for decision-makers in the banking sector to modify their practices for combating e-banking fraud and other related fraud types.

Moreover, the findings of this present study have resulted in substantial provisions for legal, regulatory and law enforcement institutions; policymakers within the executive and legislative arms of Nigerian government; executive directors of Nigerian financial institutions; and all professional accounting and banking bodies to be able to design better control and security systems against fraudulent practices within their operations.

5.3.5 Implications for the Motivated Offenders

According to one the Shakespearean Quote, the robbed that smiles, steals something from the thief, any person who is involve in the act of

stealing is equally planning to waste his future in jail, once he/she get caught! This research study have been able to discovered that the assertions as advance by the perpetrators of cybercrimes generally are founded on gross ignorance and poor parenting at the cradle through the teens and adolescent age. While majority of youth in advance economies are part of IT Innovation Service Providers and Tech Inventions, the youth in Nigeria and India (to some certain extent) has been on the news for the wrong reasons. A report by the International Organisation for Peace Building and Social Justice (PSJ) has revealed that 70 percent of Nigeria's youth embrace crime due to lack of economic opportunity and poverty in the land, instead of using their talents for breakthrough, they resorted to quick fix - by trying to get rich quicker. There's no justification for criminality.

5.4 Recommendations

The findings of this study have generated some recommendations for Nigerian banking institutions, as well as for the general transformation of the Nigerian legal and financial sectors to minimize the menace of financial cybercrimes and electronic frauds in the two countries under review, however these recommendations are for the Nigeria Principal Actors in the Banking and Cyber Space. Because this research work does not cover the legal, socio-cultural, political and economic phenomenon in India, only that efforts are geared towards establishing the assertions advanced by some of their youth as an excuse to commit crimes.

In relation to policy, it is obvious that cyber crimes and other related e-banking frauds' prevention and detection mechanisms will work if the governments of the two countries continues to assign significant funds and other resources to their improvement and advancement. The

findings show that without extradition protocols for trans-border cybercrimes, and inter-jurisdictional policy, e-banking fraud will not be combated or controlled in the cyber space.

Moreover, the findings of this study have revealed that improvement of the legal and jurisdictional system is a function of restructuring the judiciary and the law, through a combination of effective training for judges, attorneys and police on the causes, impacts, challenges, prevention and detection of e-banking fraud and other banking crimes.

Therefore, advanced IT training is necessary for all police officers through an Anti-Financial Crimes and Cyber Training Programme in order to enable police units in the country to gain advanced knowledge and ability to aid in combating e-banking and other financial frauds.This would enhance the effectiveness and efficiency of fraud control and mitigation within the industry.

Similarly, education has its own role to play. The Nigeria Inter-Bank Settlement System Plc (NIBSS) and the Nigeria Electronic Fraud Forum (NeFF) should educate prosecutors and police on the causes of e-banking fraud. Workshops and seminars should not only be for bank stakeholders, particularly customers and employees; they also should include police and the prosecutors of fraud cases. This could enhance legal skill and minimize the number of cases of fraud left undecided by the courts due to inadequate legal skills and insufficient evidence.

Also, it is obvious that the Nigerian legal system must be structurally rehabilitated towards e-banking fraud prevention and detection to advance the strength of the Nigerian banking industry. According to the findings of the study, there must be improvements in the court system

in terms of the cost and time required for prosecuting fraud to influence the banks to use prosecution as a tool for deterring and mitigating fraud. The issue of potential e-banking fraud is noted as one of the factors that put off both individuals and business organizations from the idea of internet banking. It affects the banking industry's reputation and reduces the acceptance of mobile banking even in an environment where it might feasibly be a development of the banking industry.

According to the findings, potential fraud has a negative effect on investors' confidence, affecting the country's capacity to contend with other countries in relation to economic development and foreign direct investment (FDI). Therefore, for the Nigerian banking industry to minimize the level of fraud, there is a need for government intervention to mitigate the structural problems of law enforcement agencies and prosecutors to enhance and advance the banks' perception of the judicial system.

Furthermore, individual banks should pay attention to e-banking fraud because the research has revealed that fast implementation of e-banking services security has become significant as banks have introduced e-banking to all their customers. Implementation of sophisticated mechanisms for prevention and detection should be in place, particularly for the top e-banking fraud types in Nigeria: ATM fraud, internet banking fraud, mobile banking fraud, and credit and debit card fraud.

E-banking fraudsters are unlikely to be caught by the current security systems within the individual banks, even though the EFCC has been making some arrests in recent times, some of these arrests are based on

tip offs and the extra-flamboyant life styles of these youth. Therefore, the Nigerian banking systems need to create an external environment in the facet of external information technology structures, as these structures may be vulnerable to attack from the outside, which may result in momentous losses.

Nigerian banking institutions, either jointly or individually, could check for best practice of preventing and detecting e-banking fraud in other banks or institutions worldwide. Additionally, customer awareness crusades are another issue. Banking institutions are reluctant to involve themselves in customer awareness crusades about e-banking fraud, even though they are recognized to be active, because of the potential for reputation loss.

Brand identity is vital to maintaining and sustaining customer loyalty to banks; therefore, the Nigeria Inter-Bank Settlement System Plc (NIBSS) and the Nigeria Electronic Fraud Forum (NeFF) should take on this significant role by providing education to customers and informative materials for all deposit money banks (DMBs) regarding the causes and impacts of e-banking fraud, including how to report, prevent and detect it. This might prominently improve attention to the early-warning scheme of customers' awareness without exposing the brand and product reputation of any bank to risk.

Furthermore, the establishment of a centralized fraud database would be very significant and would enhance the fraud investigation capacity of the fraud investigation teams of the deposit money banks. Likewise, centralization of Nigerian residents' identities in a nationwide database system will have a positive impact on the e-banking fraud investigation scheme and in establishing a fraud management system in the Central

Bank of Nigeria; it will also boost and strengthen jurisdictional prosecution of fraud. Therefore, this study recommends the establishing of a fraud database by the individual banks and a nationwide residents' identity database.

The Nigerian banking sector should provide antivirus software to all their customers by e-bank accounts; they should be given access to download and install it on their individual systems. This will protect individual e-banking customers from the fraudsters using viruses to hijack their account information.

The other recommendation is based on prevention and detection of e-banking fraud perpetrated by fraudsters from abroad. The Nigeria Inter-Bank Settlement System Plc (NIBSS) and the Nigeria Electronic Fraud Forum (NeFF) should associate with foreign banking associations. Such a relationship could enhance their capacities for prevention and detection of e-banking frauds from both within and outside the country and assist the cultivation of international methods and technical knowledge on preventing and detecting e-banking fraud for the use of the Nigerian banking industry.

In the same vein, it is obvious that almost all business and non-business organizations patronize the banking industry and engage with e-banking activities such as electronic points of sale (EPoS) and automated teller machines (ATMs). Therefore, Nigerian banks should create relationships, synergies or partnerships with government and nongovernment organizations, including other financial institutions within the nation, for sharing information and technology for prevention and detection of e-banking fraud, as well as improving knowledge and technology transfer. This would also provide an opportunity to educate all organizations that

prevention and detection of e-banking fraud is not only a fight for a single organization but also involves the cooperation of all organizations within the region.

The National Youth Policy should be designed in such a way that endear patriotism and entrepreneurial development which must be implemented and followed religiously. The Rewarding Systems in our Educational Systems are ridiculous (a VC handshake for passing out as Best Graduating Student or a paltry some of money) when compared to some National Reality Programme aired on TV Stations and Cable Networks with a whooping fortunes in hundreds of millions in less than 4 weeks or more.

There is the need for curriculum change or the present Educational System from Primary to Tertiary need to be overhaul and redesigned to meet the present realities of our time. If Nigeria is to be a Producing or a Services Rendering nation and a destination to go for other Countries, beginning from the sub-region, we embrace technological innovations and knowledge education - not this fundamental information educational we are doing at the moment. India has a nation was able to come out of their socioeconomic woes of the 80s by embracing Information Technological Education and Development with a national road-map for measurement and evaluation. As it stands today, they are even a Nuclear Power Nation.

5.5 Limitations of the Study

This study has produced a comprehensive assessment of the Causes of Financial Cyber Crimes and Electronic Frauds - As Advanced by Some Youngsters in the Nigeria and to some certain degree in India.

Nevertheless, there are certain limitations that were noticed in consideration and discussion of the results of this study.

First, the outcomes of the study are geographically restricted. Although they produce an insight into the Nigerian and Indian Banking Industry and the structural condition of the political and judicial systems, they cannot be applied to other nations except as general lessons and findings. In other words, these results can be applied only to the Nigerian economy and India to some certain extent. In addition, the results are temporally limited, which means that some history and present conditions were described; that is, the results of the study are based only on the historical and present conditions of Nigerian and Indian industries. Therefore, the results may not be applicable to the conditions after changes have taken place to the current situations of government or banking technology.

References

Ablon, L., Libicki, M. C., & Golay, A. A. (2014). Markets for cybercrime tools and stolen data. Rand Corporation.

Abou-Robieh, M. (2005). A study of e-banking security perceptions and customer satisfaction issues (D.B.A.). Available from ProQuest Business Collection. (305340121). Accessed on 27th October 2021 from search.proquest.com/docview/305340121?accountid=10472

Abu-Shanab, E., & Matalqa, S. (2015). Security and fraud issues of E-banking. International Journal of Computer Networks and Applications (IJCNA), 2(4), 179-187.

Abu-Shanab, E., & Pearson, J. M. (2009). Internet banking in Jordan: An Arabic instrument validation process. Int.Arab J.Inf.Technol., 6(3), 235-244.

Account takeover (2009). Tavistock Square London WC1H 9LT.: The UK's Fraud Prevention Service.

ACFE. (2006). ACFE report to the nation on occupational fraud and abuse. (Technical Report). Texas: Association of Certified Fraud Examiners.

ACFE. (2015). ACFE report to the nation on occupational fraud and abuse.Texas Technical Report, Association of Certified Fraud Examiners.

Action Fraud, (2015, 2 December). New figures show steep rise in telephone scams. Press Release UK Fraud Trends 2015.

Adams, R. (2010). Prevent, protect, pursue–a paradigm for preventing fraud. Computer Fraud & Security, 2010(7), 5-11.

Adedipe, A. A. (2016). Nigerian internet fraud: Policy/Law changes that can improve effectiveness.

Adewumi, O. (1986). "Fraud in banks: An overview. In Frauds in Banks Chartered Institute of Bankers, Nigeria.

Adeyemo K. A. (2012). Fraud in Nigerian banks: Nature, deep seated causes, aftermaths and probable remedies. Mediterranean Journal of Social Sciences, 3(2), 279-289.

Agbada, A. O., & Osuji, C. (2013). The efficacy of liquidity management and banking performance in Nigeria. International Review of Management and Business Research, 2(1), 223-233.

Agboola, A. A. & Salawu, R. O. (2008). Optimizing the use of information and communication technology (ICT) in Nigerian banks. Journal of Internet Banking and Commerce, 13(1), 1-15.

Agwu, E. (2012). A qualitative study of the problems and prospects of online banking in developing economies - case of Nigeria. Journal of Internet Banking and Commerce, 17(3), 1-20.

Aibieyi .S. (2007). Anti-corruption strategies and development in Nigeria: A case study of the independent corrupt practices commission

(ICPC) and economic and financial corruption commission (EFCC). A Journal of Contemporary Research., 4, 212-234.

AJAYI, M. A., NAGERI, I. K., ABOGUN, S., & ABDULMUMIN, B. A. (2018). Evaluation of deposit money bank's efficiency in Nigeria: Data envelopment analysis. Fountain University Osogbo Journal of Management, 2(1)

Akers, R. (Ed.). (1998). Social learning and social structure: A general theory of crime and deviance. Boston: North-eastern University Press.

Akindele, R. I. (2011). Fraud as a negative catalyst in the Nigerian banking industry. Journal of Emerging Trends in Economics and Management Sciences (JETEMS), 2(5), 357-363. doi:ournal of Emerging Trends in Ec.

ALAO, A. A. (2016). Analysis of fraud in banks: Evidence from Nigeria. International Journal of Innovative Finance and Economics Research, 4(2), 16-25.

Albrecht, C., Turnbull, C., Zhang, Y., & Skousen, C. J. (2010). The relationship between South Korean chaebols and fraud. 33(3), 257-268. Management Research Review, 33(3), 257-268.

Albrecht, W. S., Albrecht, C., & Albrecht, C. C. (2008). Current trends in fraud and its detection: A global perspective. Information Security Journal, 17, 2-12. doi:10.1080/19393550801934331

Amaratunga, R. G., Baldry, D., Sarshar, M., & Newton, D. (2002). Qualitative and Quantitative research in the built environment: Application of "mixed" research approach. Work Study (Renamed) International Journal of Productivity and Performance Management, 51(1), 17-31.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multi-method empirical examination of home computer user security behavioural intentions. MIS Quarterly, 34(3), 613-643.

Anderson, K. B. (2006). Who are the victims of identity theft? the effect of demographics. Journal of Public Policy & Marketing, 25(2), 160-171.

Anderson, R., Barton, C., Boehme, R., Clayton, R., Levi, M., Moore, T., & Savage, S. (2012). Measuring the cost of cybercrime. Paper presented at the WEIS Conference, Berlin.

Anderson, R., Bond, M., & Murdoch, S. J. (2006). Chip and spin. Computer Security Journal, 22(2), 1-6.

Anyanwu, C. M. (2010). An overview of current banking sector reforms and the real sector of the Nigerian economy. Economic and Financial Review, 48(4), 31-56.

Arrindell, W. A., & Van der Ende, J. (1985). An empirical test of the utility of the observations-to-variables ratio in factor and

components analysis. Applied Psychological Measurement, 9(2), 165-178.

ASSOCHAM (Ed.). (2015). Current fraud trends in the financial sector, joint study of associated chambers of commerce and industry of India. New Delhi: PWC. Accessed from www.pwc.in Association of Certified Fraud Examiners August 6th 2019). Report to the nation on occupational fraud.

Attrichter, H., Fieldmar, A., Posch, P., & Somekh, B. (2008). Teachers investigate their work. An introduction to action research across the professions (Second Edition ed., pp. 147). Routledge: Routledge.

AusCERT (Ed.). (2005). Australian 2005 computer crime and security survey. Brisbane:

AusCERT (Ed.). (2006). Australian 2006 computer crime and security survey. Brisbane: AusCERT.

Australian Crime Commission. (2004). Parliamentary joint committee on the Australian crime commission 2004. Cybercrime Canberra Parliament of the Commonwealth of Australia.

AvinashIngole, & Thool R. C. (2013). Credit card fraud detection using hidden Markov model and its performance. International Journal of Advanced Research in Computer Science and Software Engineering, 3(6)

Bagnoli, M., & Watts, S. (2010). Oligopoly, disclosure, and earnings management. The Accounting Review, 85(4), 191-1214.

Bahnsen, A. C., Stojanovic, A., Aouada, D., & Ottersten, B. (2013). Cost sensitive credit card fraud detection using Bayes minimum risk. Paper presented at 291292 the Proceedings-2013 12th International Conference on Machine Learning and Applications, ICMLA 2013, 1 333-338.

Bakre, O. (2007). The unethical practices of accountants and auditors and the compromising stance of professional bodies in the corporate world: Evidence from corporate Nigeria. Accounting Forum, 31, 277-303.

Banstola, A. (2007). Prospects and challenges of E-banking in Nepal. The Journal of Nepalese Business Studies, 1, 96-104.

Barker, K. J., D'Amato, J., & Sheridon, P. (2008). Credit card fraud: Awareness and prevention. Journal of Financial Crime, 15(4), 398-410. doi:http://dx.doi.org/10.1108/13590790810907236 Accessed on 16th November, 2019

Barnett, C. (2002). The measurement of white-collar crime using uniform crime reporting (UCR) data. US Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services (CJIS) Division.

Barratt, M. J., Ferris, J. A., & Lenton, S. (2015). Hidden populations, online purposive sampling, and external validity: Taking off the blindfold. Field Methods, 27(1), 3-21.

Bartholomew, D. (2008). The rhythm of identity management. Baseline, 81, 38-40.

Bartlett, M. S. (1950). Tests of significance in factor analysis. British Journal of Statistical Psychology, 3(2), 77-85.

Beard, D., & Wen, H. J. (2007). Reducing the threat levels for accounting information systems. The CPA Journal, 77(5), 34-38,40-42.

Beghdad, R. (2008). Critical study of neural networks in detecting intrusions. Computers & Security, 27(5-6), 168-175.

Belan, S., Mane, S., & Patani, T. (2014). Fraud detection in online banking using hidden markov model.

Bennett, M. J. (1986). A developmental approach to training for intercultural sensitivity. International Journal of Intercultural Relations, 10, 179-195. doi:10.1016/0147-1767(86)90005-2, Accessed on 27th July 2020

Bergadano, D., Gunetti, C., & Picardi. (2002). User authentication through keystroke dynamics. ACM Transactions on Information and System Security, 5(4), 367-397.

Bernard, H. R. (Ed.). (2006). Research methods in anthropology. Lanham: MD: Altamira Press.Bhasin, M. (2007). The bank internal auditor as fraud buster. The ICFAI Journal of Audit Practice, 4(1)

Bhasin, M. L. (2015). Menace of frauds in the indian banking industry: An empirical study. Australian Journal of Business and Management Research, 4(2), 21-33.

Bhasin, M. L. (2015). Menace of frauds in the Indian banking industry: An empirical study Australian Journal of Business and Management Research, 4(2), 21-33.

Bhasin, M. L. (2016). Combatting bank frauds by integration of technology: Experience of a developing country. British Journal of Research, doi: ISSN 2394-3718

Bhasin, M. L. (2016). Role of technology in combatting bank frauds: Perspectives and prospects. International Review of Social Sciences, 4(1), 21-37.

Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009). Biometric authentication - A review. International Journal of u- and e- Service, Science and Technology, 2(3)

BIS. (2012). 10 steps to cyber security. department for business. Innovation and Skills,

BIS. (2012). The 2011 skills for life survey: A survey of literacy, numeracy and ICT levels in England. Department of Business Innovation and Skills,

BITS. (2003). Fraud prevention strategies for internet banking, A publication of the BITS fraud reduction steering committee, 17th October,2016.

Blass, A. A., & Oved, Y. (2003). Financing R&D in mature companies: An empirical analysis. Economics of Innovation and New Technology, 12(5), 425-447.

Blumberg, B., Cooper, D. R., & Schindler, P. S. (Eds.). (2005). Business research methods. Maidenhead: McGraw Hill.

Blumer, H. (Ed.). (1969). Symbolic interactionism: Perspective and method. Englewood Cliffs: Prentice Hall.

Blunch, N. (2012). Introduction to structural equation modeling using IBM SPSS statistics and AMOS Sage.

Bo, X., & Surya , Y. (2003). (2003). Effect of online reputation service in electronic markets: A trust- based empirical study. Paper presented at the Ninth Americas Conference on Information Systems, America.

Bo, X., & Surya, Y. (2003). (2003). Effect of onine reputation service in electronic markets: A trust-based empirical study. Paper presented at the Ninth Americas Conference on Information Systems. 2003,

Boechat, G. C., Ferreira, J. C., & Carvalho, E. C. (2006). (2006). Using the keystrokes dynamic for systems of personal security. Paper presented at the Transactions on Engineering, Computing and Technology, Enformatika. 18(1) 200-205.

Boniface, C. (1991). Fraud in the banking industry. the Nigerian banker Oct.-Dec. 22&23. CIBN press.

Bossler, A. M., & Holt, T. J. (2009). Online activities, guardianship & malware infection: An examination of routine activities theory. International Journal of Cyber Criminology, 3(1), 400-420.

Bracken, S. (2010). Discussing the importance of ontology and epistemology awareness in practitioner research. Worcester Journal of Learning and Teaching, 4 Bradford, W. R. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. Journal of Research in Crime and Delinquency, 50(216) doi:10.1177/0022427811425539 Accessed on 21st June, 2020

Brar, T. P. S., Sharma, D., & Khurmi, S. S. (2012). Vulnerabilities in e-banking: A study of various security aspects in e-banking. International Journal of Computing & Business Research, , 1-14. doi:2229-6166, Accessed on 21st June, 2020

Brar, T. P., Sharma, D., & Singh Khurmi, S. (2012). Vulnerabilities in e-banking: A study of various security aspects in e-banking. International Journal of Computing & Business Research, , 1-14.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77-101.

Braun, V., Clarke, V., & Terry, G. (2014). Thematic analysis. Qual Res Clin Health Psychol, 24, 95-114.

Bridges, D., & Smith, R. D. (Eds.). (2007). Philosophy, methodology and educational research (1st ed.) Wiley-Blackwell.

Broadman, H. G., & Isik, G. (Eds.). (2007). Africa's silk road: China and India's new economic frontier. Washington: DC: World Bank.

Brown, T. A. (2014). Confirmatory factor analysis for applied research Guilford Publications.

Browne, M. W., & Cudeck, R. (1993). Alternative ways of assessing model fit. Sage Focus Editions, 154, 136-136.

Brunner, A. D., Decressin, J. W., Decressin, J., Hardy, D. C., & Kudela, B.

(2004). Germany's three-pillar banking system: Cross-country perspectives in Europe International Monetary Fund.

Bryman, A. (2004). Triangulation. In M. Lewis-Beck, A. Bryman & T. F. Liao (Eds.), Encyclopedia of social science research methods. Thousand Oaks: Sage.

Bryman, A. (2006). Integrating quantitative and qualitative research: How is it done. Qualitative Research, 6(1), 97-113.

Bryman, A. (2008). methods and methodology. Qualitative Research in Organizations and Management: An International Journal, 3(2), 159-168.

BRYMAN, A. (Ed.). (2012). Social research methods (4th ed.). Oxford: Oxford University Press. USA

Bryman, A., & Bell, E. (2015). Business research methods Oxford University Press, USA.

Bryman, A., & Bell, E. (Eds.). (2007). Business research methods (2nd ed.). Oxford New York: Oxford University Press Inc.

Calderon, T., & Green, B. P. (1994). Internal fraud leaves its mark: Here's how to spot, trace and prevent it. National Public Accountant, 39(2), 17-20.

Campbell, D. T., & Fiske, D. W. (1959). Convergent and discriminant validation by the multitrait-multimethod matrix. Psychological Bulletin, 56(2), 81-105.

Candy, P. (Ed.). (1991). Self-direction for lifelong learning. San Francisco: Jossey-Bass.

Carpenter, T., & Reimers, J. (2005). Unethical and fraudulent financial reporting: Applying the theory of planned behaviour. Journal of Business Ethics, 60(2), 115-129.

CBN Annual Report (2016). Financial institutions under the supervisory purview of CBN.

CBN Bank supervision report. (2018). Financial institutions under the supervisory purview of CBN: Deposit money banks, Accessed on 22nd May, 2019 https://www.cbn.gov.ng/supervision/AllFinInstitutions.asp

CBN. (2009). Economic report for the fourth quarter of the CBN. Collier, P. & A, 4(4)

Central Bank of Nigeria (CBN). (2002). Financial institutions under the supervisory purview of CBN.

Central Bank of Nigeria (CBN). (2017). Financial institutions under the supervisory purview of CBN.

Central Bank of Nigeria. (2014). Economic report for the first half of 2002. Abuja: Central Bank of Nigeria,

Chakrabarty, K. C. (2013). (2013). Fraud in the banking sector – causes, concerns and cures. Paper presented at the National Conference on Financial Fraud Organised by ASSOCHAM, New Delhi.

Chakraborty, S. (2013, September 13, 2013). Indian banking set to become fifth largest by 2020: KPMG-CII report. Business Standard News

Chan, P. K., Fan, W., Prodromidis, A. L., & Stolfo, S. J. (1999). Distributed data mining in credit card fraud detection. IEEE Intelligent Systems and their Applications, 14(6), 67-74.

Chanson, S. T., & Cheung, T. W. (2001). Design and implementation of a PKI-based end-to-end secure infrastructure for mobile e-commerce. World Wide Web, 4(4), 235-253.

Chanson, S.T., Cheung, T.W. (2001). Design and implementation of a PKI-based end-to-end secure infrastructure for mobile e-commerce. World Wide Web, 4(4), 235-253.

Chartered Institute of Management Accountants. (2008). Fraud risk management: A guide to good practice. Chartered Institute of Management Accountants, 1-80.

Chaturvedi, A., & Meena, A. (2016). Analyzing the impacts of phishing and vishing attacks in internet banking. International Journal of Advanced Research in Computer Science and Software Engineering, 6(3), 16-21.

Chaudhary, K., Yadav, J., & Mallick, B. (2012). A review of fraud detection techniques: Credit card. International Journal of Computer Applications (0975 – 8887), 45(1), 39-44.

Chaudhry, P. E., Chaudhry, S., & Reese, R. (2012). Developing a model for enterprise information systems security. Economics, Management and Financial Markets, 7(4), 587-599.

Chen, C. C., Shaw, R. S., & Yang, S. C. (2006). Mitigating information security risks by increasing user security awareness: A case study

of an information security awareness system. Information Technology, Learning, and Performance Journal, 24(1), 1-14.

Chen, Y., & Tang, T. L. (2006). Attitude towards and propensity to engage in unethical behaviour: Measurement invariance across major among university students. Journal of Business Ethics, 69(1), 77-93.

Chenery, S., Henshaw, C., & Pease, K. (1999). Elegal parking in disabled bays: A means of offender targeting. (briefing note 199.) London, UK: Policing and reducing crime unit, home office research, development and statistics directorate.

Chiemeke, S., Evwiekpaefe, A., & Chete, F. (2006). The adoption of internet banking in Nigeria: An empirical investigation. Journal of Internet Banking and Commerce, 11(3), 1-10.

Chiezey, U., & Onu, A. C. (2013). Impact of fraud and fraudulent practices on the performance of banks in Nigeria. British Journal of Arts and Social Sciences, 15(1)

Chigada, J., & Ngulube, P. (2015). Knowledge-management practices at selected banks in south Africa. South African Journal of Information Management, 17(1), 1-10.

Choo, K. R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & Security, 30(8), 719-731.

Choplin, J. M., & Stark, D. P. (2013). Doomed to fail: A psychological analysis of mortgage disclosures and policy implications. Banking & Financial Services Policy Report, 32(10), 11-19.

Choraś, M., Mroczkowski, P. (2007). (2007). Web security enhancement based on keystroke dynamics. Paper presented at the Third International Conference on Web Information Systems and Technologies. doi:10.5220/0001264903370340 Accessed on 14th April 2020

CIFAS (Ed.). (2009). The anonymous attacker: A special report on identity fraud and account takeover. Tavistock Square London: The UK's Fraud Prevention Service.

CIMA (Ed.). (2009). Fraud risk management A guide to good practice (2nd ed.). 26 Chapter Street London SW1P 4NP United Kingdom: The Chartered Institute of Management Accountants, doi:978-1-85971-611-3, Accessed on the 12th February, 2020

Clarke, R. V. (1999). Hot products: Understanding, anticipating and reducing demand for stolen goods (paper 112), B. Webb (ed.). London: Home office, research development and statistics directorate.

Clarke, R. V., & Cornish, D. B. (1985). Modeling offenders' decisions: A framework for research and policy. In M. Tonry, & N. Morris

(Eds.), Crime and justice: A review of research, vol. 6. (). Chicago, IL: University of Chicago Press.

Clarke, R. V., & Felson, M. (Eds.). (1993). Routine activity and rational choice, advances in criminological theory. (Vol.5 ed.). New Brunswick NJ: Transaction Book.

Cohen, L., & Manion, L. (2000). Research methods in education. (5th ed., pp. 254) Routledge.

Cohen, L.E. and Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588-608.

Cohen, Lawrence E.; Kluegel, James R.; Land, Kenneth C. (1981). "Social Inequality and Predatory Criminal Victimization: An Exposition and Test of A Formal Theory". American Sociological Review. 46 (5): 505–524. doi:10.2307/2094935. JSTOR 2094935.

Collins, K. M. T., Onwuegbuzie, A. J., & Sutton, I. L. (2006). A model incorporating the rationale and purpose for conducting mixed-methods research in special education and beyond, learning disabilities. A Contemporary Journal, 4(1), 67-100.

Collis, J., & Hussey, R. (Eds.). (2009). Business research: A practical guide for undergraduate and postgraduate students (3rd ed.). New York: Palgrave Macmillan.

Comrey, A. L., & Lee, H. B. (2013). A first course in factor analysis Psychology Press.

Conradt, C. (2012). Online auction fraud and criminological theories: The Adrian Ghighina case. International Journal of Cyber Criminology, 6(1), 912-923.

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Worley's critique of situational crime prevention. Crime Prevention Studies, 16, 41-96.

Cornish, D. B., & Clarke, R. V. (Eds.). (1986). The reasoning criminal: Rational choice perspectives on offending (eds. ed.). New York, NY: Springer-Verlag.

Council, F. F. I. E. (2011). Authentication in an internet banking environment.

Coxon, A. P. (Ed.). (2005). Integrating qualitative and quantitative data: What does the user need? (3rd ed.) Open University Press.

Cressey, D. R. (Ed.). (1953). Other People's money. Montclair, NJ: Patterson Smith.

Creswell, J. W. (Ed.). (2009). Research design; qualitative, and mixed methods approaches (3rd ed.). Sage Publications:

Creswell, J. W., Plano, C. V. L., Gutmann, M. L., & Hanson, W. E. (2003). Advanced mixed methods research designs". In A. Tashakkori, & C. Teddlie (Eds.), Handbbok of mixed methods in social

and behavioural research thousand oaks (pp. 209-240) CA: Sage Publications.

Crotty, M. (Ed.). (1998). The foundations of social research: Meaning and perspective in the research process. London: Sage Publications.

Crowther, D., & Lancaster, G. (Eds.). Research methods: A concise introduction to research in management and business consultancy. (2nd ed.). London: Elsevier Ltd.

Çule, M., & Fulton, M. (2009). Business culture and tax evasion: Why corruption and the unofficial economy can persist. Journal of Economic Behaviour and Organisation, 73(3), 811-822.

Curt's carpet services. (2013). (). Costa Mesa, United States, Costa Mesa: Experian Information Solutions, Inc. Retrieved from ABI/INFORM Collection Accessed on 13th January, 2020 from https://search.proquest.com/docview/1587783885?accountid=1047

Dalton, G., & Colombi, J. (2006). (2006). Analyzing attack trees using generalized stochastic petri nets. Paper presented at the 2006 IEEE Workshop on Information Assurance, NY, USA. 116-123.

Dandash, O., Wang, Y., Leand, D. P., & Srinivasan, B. (2008). Fraudulent internet banking payments prevention using dynamic key. Journal of Networks, 3(1), 25-34. doi:10.4304/jnw.3.1.25-34

Darlington, L. (Ed.). (1999). Banking without boundaries: How the banking industry is transforming itself for the digital age, blueprint for the digital economy. New York: McGraw Hill.

David, M., and Sutton, C. (2004). Social research: The basics, Thousand Oaks, CA: Sage,

Deloitte Fraud Survey. (April 23, 2015). The Deloitte India banking fraud survey. (No. Report Edition II). Press Trust of India Report.

Deloitte Survey. (2012, February 8). Indian banking fraud survey. Business Standard,

Denning, D. (2000). Reflections on cyberweapons controls. Computer Security Journal, 16(4), 3-53.

Denscombe, M. (Ed.). (2008). The good research guide. (3rd ed.) Open University Press

Denzin, N. K. (Ed.). (1978). Sociological methods: A source book (2nd ed.) N.Y: McGraw Hill.

Denzin, N. K. (Ed.). (1978). The research act: A theoretical introduction to sociological methods. USA: McGraw-Hill, Inc.

Denzin, N. K., & Lincoln, Y. S. (Eds.). (2003). Strategies of qualitative inquiry. London: Sage Publications.

DeVellis, R. (1991). Scale development theory and applications. Applied Research Methods Series, 26, 51-90.

Diebold, I. (2002). ATM fraud and security: White paper. New York,

Dimitrios, M., Dimitrios, C., & Lazaros, S. (2013). An examination of the critical factors affecting consumer acceptance of online banking: A focus on the dimensions of risk. Journal of Systems and Information Technology, 15(1), 97-116.

Dionco-Adetayo, E. (2011). In Second Edition (Ed.), Guide to business research and thesis writing. Ibadan, Nigeria: Rasmed Publications Limited.

Dorminey, J. W., Fleming, A. S., Kranacher, M., & Riley, R. A.,Jr. (2010). Beyond the fraud triangle. The CPA Journal, 80(7), 17-23,3.

Dorminey, J. W., Fleming, A. S., Kranacher, M., & Riley, R. A.Jr. (2012). Financial fraud. The CPA Journal, 82(6), 61-65.

Dorminey, J., Fleming, A. S., Kranacher, M., & Riley, R. A.,Jr. (2012). The evolution of fraud theory. Issues in Accounting Education, 27(2), 555-579.

Duffield, G., & Grabosky, P. (2001). The psychology of fraud. Trends and Issues in Crime and Criminal Justice, 199, 1-6.

Dures, E., Rumsey, N., Morris, M., & Gleeson, K. (2011). Mixed methods in health psychology: Theoretical and practical considerations of the third paradigm. Journal of Health Psychology, 16(2), 332-341.

Dzomira, S. (2015). Cyber-banking fraud risk mitigation: Conceptual model. Banks and Bank System, 10(2), 7-14.

Dzomira, S. (2015). Online & electronic fraud prevention & safety tips cognizance in south African banks. Socioeconomical – the Scientific Journal for Theory and Practice of Socio-Economic Development, 4(8), 527-540. Accessed on 20th December 2021 doi: dx.doi.org/10.12803/SJSECO.48131

Easterby-Smith, M., Thorpe, R., & Lowe, A., (Eds.). (2002). Management research: An introduction, London (2nd ed.). London: Sage Publication.

Eck, J. E., & Clarke, R. V. (2003). Classifying common police problems: A routine activity approach. Crime Prevention Studies, 16, 7-39.

El-Guindy, M. N. (2008). Cybercrime in the middle east Egypt. SSA Journal.

ENISA. (2012). National cyber security strategies: Setting the course for national efforts to strengthen security in cyberspace. European Union Agency for Network and Information Security,

ENISA. (2014).16 million E-identities and passwords theft. European Union Agency for Network and Information Security.

Eskin, E., & Stolfo, S. J. (2007). System and Methods for Intrusion Detection with Dynamic Window Sizes,

European Central Bank. (2014). Third report on card fraud. Third Report on Card Fraud F e b r u ary 2014.,

EveryoneAPI. (2014). Fraud mitigation and identity verification for card not present transactions.

Ezeoha, A. (2007). Structural effects of banking industry consolidation in Nigeria: A review. Journal of Banking Regulation, 8(2), 159-176.

Ezeoha, A. E. (2005). Regulating internet banking in Nigeria, problem and challenges (part 1). Journal of Internet Banking and Commerce, 10(3)

Fabrigar, L. R., Wegener, D. T., MacCallum, R. C., & Strahan, E. J. (1999). Evaluating the use of exploratory factor analysis in psychological research. Psychological Methods, 4(3), 272.

Fatokun, D. (2016). Fraud landscape in Nigeria. A Changing Payments Ecosystem: The Security Challenge.

Felson, M. (1995.). Those who discourage crime. In John E. Eck, & W. David (Eds.), Crime and place: Crime prevention studies. Monsey, NY: Criminal Justice Press.

Felson, M. (2008). Routine activity approach. In R. Wortley, & L. Mazzerole (Eds.), Environmental criminology and crime analysis (pp. 70-77). New York: Willan Publishing.

Felson, M., & Clarke, R. V. (1998). Opportunity makes the thief: Practical theory for crime prevention. (police research series paper 98.) London, UK: Policing and reducing crime unit, home office research, development and statistics directorate.

Felson, M., & Rachel, B. (Eds.). (2010). Crime and everyday life (4th ed.) Sage Publications.

Ferguson, E., & Cox, T. (1993). Exploratory factor analysis: A users' guide. International Journal of Selection and Assessment, 1(2), 84-94.

Financial Fraud Action UK (FFA UK). (2016). Fraud update: Payment cards, remote banking and cheque. 2016, May 2016.

Financial Fraud Action UK, (2015, 27 March). Scams and computer viruses contribute to fraud increases – calls for national awareness campaign. Press Release

Finch, E. (2010). Strategies of adaptation and diversification: The impact of chip and PIN technology on the activities of fraudsters. Security Journal,

Finger, P. T., Tran, H. V., Turbin, R. E., Perry, H. D., Abramson, D. H., Chin, K., Ritch, R. (2003). High-frequency ultrasonographic evaluation of conjunctival intraepithelial neoplasia and squamous cell carcinoma. Archives of Ophthalmology, 121(2), 168-172.

Finkle, J., & Hosenball, M. (Eds.). (2014). FBI warns retailers to expect more credit card breaches. Reuters.

Fisher, B. S., Daigle, L. E., & Cullen, F. T. (2010). Unsafe in the ivory tower: The sexual victimization of college women. Thousand Oaks, CA: Sage.,

Fleetwood, S. (Ed.). (1999). Critical realism in economics: Development and debate. London: Routledge.

Ford, N. (2011). Banking security: How to beat the fraudsters. African Banker, (15), 20-22,24.

Ford, N. (2015). Fighting the techno criminals. African Banker, (31), 34-36.

Frazer, L., & Lawley, M. (2000). Questionnaire design and administration. A Practical Guide", Milton, QLD: John Wiley and Sons,

Ganesan, R., & Vivekanandan, K. (2009). A secured hybrid architecture model for internet banking (e-banking). Journal of Internet Banking and Commerce, 14(1), 1-17.

Garson, G. D. (2008). Structural equations modelling, from stat notes: Topics in multivariate analysis. Retrieved on June, 15

Gates, T., & Jacob, K. (2009). Payments fraud: Perception versus reality. Economic Perspectives, 33(1), 7-15.

George, T. K., & Jacob, P. (2015). Fraud detection and mitigation in secure e-payment transaction. International Journal of Scientific & Engineering Research, 6(2), 1217-1220. doi:ISSN 2229-5518

Gertler, M., & Nobuhiro, K. (2010). Financial intermediation and credit policy in business cycle analysis. In Friedman, Benjamin M., and Michael Woodford (Ed.), Handbook of monetary economics (pp. 547- 599). Amsterdam, The Netherlands: Elsevier.

Ghosh, A. K., Schatz, M., Michael, C. C., & Schwartzbard, A. (2007). Computer Intrusion Detection System and Method Based on Application Monitoring,

Ghosh, A. K., Schwartzbard, A., & Schatz, M. (1999). (1999). Learning program behavior profiles for intrusion detection. Paper presented at the Workshop on Intrusion Detection and Network Monitoring, 51462 1-13.

Giacinto, G., Roli, F., & Didaci, L. (2003). Fusion of multiple classifiers for intrusion detection in computer networks. Pattern Recognition Letters, 24(12), 1795-1803.

Giles, J. (2010). Scareware: The inside story. New Scientist, 205(2753), 38-41.

Gillett, P., & Uddin, N. (2005). CFO intentions of fraudulent financial reporting. Auditing Journal of Practice and Theory, 24(1), 55-75.

Glorfeld, L. W. (1995). An improvement on horn's parallel analysis methodology for selecting the correct number of factors to retain. Educational and Psychological Measurement, 55(3), 377-393.

Gorman, G. E. (2006). What does "online" mean in 2006? Online Information Review, 30(5), 481-484. doi:http://dx.doi.org/10.1108/14684520610713822 Accessed on 30 September, 2020

Gorsuch, R. L. (1997). Exploratory factor analysis: Its role in item analysis. Journal of Personality Assessment, 68(3), 532-560.

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

Gottschalk, P. (2010). Categories of financial crime. Journal of Financial Crime, 17(4), 441-458.

Grabosky, P., & Smith, R. (2001). Telecommunication fraud in the digital age. Wall DS. London Routledge: Crime and the Internet.

Grabosky, P., Russell, G. S., & Dempsey, G. (Eds.). (2001). Electronic theft unlawful acquisition in cyberspace. Cambridge: Cambridge University Press.

Graham, J. R., Li, S., & Qiu, J. (2008). Corporate misreporting and bank loan contracting. Journal of Financial Economics, 89, 44-61.

Graycar, A., & Smith, R. (2002). (2002). Identifying and responding to electronic fraud risks. Paper presented at the 30th Australasian Registrars' Conference Canberra,

Greene, J. C. (2008). Is mixed methods social inquiry a distinctive methodology? Journal of Mixed Methods Research, 2(1), 7-22.

Greene, J. C., Caracelli, V. J., & Graham, W. F. (1989). Towards a conceptual framework for mixed-method evaluation designs. Educational Evaluation and Policy Analysis, 11(3), 255-274.

Grix, J. (Ed.). (2004). The foundations of research. London: Macmillan.

Gunathilake, N., Padikaraarachchi, A., Koralagoda, S., Jayasundara, M., Paliyawadana, P., Manawadu, C., & Rajapaksha, U. (2013). Enhancing the security of online banking systems via keystroke dynamics. Paper presented at the Computer Science & Education (ICCSE), 2013 8th International Conference on, 561-566.

Gunetti, D., & Picardi, C. (2005). Keystroke analysis of free text. ACM Transactions on Information and System Security (TISSEC), 8(3), 312-347.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (Eds.). (2010). Multivariate data analysis: A global perspective. (7th ed.) New Jersey: Pearson Prentice Hall.

Hair, J., Money, A., Page, M., & Samouel, P. (Eds.). (2007). Research methods for business (First Edition ed.). The Atrium, Southern Gate, Chichester, West Sussex PO198SQ, England: John Wiley & Son Ltd. doi:978-0-470-03404

Halfpenny, P. (1997). The relationship between quantitative and qualitative social research. Bulletin De Methodologie Sociologique, 57, 49-64.

Hamilton, D. I., Justin, M., & Odinioha, G. (2012,). Dimensions of fraud in Nigeria quoted firms. American Journal of Social and Management Sciences, 3(3)(2156-1540 2151-1559), : 112-120. doi:10.5251/ajsms.2012.3.3.112.120

Hammersley, M. (1996). The relationship between qualitative and quantitative research: Paradigm loyalty versus methodological eclecticism. In J. E. T. Richardson (Ed.), Handbook of qualitative research methods for psychology and the social sciences (pp. 159-174). Leicester: British Psychological Society.

Hansen, J., McDonald, J., Messier, W., & Bell, T. (1996). A generalized qualitative response model and the analysis of management fraud. Management Science, 42, 1022-1033.

Harrell, E., & Lynn, L. (Eds.). (2013). Victims of identity theft, 2012. Bulletin NCJ 243779: U.S. Department of Justice Bureau of Justice Statistics.

Harwood, T. G., & Garry, T. (2003). An overview of content analysis. The Marketing Review, 3(4), 479-498.

Hayton, J. C., Allen, D. G., & Scarpello, V. (2004). Factor retention decisions in exploratory factor analysis: A tutorial on parallel analysis. Organizational Research Methods, 7(2), 191-205.

Henn, M., Weinstein, M., & Foard, N. (Eds.). (2009). A short introduction to social research. London: Sage Publications.

Hill, M. R. (1984). Epistemology, axiology, ideology in sociology. Mid-American Review in Sociology, 9(2), 59-77.

Ho, R. (Ed.). (2006). Handbook of univariate and multivariate data analysis and interpretation with SPSS. London: Chapman and Hall/ CRC.

Hoang, X. D., Hu, J., & Bertok, P. (2003). (2003). A multi-layer model for anomaly intrusion detection using program sequences of system calls. Paper presented at the 11th IEEE International Conf. Networks, 531-536.

Hoehle, H., Scornavacca, E., & Huff Sid. (2012). Three decades of research on consumer adoption and utilization of electronic banking channels: A literature analysis.54(1), 122-132. Accessed on 24th May, 2020, doi:http://doi.org/10.1016/j.dss.2012.04.010

Hoffman, D. G. (Ed.). (2002). Managing operational risk: 20 firm-wide best practice strategies. London: John Wiley and Sons.

Holden, M. T., & Lynch, P. (2004). choosing the appropriate methodology understanding research philosophy. Waterford: Waterford Institute of Technology.

Holden, M. T., & Lynch, P. (Eds.). (2004). Choosing the appropriate methodology understanding research philosophy. Waterford.: Waterford Institute of Technology.

Hollinger, R. D., & Clark, J. P. (Ed.). (1983). Theft by employees. Lexington: Lexington Books.

Hollis-Peel, M. E., Reynald, D. M., van Bavel, M., Elffers, H., & Welsh, B. C. (2011).

Guardianship for crime prevention: A critical review of the literature. Crime, Law and Social Change, 56(1), 53-70.

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimisation', deviant behaviour, (30), 1-25.

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. Deviant Behavior, 30(1), 1-25.

Holt, T. J., & Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimisation. Deviant Behavior, 30(1), 25.

Holtfreter, K. (2005). Is occupational fraud "typical" white-collar crime? A comparison of individual and organisational characteristics. Journal of Criminal Justice, 33, 353-365.

Holtfreter, K., Beaver, K. M., Reisig, M. D., & Pratt, T. C. (2010). Low self-control and fraud offending. Journal of Financial Crime, 17(3), 295-307. doi:http://dx.doi.org/10.1108/13590791011056264

Hooks, K. L., Kaplan, S. E., Schultz, J. J.,Jr, & Ponemon, L. A. (1994). Enhancing communication to assist in fraud prevention and detection; comment: Whistle blowing as an internal control mechanism: Individual and organizational considerations. Auditing, 13(2), 86.

Horn, R. (Ed.). (2010). Designing A trading system. CC Suite 509, Private Bag X503 Northway, 4065, KZN, ZA: Alaziac Trading CC Nominee Old Tree Publishing.

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives, 6 (1) p.p. 155, 1999. Structure Equation Modelling, 6(1), 155.

Hutcheson, G. D., & Sofroniou, N. (1999). The multivariate social scientist: Introductory statistics using generalized linear models Sage.

Hutchings, A., & Hayes, H. (2009). Routine activity theory and phishing victimization: Who gets caught in the 'Net'? Current Issues in Criminal Justice, 20(3), 433-451.

Ibor, B. I. (2016). An empirical investigation of the human resources nexus to frauds in the Nigerian banking sector. International Journal of Scientific and Research Publications, 6(6), 231-247.

Idowu, A., & Adedokun, T. O. (l2013). Evaluation of the effect of monitoring and control activities on fraud detection in selected Nigerian commercial banks. Research Journal of Finance and Accounting, .4(6), 37-54.

Igbaekemen, G. O., Abbah, M. T., & Geidam, M. M. (2014). The effect of corruption on socio-economic development of Nigeria. Canadian Social Science, 10(6), 149-157.

IIA, AICPA, & ACFE. (2015). Managing the business risk of fraud: A practical guide.

Imala, O. (2001). The impact of the previously liquidated Banks/Financial institutions and the efficacy of the measures put in place by the supervisory and the regulatory. Authorities. A Paper Presented at the Public Hearing on Developments in the Banking. System Organized by House Committee on Banking and Currency,

Abuja, June, 1

Imiefoh, P. (2012). Towards effective implementation of electronic banking in Nigeria. African Research Review, 6(2), 290-300.

Iminza, N. W., Gikiri, W. l., & Kiragu, D. N.,. (2015). Operational governance and occupational Fraud Risk in commercial banks in Kenya. European Journal of Business Management, 2(1), 401-442.

Iwuagwu, O. (2000). Corruption: A threat to democracy and national development. Journal of National Economic Group of Nigeria, 8(1), 12-16.

Jackson, C., Barth, A., Bortz, A., Shao, W., & Boneh, D. (2009). Protecting browsers from DNS rebinding attacks. ACM Transactions on the Web (TWEB), 3(1), 2.

Jakobsson, M. (2005). (2005). Modeling and preventing phishing attacks. Paper presented at the Financial Cryptography, 5.

James, F., Stratman, T., Duffy, M. (1990). Conceptualizing research on written management communication looking through a glass onion. Management Communication Quarterly: McQ (1986-1998), 3(4), 429.

Jamieson, R., Stephens, G., & Winchester, D. (2007). An identity fraud model categorizing perpetrators, channels, methods of attack, victims and organizational impacts. Paper presented at the Pacific Asia Conference on Information Systems (PACIS) 2007 Proceedings.

Jansen, J., & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis

of factors leading to victimization. International Journal of Cyber Criminology, 10(1), 79-91. doi:10.5281/zenodo.58523

Jassal, R. K., & Sehgal, R. K. (2013). Online banking security flaws: A study. International Journal of Advanced Research in Computer Science and Software Engineering, 3(8), 1016-1021.

Jeffords, R., Marchant, M. L., & Bridendall, P. H. (1992). How useful are the tread way risk factors? Internal Auditor, 60-62.

Jenkins, H. W.,Jr. (2004, Apr 14, 2004). Business world: Is corporate fraud too hard for juries? Wall Street Journal, pp. A.15. accessed on 13th November, 2019 from http://search.proquest.com/docview/398911418?accountid=10472

Johnson, M. (2008). Johnson, M. (2008). A new approach to internet banking. (Unpublished PhD Thesis). University of Cambridge, Cambridge, UK. Accessed on 16th December, 2020 from http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-731.pdf (731)

Johnston, A. (2014). Rigour in research: Theory in the research approach. European Business Review, 26(3), 206-217. doi:http://dx.doi.org/10.1108/EBR-09-2013-0115

Kadushin, C., Sasson, T., & Saxe, L. (2008). Triangulation and mixed methods designs: Practicing what we preach in the evaluation of an Israel Experience educational program. SAGE Journals Online and High Wire Press Platforms, 20(1),46-65. doi:10.1177/1525822X07307426

Kaiser, M. (1974). Kaiser-Meyer-Olkin measure for identity correlation matrix. Journal of the Royal Statistical Society, 52, 296-298.

Kanu, S. I., & Okorafor, E. O. (2013). The nature, extent and economic impact of fraud on bank deposits in Nigeria. Interdisciplinary Journal of Contemporary Research in Business, 4(9), 253-265.

Karlsen, K. N., & Killingberg, T. (2008). Profile based intrusion detection for internet banking systems. Norwegian University of Science and Technology

Karmen, A. (Ed.). (2010). Crime victims: An introduction to victimology. Belmont, CA: Cengage Wadsworth Learning.

Kassem, R., & Higson, A. (2012). The new fraud triangle model. Journal of Emerging Trends in Economics and Management Sciences, 3(3), 191-195.

KATHIRVEL, K. (2013). Credit card frauds and measures to detect and prevent them. International Journal of Marketing, Financial Services & Management Research, 2(3), 172-179.

Keivani, F. S., Jouzbarkand, M., Khodadadi, M., & Sourkouhi, Z. K. (2012). (2012). A general view on the E-banking. Paper presented at the International Proceedings of Economics Development & Research, ,43

Kelling, G. L., Pate, T., Dieckman, D., & Brown, C. E. (1974). The Kansas city preventive patrol experiment. (A Summary Report No. Catalog Number 74-24739). 1201 Connecticut Avenue, NW, Suite 200 Washington, DC 20036-2636: Police Foundation. Accessed on 2nd March, 2022 from http://www.policefoundation.org/docs/copyright.html

Kemper, E. A., Stringfield, S., & Teddlie, C. (2003). Mixed methods sampling strategies in social science research. Handbook of Mixed Methods in Social and Behavioral Research, , 273-296.

Kemper, E. A., Stringfield, S., & Teddlie, C. (2003). Mixed methods sampling strategies in social science research. Handbook of Mixed Methods in Social and Behavioral Research, , 273-296.

Kennedy, L. W., & Forde., D. R. (1990). Routine activities and crime: An analysis of victimization in Canada. Criminology, 28(1), 137-151.

Kevin Wang, S., & Huang, W. (2011). The evolutionary view of the types of identity thefts and online frauds in the era of the internet. Internet Journal of Criminology, , 1-21. doi:2045-6743

Khin, E. W. S., & Heng, T. N. (2012). Epistemological taxonomy in management & accounting research philosophy. Actual Problems of Economics, 131(330), 338.

Kimani, W. (2013,). EAC banks grapple with fraud cases. Daily Nation, Smart Company, pp. 2-3.

Kinkela, K., & Harris, P. (2014). ACFE releases 2014 international study on internal fraud investigation, advocating internal audit. Internal Auditing, 29(5), 10-14.

Kiolbassa, K., Miksch, A., Hermann, K., Loh, A., Szecsenyi, J., Joos, S., & Goetz, K. (2011). Becoming a general practitioner-which factors have most impact on career choice of medical students? BMC Family Practice, 12(1), 25.

Kirda, E., & Kruegel, C. (2006). Protecting users against phishing attacks. The Computer Journal, 49(5), 554-561.

Kline, P. (2014). An easy guide to factor analysis Routledge.

Kocsis, R. (Ed.). (2006). Criminal profiling: principals and practice. NJ: Humana Press.

Kolapo, T. F., Ayeni, R. K., & Oke, M. O. (2012). Credit risk and commercial banks' performance in Nigeria: A panel model approach. Australian Journal of Business and Management Research, 2(2), 31.

Kothari, C. R. (2004). Research methodology: Methods and techniques New Age International.

Kothari, C. R. (Ed.). (2004). Research methodology: Methods and techniques (Second Edition ed.). 4835/24, Ansari Road, Daryaganji,

New Delhi- 110002: New Age International (P) Limited, Publishers. doi:NSBN (13) :978-81-224-2488-1

Kothari, C. R., & Garg, G. (Eds.). (2014). Research methodology: Methods and techniques (3RD ed.). 4835/24, Ansari Road, Daryaganji, Delhi-110002: New Age International (P) Limited, Publishers. doi:978-81-224-3623-5

Kou,Y., Lu,C.,and Sirwongwattana, S. (2004)). Survey of fraud detection techniques. In 2004 International Conference on Network, Sensing and, Control, , 749-754.

Kovach, S., & Ruggiero, W. V. (2011). (2011). Online banking fraud detection based on local and global behavior. Paper presented at the The Fifth International Conference on Digital Society, Guadeloupe, France. 166-171.

KPMG Forensic. (2006). Guide to preventing workplace fraud. Taking action to reduce business crime exposure.

KPMG. (2000). E-commerce and cybercrime: New strategies for managing the risks of exploitation. Forensic and Litigation Services, KPMG LLP, USA, , 27 March 2015.

KPMG. (2005, African fraud and misconduct survey.

KPMG. (2012). Government and public-sector cybercrimes. A Financial Sector View.

Krambia-Kapardis, M. (2002). A fraud detection model: A must for auditors. Journal of Financial Regulation and Compliance, 10(3), 266-278.

Kranacher, M. J., Riley, R. A., & Wells, J. T. (Eds.). (2011). Forensic accounting and fraud examination. London: John Wiley and Sons.

Krauss, S. E. (2005). Research paradigms-qualitative report article. The Qualitative Report, 10(4), 758-770.

Lancaster, G. (Ed.). (2005). Research methods in management (First ed.). Linacre House, Jordan Hill, Oxford OX2 8DP, 30 Corporate Drive, Burlington, MA01803: Elsevier Butterworth- Heinemann. doi:0750662123 Accessed on 11th March, 2022 from http://www.elsevier.com

Langenderfer, J., & Shimp, T. (2001). Consumer vulnerability to scams, swindles and fraud: A new theory of visceral influences on persuasion. Psychology & Marketing, , 763-769.

Laurens, R., & Zou, C. C. (2016). (2016). Using Credit/Debit card dynamic soft descriptor as fraud prevention system for merchant. Paper presented at the Global Communications Conference (GLOBECOM), 2016 IEEE, 1-7.

Lawson, T. (Ed.). (2004). A conception of ontology. Cambridge: University of Cambridge Press.

Ledesma, R. D., & Valero-Mora, P. (2007). Determining the number of factors to retain in EFA: An easy-to-use computer program for carrying out parallel analysis. Practical Assessment, Research & Evaluation, 12(2), 1-11.

Ledesma, R. D., & Valero-Mora, P. (2007). Determining the number of factors to retain in EFA: An easy-to-use computer program for carrying out parallel analysis. Practical Assessment, Research & Evaluation, 12(2), 1-11.

Leukfeldt, E. R. (2014). Phishing for suitable targets in the netherlands: Routine activity theory and phishing victimization. Cyberpsychology, Behavior, and Social Networking, 17(8), 551-555.

Leukfeldt, E. R. (2014). Phishing for suitable targets in the netherlands: Routine activity theory and phishing victimization. Cyberpsychology, Behavior, and Social Networking, 17(8), 551-555.

Leukfeldt, E. R. (2014). Phishing for suitable targets in the netherlands: Routine activity theory and phishing victimization. Cyberpsychology, Behavior, and Social Networking, 17(8), 551-555.

Leung, A., Yan, Z., & Fong, S. (2004). (2004). On designing a flexible e-payment system with fraud detection capability. Paper presented at the 236-243. 311Levi, M., & Williams, M. L. (2013). Multi-agency partnerships in cybercrime reduction: Mapping the network and cooperation space. Information Management and Computer Security, 21(fadayomatthew@yahoo.com), 420-443.

Lewis, C. (2011). Empowering regulators to protect consumer rights in the ICT sector: Final technical report.

Lindner, J. R., Murphy, T. H., & Briers, G. E. (2001). Handling nonresponse in social science research. Journal of Agricultural Education, 42(4), 43-53.

Lister, L. M. (Ed.). (2007). A practical approach to fraud risk: Internal auditors.

Loehline, J. C. (Ed.). (1987). Latent variable structural models: An introduction to factor path, and structural analysis. Hillsdale NJ: Lawrence Erlbaum Associates, Inc.

Longo, E., & Stapleton, J. (2002). (2002). PKI note: Smart cards. . PKI Note Series, PKI Forum,

Loonam, M., & O'Loughlin, D. (2008). An observation analysis of e-service quality in online banking. Journal of Financial Services Marketing, 13(2), 164-178.

Losee, J. (Ed.). (1993). A historical introduction into the philosophies of science (3rd ed.). Oxford: Oxford University press.

Lynch, J. (2005). Identity theft in cyberspace: Crime control methods and their effectiveness in combating phishing attacks. Berkeley Technology Law Journal, 20, 259-300.

Mac, F. (2015). Fraud Mitigation Best Practices, January,

MacCallum, R. C., Widaman, K. F., Zhang, S., & Hong, S. (1999). Sample size in factor analysis. Psychological Methods, 4(1), 84.

MacGibbon, A. (Ed.). (2005). Australian e-commerce safety guide Sydney eBay.

Mahdi, M. D. H., Rezaul, K. M., & Rahman, M. A. (2010). (2010). Credit fraud detection in the banking sector in UK: A focus on e-business. Paper presented at the Paper Presented at the Proc. of the 4th International Conference on Digital Society (ICDS '10), St. Maarten. 232-237.

Mahdi, M. D. H., Rezaul, K. M., & Rahman, M. A. (2010). (2010). Credit fraud detection in the banking sector in UK: A focus on e-business. Paper presented at the Proc. of the 4th International Conference on Digital Society (ICDS '10), St. Maarten. 232-237.

Manyika, J., & Roxburgh, C. (2011). The great transformer: The impact of the internet on economic growth and prosperity. McKinsey Global Institute,

Marascuilo, L. A., & Levin, J. R. (1983). Multivariate statistics in the social sciences: A researcher's guide Wadsworth Publishing Company.

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. Deviant Behaviour, 31(5), 381-410. doi:10.1080/01639620903004903

Marsh, H. W., & Hocevar, D. (1985). Application of confirmatory factor analysis to the study of self-concept: First-and higher order factor models and their invariance across groups. Psychological Bulletin, 97(3), 562.

Masocha, R., Chiliya, N., & Zindiye, S. (2011). E-banking adoption by customers in the rural milieus of south africa: A case of alice, eastern cape, south africa. African Journal of Business Management, 5(5), 1857-1863. doi:http://dx.doi.org/10.5897/AJBM10.850

Mhamane, S. S., & Lobo L m r j. (2012). Use of hidden markov model as internet banking fraud detection. International Journal of Computer Applications, 45(21) doi:10.5120/7071-9556

Mhamane, S. S., & Lobo, L. M. R. (2012). (2012). Internet banking fraud detection using HMM. Paper presented at the icccnt'12, Coimbatore, India. IEEE-20180.

Miesch, A. (1975). Variograms and variance components in geochemistry and ore evaluation. Geological Society of America Memoir, 142, 333-340.

Miles, M. B., & Huberman, A. M. (Eds.). (1994). Qualitative data analysis: An expanded source book . London: Sage Publications.

Miller, J. (2013). Individual offending, routine activities, and activity settings: Revising the routine activity theory of general deviance. Journal of Research in Crime and Delinquency, 50(3), 390-416.

Miller, J. M. (Ed.). (2014). The encyclopedia of theoretical criminology (vol. 1). John Wiley & Sons.

Mirjana Pejic-Bach (Ed.). (2010). Profiling intelligent systems applications in fraud detection and prevention: Survey of research articles Mitchell, M., & Jolley, J. (2004). Measuring and manipulating variables: Reliability and validity. Research Design Explained 5th Edition (Pp, 104 & 536),

Monrose, F., & Rubin, A. (2000). Keystroke dynamics as a biometric for authentication International Journal of Future Generation Computer Systems, 16(4), 351-359. doi:PII: S0167-739X(99)00059-X

Moore, T., & Clayton, R., & Anderson, R. (2009). The economics of online crime 23 (3), 3-20. The Journal of Economic Perspectives, 23(3), 3-20.

Moskovitch, R., Feher, C., Messerman, A., Kirschnick, N., Mustafic, T., Camtepe, A., Elovici, Y. (2009). Identity theft computers and behavioral biometrics. intelligence and security Informatics . ISI '09. IEEE International Conference on, doi:10.1109/ISI.2009.5137288

Mroczkowski, P., & Choras, M. (2006). (2006). Keystroke dynamics in biometrics client server password hardening system. Paper presented at the Advanced Computer Systems (ACS), Miedzyzdroje, Poland. , 2 75-82.

Murdoch, S., & Anderson, R. (2010). Verified by visa and MasterCard SecureCode: How not to design authentication. In R. Sion (Ed.), Financial cryptography and data security (6052nd ed., pp. 336-342). Heidelberg: Springer Berlin.

Muscat, G., James, M., & Graycar, A. (2002). Older people and consumer fraud, Trends and Issues in Crime and Criminal Justice, 220, 1-6.

Nahar, A., Roy, S., & Hasan, S. S. (2016). A survey on different approaches used for credit card fraud detection. International Journal of Applied Information Systems (IJAIS), 10(4), 31-34.

Nance, W. D., & Straub, D. W. (1988). An investigation into the use and usefulness of security software in detecting computer abuse, (eds), , pp. 283-294. In J.I. DeGloss, & M. H. Olson (Eds.), Proceedings of

the ninth international conference on information systems (pp. 283-294). MN: Minneapolis.

Narekar, Y. M., & Chavan, S. K. (2015). A review on credit card fraud Detection Using BLAST-SSAHA Method. International Journal of Advanced Research in Computer and Communication Engineering, 4(11), 425-433.

Neha Sindhu, 2021 Cyber Crime in India: Features, cause, and Elements of Cyber Crime, https://byjus.com/bank-exam/history-banking-india/visited on 20th July, 2021

NDIC. (2012). Annual reports and statement of accounts, .Nigeria Deposit Insurance Corporation.

NDIC. (2012). Nigeria deposit insurance corporation (NIDC) annual. (Annual Report).

Nedelescu, M., & Stănescu, C. (2012). Produse şi servici bancare. Editura Universitară, Bucureşti, 314NeFF. (2016). A changing payments ecosystem: The security challenge. Annual Report, 2016,

Neuman, L. W., & Neuman, W. L. (Eds.). (2000). Social research methods quantitative and qualitative approaches (4th ed.) Allyn & Bacon. doi:13: 9780205297719

Newman, C. J., & Neier, D. S. (2014). Become proactive, not reactive, to anti-fraud and anti-corruption programs. Financial Executive, 30(4), 14-16.

Newman, G., & Clarke, R. V. (Eds.). (2003). Superhighway robbery: Preventing E-commerce crime. . Portland, Willan Publishing.

NIBSS, & Diamond Bank. (2015, 10 April). The evolution of the Nigerian payment system. POS Adoption Study-Lagos State, , 8-9.

Nigerian Deposit Insurance Scheme (NDIC). (2008-2011). Annual reports and statement of accounts.

Njenga, N. M., & Osiemo. (2013). Effect of fraud risk management on organization performance: A case of deposit-taking microfinance institutions in Kenya. International Journal of Social Sciences and Entrepreneurship, 1(7), 1-17.

Njenga, N.Osiemo (2013). effect of fraud risk management on organization performance: A case of deposit-taking microfinance institutions in Kenya. International Journal of Social Sciences and Entrepreneurship, 1(7), 490-507.

Nkemdili, N. A., Bonaventure, U., & Kingsley, A. (2013). No light at the end of the tunnel: Corruption and insecurity in Nigeria. Arabian Journal of Business and Management Review (Oman Chapter), 2(12), 41-54.

Nor, K. M., Shanab, E. A. A., & Pearson, J. M. (2008). Internet banking acceptance in Malaysia based on the theory of reasoned action.

JISTEM-Journal of Information Systems and Technology Management, 5(1), 03-14.

Norse (Ed.). (2014). Account takeover: A complex and growing problem Norse Corporation.

Nunnally, J. (1978). Psychometric methods. 2nd Edition, McGraw-Hill, New York.

Nunnally, J. C., & Bernstein, I. (1994). Psychometric theory (McGraw-hill series in psychology) McGraw-Hill New York.

Nwankwo, O. (2013). Implications of fraud on commercial banks performance in Nigeria. International Journal of Business and Management, 8(15), 144-150.

Nwaze, C. (Ed.). (2006). Bank fraud exposed with cases and preventive measures. Lagos: Control and Surveillance Associates Ltd.

Obalola, M. A. (2010). Ethics and social responsibility in the Nigerian insurance industry: A multi-methods approach. (Unpublished Doctoral thesis). De Montfort University, Leicester, UK.

Odediran, O. (2014). Holistic approach to electronic channels fraud management. Nigeria Electronic Fraud Forum (NeFF) 2014 Annual Report,

Odusami, M. (2015). 3 party cyber risk management using security ratings to manage cyber risk. In Nigerian e-Fraud Forum (NeFF), & Central Bank of Nigeria (CBN) (Eds.), The 2015 annual report , NeFF: Improving and securing the cyber environment (pp. 40-52)

Office for National Statistics. (2015). Crime in England and wales. Year Ending December 2014,

Ogbuji, C. N., Onuoha, C. B., & Izogo, E. E. (2012). Analysis of the negative effects of the automated teller machine (ATM) as a channel for delivering banking services in Nigeria. International Journal of Business and Management, 7(7), 180-190.

Oghenerukevbe, E. A., DME. (2008). Customers perception of security indicators in online banking sites in nigeria. Journal of Internet Banking and Commerce, 13(3), 1-14.

Oghenerukeybe, E. A., DME. (2009). Customers perception of security indicators in online banking sites in Nigeria. Journal of Internet Banking and Commerce, 14(1), 1-15.

Ojo. (2008). Effect of frauds on banking operations in Nigeria. International Journal of Investment and Finance, 1(1), 103.

Oko, S., & Oruh, J. (2012). Enhanced ATM security system using biometric. International Journal of Computer Science Issues (IJCSI), 9(5), 352.

OKOH, J. I., & OKOH, J. O. (2020). Banking sector reforms in Nigeria and unemployment implications. Government, University of Nigeria, Nsukka, , 116.

Olaoye, C. O., & Adekola, D. R. (2014). Analysis of frauds in banks: Nigeria's experience. European Journal of Business and Management, 6 (31)(2222-1905; 2222-2839), 90-99.

Olawale, F., & Garwe, D. (2010). Obstacles to the growth of new SMEs in south Africa: A principal component analysis approach. African Journal of Business Management, 4(5), 729-738.

Olodude, O. (2015). Ransomware: An evolving threat. (The NeFF 2015 Annual Report). Central Bank of Nigeria (CBN). (NeFF: Improving and Securing the Cyber Environment)

Olsen, W. K. (2004). Triangulation in social research: Qualitative and quantitative methods can really be mixed. In M. Holborn, & U. Haralambos (Eds.), Developments in sociology () Causeway Press. doi:d093fbb8-6c02-4915-9d90-907d8c82105d

Omar, A. B., Sultan, N., Zaman, K., Bibi, N., Wajid, A., & Khan, K. (2011). Customer perception towards online banking services: Empirical evidence from Pakistan. Journal of Internet Banking and Commerce, 16(2), 1-24.

Omariba, Z., Masese, N., & Wanyembi, G. (2012). Security and privacy of electronic banking. IJCSI International Journal of Computer Science, 9(3), 432-446.

Ombudsman. (2015). Calling time on telephone fraud a review of complaints about "vishing" scams. (Financial Ombudsman Service insight report). United Kingdom:Financial Ombudsman Service Limited.

Omotayo, T. and Kulatunga, U. (2015). (2015). The research methodology for the development of a kaizen costing frame-work suitable for indigenous construction firms in lagos, Nigeria. . Paper presented at the ARCOM Doctoral Workshop Research Methodology, Grange Gorman Campus, Dublin Institute of Technology.

Omoteso, K. (2006). The impact of information communication technology on auditing. (Unpublished PhD Thesis). De Montfort University, United Kingdom.

Online banking frauds in India cause us$1.3mln in 2009 losses. (2011, Aug 5, 2011). Asia Pulse, pp. n/a. Accessed on 12th April, 2020 from ://search.proquest.com/docview/881769564?accountid=10472

Onwuegbuzie, A. J., Leech, N. L., & Collins, K. T. (2012). Qualitative analysis techniques for the review of the literature. The Qualitative Report, 17(56), 1-28.

Orakci, Ş., & Toraman, Ç. (2018). The validity and reliability studies of the scale attitude toward pedagogical teacher training programme. MOJES: Malaysian Online Journal of Educational Sciences, 6(3), 49-61.

Orji, V., O. (2015). Knowledge management systems: Issues, challenges, and benefits. Communications of the Association for Information Systems, 1(7)

Owolabi S. A. (2010). Fraud and fraudulent practices in Nigerian banking industry. African Research Review, 4(3), 240--256.

Owolabi, A. (2011). Corruption and the environment of accounting and auditing in Africa. International Journal of Critical Accounting, 3(1-3) doi:10.1504/IJCA.2011.039752

Paler-Calmorin, L., & Calmorin, M. A. (2007). Research methods and thesis writing Rex Book Store.

Pallant, J. (2001). SPSS survival manual: A step by step guide to data analysis using SPSS for windows (versions 10 and 11): SPSS student version 11.0 for windows Open University Press Milton Keynes.

Pallant, J. (2005). SPSS survival manual: A step by step guide to data analysis using SPSS for windows (version.)

Pallant, J. (2010). SPSS survival manual: A step by step guide to data analysis using SPSS . maidenhead.

Pallant, J. (2013). SPSS survival manual McGraw-Hill Education (UK).

Pallant, J. (Ed.). (2007). SPSS survival manual. a step by step guide to data analysis using SPSS for windows. UK: McGraw Hill.

Palmerino, M. B. (1999). Take a quality approach to qualitative research. Marketing News, 33(12), 35-36.

Pandey, M., (2010). A model for managing online fraud risk using transaction validation. The Journal of Operational Risk, 5(1), 49-63.

Pandy, S. (2016). Mitigating fraud risk in the card-not-present environment. Federal Reserve Bank of Boston,

Pandy, S. (Ed.). (2016). Payment strategies: Mitigating fraud risk in the card-not Present environment Federal Reserve Banks of Boston and Atlanta.

Papazoglou, M. P. (2003). Web services and business transactions. World Wide Web, 6(1), 49-91.

Park, S. (2015). Winning the online banking war. Blackhat USA: TrendMicro. Parliamentary Joint Committee on the Australian Crime Commission (2004). Cybercrime Canberra parliament of the commonwealth of Australia.

Patil, R. A., & Renke, A. L. (2016). Keystroke dynamics for user authentication and identification by using typing rhythm. International Journal of Computer Applications (0975 – 8887), 144(9)

Patton, M. Q. (Ed.). (1990). Qualitative evaluation and research methods (2nd ed.). London: Sage Publications.

Pedneault, S., Silverstone, H., Rudewicz, F., & Sheetz, M. (2012). Forensic accounting and fraud investigation for non-experts John Wiley & Sons.

Peotta, L., Holtz, M., David, B., Deus, F., & Sousa Jr, R. (2011). A formal classification of interest banking attacks and vulnerabilities. International Journal of Computer Science & Information Technology (IJCSIT), 3(1), 186-197.

Perkins, E. D., & Annan, J. (2013). Factors affecting the adoption of online banking in Ghana: Implications for bank managers. International Journal of Business and Social Research (IJBSR), 3(6), 94-108.

Perlroth, N., & Gelles, D. (Eds.). (2014). Russian hackers amass over a billion internet passwords. . New York: New York Times.

Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. ArXiv Preprint arXiv:1009.6119,

Piazza, P. (2005). Defending networks against targeted trojans. Security
Management, 49(9), 52-52,54.

Polonsky, M. J., & Waller, D. S. (2005). Research project: Designing and managing a business student guide. 2455 Teller Road Thousand Oaks, California 91320: Sage Publications Inc. doi:0-76192249-0

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. Journal of Research in Crime and Delinquency, 47(3), 267-296.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. Journal of Research in Crime and Delinquency, 47(3), 267-296.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. Journal of Research in Crime and Delinquency, 47(3), 267-296.

Rae, K., & Subramaniam, N. (2008). Quality of internal control procedures: Antecedents and moderating effect on organizational justice and employee fraud. Managerial Auditing Journal, 23(2), 104-124.

Rajdeepa B., & Nandhitha D. (2015). Fraud detection in banking sector using data mining. International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064, 4(7), 1822-1825.

Rampini, A. A., & Viswanathan, S. (2010). Collateral, risk management, and the distribution of debt capacity, journal of finance.65, 2293-2322.

Rampini, A. A., & Viswanathan, S. (2015). Financial intermediary capital. Working Paper, Duke University,

Raykov, T., & Penev, S. (2001). The problem of equivalent structural equation models: An individual residual perspective. New Developments and Techniques in Structural Equation Modeling, , 297-321.

Regha, O. (2015). Cybercrime: A risk information centre to the rescue. Nigeria Electronic Fraud Forum (NeFF) 2015 Annual Report, , 72-77.

Reisinger, Y., & Mavondo, F. (2007). Structural equation modeling: Critical issues and new developments. Journal of Travel & Tourism Marketing, 21(4), 41-71.

Reserve Bank of India, 2000. Directory of Commercial Bank Offices in India (Volume 1). Mumbai.

Reserve Bank of India, Various Issues. Statistical Tables Relating to Banks in India. Mumbai.

Reserve Bank of India, Various Issues. Report on Trend and Progress of Banking in India. Mumbai.

Revett, K. (2009). A bioinformatics-based approach to user authentication via keystroke dynamics. International Journal of Control, Automation, and Systems, 7(1), 7-15. doi:http://dx.doi.org/10.1007/s12555-009-0102-2

Revett, K., De Magalhães, S. T., & Santos, H. M. (2005). Password secured sites stepping forward with keystroke dynamics. in next generation web services practices. . Paper presented at the NWeSP 2005. International Conference on IEEE.

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. Journal of Research in Crime and Delinquency, 50(2), 216-238.

Reyns, B. W., & Henson, B. (2013). Security in a Digital World: Understanding and Preventing Cybercrime Victimization,

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. International Journal of Offender Therapy and Comparative Criminology, 60(10), 1119-1139.

Reyns, B., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyber-life style-routine activities theory to cyber-stalking victimization. Criminal Justice and Behavior, 38(11), 1149-1169.

Roberds, W. (1998). The impact of fraud on new methods of retail payment. Economic Review - Federal Reserve Bank of Atlanta, 83(1), 42-52.

Rocco, T. S., Bliss, L. A., Gallagher, S., & Perez-prado, A. (2003). Taking the next step: Mixed methods research in organizational systems. information technology. Learning and Performance Journal, 21(1), 19-29.

RSA (2010) A monthly intelligence report from the RSA anti-fraud command centre. (online fraud report).

Sahin, Y., & Duman, E. (2010). (2010). An overview of business domains where fraud can take place, and a survey of various fraud detection techniques. Paper presented at the 1st International Symposium on Computing in Science and Engineering, Aydin, Turkey.

Saleh, Z. (2013). The impact of identity theft on perceived security and trusting E-commerce. Journal of Internet Banking and Commerce, 18(2), 1-11.

Saleh, Z. I. (2011). Improving security of online banking using RFID. Academy of Banking Studies Journal, 10(2), 1.

Salim, H. (Ed.). (2014). Cyber safety: A systems thinking and systems theory approach to managing cyber security risks. Massachusetts Institute of Technology Cambridge: Composite Information Systems Laboratory (CISL) Sloan School of Management. doi:MA 02142

Salu, A. O. (2004). Online crimes and advance fee fraud in Nigeria - are available legal remedies adequate? Journal of Money Laundering Control, 8(2), 159-167.

Sanusi, L. (2010). The Nigerian banking industry: What went wrong and the way forward. Delivered at Annual Convocation Ceremony of Bayero University, Kano Held on, 3(1), 2010.

Sanusi, S. L. (2011). Banking reform and its impact on the Nigerian economy. CBN Journal of Applied Statistics, 2(2), 115-122.

Sanusi, S. L. (2011). Global financial meltdown and the reforms in the Nigerian banking sector. CBN Journal of Applied Statistics, 2(1), 93-108.

Saranya, K. & Gunasri, K. (2013). Challenges in E-banking. International Journal of Scientific Research and Management (IJSRM), (22), 27.

Sarma, G., & Singh, P. K. (2010). Internet banking: Risk analysis and applicability of biometric technology for authentication. International Journal of Pure and Applied Sciences and Technology, 1(2), 67-78.

Saudi, M. M., Ismail, S., Tamil, E. M., & Idris, M. Y. I. (2007). Phishing: Challenges and issues in malaysia. International Journal of Learning, 14(8), 79-88.

Saunders, M. L. and Thornhill P. (2003). Research Methods for Business Students,

Saunders, M., Lewis, P., & Thornhill, A. (2009). Understanding research philosophies and approaches. Research Methods for Business Students, 4, 106-135.

Saunders, M., Lewis, P., & Thornhill, A. (Eds.). (2007). Research methods for business students (4th Edition ed.). Edinburgh Gate, Harlow, Essex CM20 2JE, England: Pearson Education Limited. doi:13-978-0-273-70148-4 Accessed on 15th May, 2021 from www.pearsoned.co.uk

Saunders, M., Lewis, P., & Thornhill, A. (Eds.). (2015). Research methods for business students (Seventh ed.). Edinburgh Gate, Harlow, Essex CM20 2JE, England: Pearson Education Limited. doi:978-1-292-01662-7 Accessed on 7th May, 2020 from www.pearson.com/uk

Saunders, M., Lewis, P., & Thronhill, A. (Eds.). (2012). Research methods for business students (4th ed.). Harlow: Pearson Education Ltd.

Schneier, B. (2011). Secrets and lies: Digital security in a networked world John Wiley &Sons.

Schumacker, R. E., & Lomax, R. G. (2012). A beginner's guide to structural equation modeling Routledge.

Schumacker, R. E., & Lomax, R. G. (Eds.). (2004). A beginner's guide to structural equation modeling. Mahwah, N.J: Lawrence Erlbaum Associates.

Schutt, R. K. (Ed.). (2003). Investigating the social world: The process and practice of research. Newbury Park: CA: Pine Forge Press.

Sekaran, U. (Ed.). (2003). Research methods for business: A skill building approach (Fouth ed.). Jose Ortega/Stock Illustration Source: Hermitage Publishing Services, doi:0-471-38448-8; 0-471-2036606

Sekaran, U., & Bougie, R. (Eds.). (2010). Research methods for business: A skill building approach (Fifth Edition ed.). The Atrium, Southern Gate, Chichester, West Sussex, PO198SQ, United Kingdom: John Wiley & Sons Ltd. doi:978-470-74479-6

Sekaran, U., & Bougie, R. (Eds.). (2013). Research methods for business: A skill building approach (Sixth Edition ed.). The Atrium, Southern Gate, Chichester, West Sussex, PO198SQ, United Kingdom: John Wiley & Son Ltd. doi:978-1-118-52785-6 accessed from www.wileyopenpage.com

Shah, M. (2009). E-banking management: Issues, solutions, and strategies: Issues, solutions, and strategies IGI Global.

Shah, M. H., Braganza, A., & Morabito, V. (2007). A survey of critical success factors in e-banking: An organizational perspective.

European Journal of Information Systems, 16(4), 511-524. doi:http://dx.doi.org/10.1057/palgrave.ejis.3000693

Shanmugapriya, D., & Padmavathi, G. (2009). A survey of biometric keystroke dynamics: Approaches, security and challenges. International Journal of Computer Science and Information Security, IJCSIS, 5(1), 115-119. doi:ISSN 1947 5500

Shannak, R. O. (2013). Key issues in E-banking strengths and weaknesses. The Case of Two Jordanian Banks, European Scientific Journal, 9(7), 239-263.

Silverstone, H., & Sheetz, M. (Eds.). (2007). Forensic accounting and fraud investigation for non-experts (2nd ed.). New Jersey, USA: John Wiley & Sons, Inc.

Singh, P., & Singh, M. (2015). Fraud detection by monitoring customer behavior and activities. International Journal of Computer Applications (0975 – 8887), 111(11), 23-32.

Singh, Y. K. (Ed.). (2006). Fundamental of research methodology and statistics (1ST ed.). 4835/24, Ansari Road, Daryaganji, New Delhi-110002: New Age International. Publishers. doi:ISBN : 978-81-224-2418-8.

Smith, R. (2007). Biometric solutions to identity-related cybercrime' in jewkes Y (ed) crime online Devon Willan publishing.

Smith, R., & Akman, T. (2008). Raising public awareness of consumer fraud in Australia. Trends and Issues in Crime and Criminal Justice, 349, 1-6.

Snyder, J. M. (2000). Online auction fraud: Are the auction houses doing all they should or could to stop online fraud? Federal Communications Law Journal, 52(2), 453-472.

Soltani, B. (2014). The anatomy of corporate fraud: A comparative analysis of high profile American and European corporate scandals. Journal of Business Ethics, 120(2), 251-274. doi:http://dx.doi.org/10.1007/s10551-013-1660-z 323324

Srivastava, A., Kundu, A., Sural, S., & Majumdar, A. (2008). Credit card fraud detection using hidden markov model. IEEE Transactions on Dependable and Secure Computing, 5(1), 37-48.

Srivastava, Abhinav, Amlan, K., Shamik, S., & Arun, K. M. (2008). Credit card fraud detection using Hidden markov model. IEEE Transactions on Dependable and Secure Computing, 5(1), 37-48.

Sruthi T.V., & Prasanna. (2016). Fraud detection in banking institutions. International Journal of Engineering and Technology (IJET), 8(2), 1127-1130.

Sruthi, T., & Prasanna. (2016). Fraud detection in banking institutions. International Journal of Engineering and Technology (IJET), 8(2), 1127-1130. doi:p-ISSN : 2319-861

Stemler, S. (2001). An overview of content analysis. Practical Assessment, Research & Evaluation, 7(17), 137-146.

Subramanian, R. (Ed.). (2014). Bank fraud: Using technology to combat losses. Carry, North Carolina, USA.: SAS institute Inc.

Suleiman, G. P., Kamariah, M., Adesiyan, O. I., Mohammed, A. S., & Jamal, A. (2012). Customer loyalty in e-banking: A structural equation modelling (SEM) approach. American Journal of Economics, , 55-59. doi:10.5923/j.economics.20120001.13

Sullivan, R. J. (2014). Controlling security risk and fraud in payment systems. Economic Review - Federal Reserve Bank of Kansas City,5-36.

Sutton, M. (2009). Product design: CRAVED and VIVA. In B. S. Fisher, & Lab S. P. (Eds.), Encyclopedia of victimology and crime prevention. Sage: Thousand Oaks.

Sydney, I. F. (1986). "Management control system, prevention and detection of frauds. A Paper Presented at the Seminar on Frauds in Banks Organized by the Nigerian Institute of Bankers, Lagos, Nigeria,

Symantec Security Response. (2005). "Phishing in the middle of the stream" - Today's threats to online banking. Paper presented at the The AVAR 2005 Conference, Symantec Security Response, Dublin. 1-28.

Symantec. (2015). ISTR 20: Internet security threat report. Tabachnick, B. G., & Fidell, L. S. (Eds.). (2007). Using multivariate statistics (5th ed.). Boston: Allyn and Bacon.Tan, T. M., & Rasiah, D. (2011). A review of online trust branding strategies of financial services industries in Malaysia and Australia., Advances in Management & Applied Economics, International Scientific Press, 1(1), 125-150.

Tandon, Prakesh, 1989. Banking Century: A Short History of Banking in India. Viking: New Delhi.

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. International Journal of Medical Education, 2, 53-55. doi: ijme.2.5355 [pii]

Taylor, J. (Ed.). (2011). Forensic accounting. (1st ed.). Edinburg Gate Harlow Essex CM20 2JE, England: Pearson education.

Teoh, S. T., Ma, K., Wu, S. F., & Jankun-Kelly, T. (2004). Detecting flaws and intruders with visual data analysis. IEEE Computer Graphics and Applications, 24(5), 27-35.

Tessier, D. R. (2013). The fraud triangle theory: how a three-pronged approach can improve your bottom line. The CLM.

Tewksbury, R., & Mustaine, E. E. (2001). Lifestyle factors associated with the sexual assault of men: A routine activity theory analysis. The Journal of Men's Studies, 9(2), 153-182.

Thamizhchelvy, K., & Geetha, G. (2012). E-banking security: Mitigating online threats using message authentication image (MAI) algorithm. International Conference on Computing Sciences, , 176-284. doi:10.1109/ICCS.2012.29

The World Bank. (2015). Information communications technology for development. 2015 LIMA Annual Meeting, Wor;Ld Bankn Group , International Monetory Funds,

Tilley, N. (2009). Crime prevention: criminal justice series (Illustrated ed.). Pennsylvania State University: Willan Publishing.

Tillyer, M. S., & Eck, J. E. (2009). Routine activities. In J. M. Miller (Ed.), 21st century criminology: A reference handbook (pp. 279-287). Thousand Oaks: CA: Sage.

Tillyer, M. S., & Eck, J. E. (2010). Getting a handle on crime: A further extension of routine activities theory. Security Journal. Online First Edition, doi:10.105710.1057

Tongco, M. D. C. (2007). Purposive sampling as a tool for informant selection. Ethnobotany Research and Applications, 5, 147-158.

Tran, V. M., & Perry, J. A. (2003). Challenges to using neem (azadirachta indica var., sianensis valenton) in Thailand. Economic Botany, 57(1), 93.

Trochim, W. K., & O'Donnelly, J. P. (Eds.). (2006). The research methods knowledge base . (3rd ed.). New York: Thomson.

Tseloni, A., Wittebrood, K., Farrell, G., & Pease, K. (2004). Burglary victimization in England and Wales, the united states and the Netherlands: A cross national comparative test of routine activities and lifestyle theories. British Journal of Criminology, 4(1), 66-91.

Uchenna, C., & Agbo J. C. (2013). Impact of fraud and fraudulent practices on performance of banks in Nigeria. British Journal of Arts and Social Science, 15(1)

Udoayang, J. O., James, F. U. (2004). Auditing and investigation. Calabar: University of Calabar Press.,

Udofia, E. P. (Ed.). (2011). Applied statistics with multivariate methods. Enugu: Immaculate Publications Ltd.

Ulbrich, I., Canagaratna, M., Zhang, Q., Worsnop, D., & Jimenez, J. (2009). Interpretation of organic components from positive matrix factorization of aerosol mass spectrometric data. Atmospheric Chemistry and Physics, 9(9), 2891-2918.

Ureche, O., & Plamondon, R. (2000). Digital payment systems for internet commerce:The state of the art. World Wide Web, 3(1), 1-11.

US-CERT. (2015). Federal incident reporting guidelines. Official Website of the Department of Homeland Security,

Usman, A. K., MSc, & Shah, M. H., PhD. (2013). Critical success factors for preventing e-banking fraud. Journal of Internet Banking and Commerce, 18(2), 1-15.

Usman, A. K., MSc, & Shah, M. H., PhD. (2013). Strengthening E-banking security using keystroke dynamics. Journal of Internet Banking and Commerce, 18(3), 1-11.

Van Wilsem, J. (2013). "Bought it, but never got it" assessing risk factors for online consumer fraud victimization. European sociological review. Oxford: Oxford University Press, doi:10.1093/esr/jcr053

Vandommele, T. (2010). Biometric authentication today. Seminar on Network Security, doi: T-110.5290

Vasiu, L. (2004). (2004). A conceptual framework of eFraud control in an integrated supply chain. Paper presented at the Proceedings of European Conference on Information Systems (ECIS), 161-174.

Velicer, W. F., & Fava, J. L. (1998). Effects of variable and subject sampling on factor pattern recovery. Psychological Methods, 3(2), 231.

Velicer, W. F., Eaton, C. A., & Fava, J. L. (2000). Construct explication through factor or component analysis: A review and evaluation of alternative procedures for determining the number of factors or components. Problems and solutions in human assessment (pp. 41-71) Springer.

Vrincianu, M., & Popa, L. (2010). Considerations regarding the security and protection of E-banking services consumers' interests. . Journal of Internet Banking and Commerce, 12(28), 388-403.

Wada, F., & Odulaja G.O. (2012). Electronic banking and cybercrime in Nigeria: A theoretical policy perspective on causation. African Journal of Computer and ICTs, 5(1), 69-82.

Wada, F., & Odulaja, G. (2012). Assessing cybercrime and its impact on e-banking in Nigeria using social theories. African Journal of Computing & ICT, 5(1), 69-82.

Wada, F., & Odulaja, G. (2012). Electronic banking and cybercrime in Nigeria-A theoretical policy perspective on causation. African Journal of Computing & ICT www.Ajocict.Net, 4(3), 69-82.

Wang, S. K., & Huang, W. (2011). The evolutionary view of the types of identity thefts and online frauds in the era of the interne. Internet Journal of Criminology, 1-14.

Wang, W. Y. C., Rashid, A., & Chuang, H. (2011). Toward the trend of cloud computing. Journal of Electronic Commerce Research, 12(4), 238.

Wang, W., Yuan, Y., & Archer, N. (2006). A contextual framework for combating identity theft, IEEE security and privacy. . IEEE Computer Society,

Webb, E. J., Campbell, D. T., Schwartz, R. D., & Sechrest, L. (Eds.). (1966). Unobtrusive measures: Nonreactive research in the social sciences. Chicago: Rand McNally.

Wei, W., Li, J., Cao, L., Ou, Y., & Chen, J. (2012). Effective detection of sophisticated online banking fraud on extremely imbalanced data. World Wide Web (Internet and Web Information Systems), , 1-29. doi:10.1007/s11280-012-0178-0

Wells, J. (Ed.). (2014). Corporate fraud handbook: Prevention and detection (2nd ed.). London: John Wiley and Sons.

Wells, J. T. (2002). Occupational fraud: The audit as deterrent. Journal of Accountancy, 193(4), 24-28.

Wells, J. T. (Ed.). (2005). New approaches to fraud deterrence. The Institute of Chartered Accountants of India, New Delhi: The Chartered Accountant. doi:1453-1455

Wells, J. T. (Ed.). (2011). Corporate fraud handbook: Prevention and detection (3rd ed.). Hoboken, New Jersey: John Wiley & Sons Inc.

Wells, J. T. (Ed.). (2014). Principles of fraud examination (4th ed.). United State of America: John Wiley &Sons. Inc. doi:978-1-118-58288-6; 10987654321

Wesley, K. (2004). Fraud management life-cycle theory. A holistic approach to Fraud Management. Journal of Economic Crime Management, 2(2)

Wilcox, P., Madensen, T. D., & Tillyer, M. S. (2007). Guardianship in context: Implications for burglary victimisation risk and prevention', , 44: 771– 803. Criminology, (44), 771-803.

Wilhelm, W. K. (2004). The fraud management lifecycle theory: A holistic approach to fraud management. Journal of Economic Crime Management, 2(2), 1-38.

Williams, B., Onsman, A., & Brown, T. (2010). Exploratory factor analysis: A five-step guide for novices. Australasian Journal of Paramedicine, 8(3)

Williams, M. L. (2015). Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. British Journal of Criminology, 56(1), 21-48.

Williams, M. L., & Levi, M. (2012). Perceptions of the eCrime controllers: Modelling the influence of cooperation and data source factors Security. Journal, doi:10.1057/sj.2012.47.

Wilmot, A. (2005). Designing sampling strategies for qualitative social research: With particular reference to the office for national

statistics' qualitative respondent register. Survey Methodology Bulletin-Office for National Statistics-, 56, 53.

Wilsem van, J. A. (2013). Bought it, but never got it: Assessing risk factors for online consumer fraud victimization. European Sociologic Review, 29(2), 168-178.

Wisdom, K. (2012). The impact of electronic banking on service delivery to customers of Ghana commercial bank limited (Ph.D. Thesis,).

Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. The CPA Journal, 74(12), 38-42.

World Bank. (Ed.). (2014). Cyber security: A model for protecting the network World Bank.

Wothke, W. (2000). Longitudinal and multi-group modeling with missing data. In T. D. Little, K. U. Schnabel & J. Baumert (Eds.), Modeling longitudinal and multiple group data: Practical issues, applied approaches and specific examples. Mahwah, New Jersey: Lawrence Erlbaum Associates.

Wothke, W. A. (1993). Wothke, W. A. (1993). nonpositive definite matrices in structural modeling. in (eds.), (pp. 256– 293) 3, 4, 5, 9. In K. A. Bollen, & Long J. S. (Eds.), Testing structural equation models. Newbury Park,: CA: Sage.

Wright, R. (2007). Developing effective tools to manage the risk of damage caused by economically motivated crime fraud. Journal of Financial Crime, 14(1), 17-27.

Yan, A. W., Md-Nor, K., Abu-Shanab, E., & Sutanonpaiboon, J. (2009). Factors that affect mobile telephone users to use mobile payment solution. International Journal of Economics and Management, 3(1), 37-49.

Yan, W. N., & Chiu, D. K. (2007). (2007). Enhancing e-commerce processes with alerts and web services: A case study on online credit card payment notification. Paper presented at the Machine Learning and Cybernetics, 2007 International Conference on, 7 3831-3837.

Yar, M. (2005). The novelty of 'Cybercrime' an assessment in light of routine activity theory. European Journal of Criminology, 2(4), 407-427.

Yar, M. (2005). The novelty of cybercrime: An assessment in light of routine activity theory. , 2(4), 407–427. European Journal of Criminology, 2(4), 407-427.

Yazdanifard, R., WanYusoff , W. F., Behora, A. C., & Abu Bakar Sade. (2011). Electronic banking fraud; the need to enhance security and customer trust in online banking. International Journal in Advances in Information Sciences and Service Sciences, 3(10.61), 505-509.

Zahra, S., Priem, R., & Rasheed, A. (2005). The antecedents and consequences of top management fraud. Journal of Management, 31(6), 803-828.

Zhang, W., Zhang, Y., & Kim, T. (2014). Detecting bad information in mobile wireless networks based on the wireless application protocol. Computing. Archives for Informatics and Numerical Computation, 96(9), 855-874. doi:http://dx.doi.org/10.1007/s00607-013-0325-1

Zimucha, T., Zanamwe, N., Chimwayi, K., Chakwizira, E., Mapungwana, P., & Maduku, T. (2012). An evaluation of the effectiveness of E-banking security strategies in Zimbabwe: A case study of Zimbabwean commercial banks. Journal of Internet Banking and Commerce, 17(3), 1-16.