Chapter One

Introduction

1.1 Background to the Study

Fraud is ostensibly a growing problem in Nigeria, holding back the country's growth, breaking trust, and damaging society. It is affecting both government offices and businesses, leading to lost chances and less confidence. This issue is getting worse, with large amounts of money being lost to fraud and it seems to be leaving many in despair. While technology and globalization offer new opportunities, they also make it easier for fraudsters to use more complex methods that may destabilize people and institutions. Fraud is basically when someone uses trickery or lies to get someone else to give up something valuable or their legal rights. It often happens through dishonest business practices, with the intention to break the law or damage trust. This can include hiding the true purpose of an action, lying to mislead the victim, or covering up the fraud once it happens.

In Nigeria, fraudsters are constantly finding new ways to take advantage of people's weaknesses. While the systems have its flaws, different agencies approach fraud investigations in different ways. Each agency has its own role and methods based on what it is responsible for. Some focus on ensuring people follow regulations, pay taxes, or adhere to specific rules. In these cases, those involved in fraud might avoid criminal charges by paying fines or settling through other administrative measures. For example, a tax agency might drop criminal charges if the person agrees to pay their overdue taxes with interest and penalties. This situation appears to highlights the need for thorough research to understand the growing and changing patterns of fraud.

Lead City University Ibadan DO NOT COPY

Agencies involved in fraud investigations have a wide range of powers, but these powers vary significantly between organizations and when multiple agencies work together, deciding which one should take the lead can be difficult, especially if their powers don't align well. Research showed that there were 26,182 reported attempts of fraud and forgery in 2017, an increase from the 16,751 cases in 2016, that year, fraud led to an actual financial loss of about N2.4 billion and the Nigeria Deposit Insurance Corporation records also reveal that technology-based financial platforms are particularly vulnerable, accounting for a large share of the fraud cases and related losses[1].

To effectively combat financial crime and corruption, Nigeria established the Economic and Financial Crime Commission and Independent Corrupt Practices and Other Related Offences Commission with distinct roles. The EFCC is responsible for investigating financial crimes like money laundering and fraud, while the ICPC primarily focuses on public sector corruption, addressing issues like bribery, graft, and misuse of office. However, the ICPC's role is limited by its mandate, which focuses more on advising public officers on anti-corruption practices than on conducting deep investigations or prosecutions. The EFCC, on the other hand, has broader powers under its founding law, allowing it to investigate, prevent, and prosecute a wide range of financial crimes. Its mandate includes enforcing all laws related to economic and financial crimes and using advanced methods for investigation and prevention.

This extensive scope makes the EFCC a key player in Nigeria's anti-corruption efforts, allowing it to address crimes beyond corruption, including terrorism financing. Although the EFCC can pursue assets gained through terrorism or economic crimes, a separate law assigns

Lead City University Ibadan DO NOT COPY

the primary responsibility for counterterrorism to the police. Despite the EFCC and police both having significant powers, their effectiveness relies on close collaboration.

To help fight financial crime and corruption, Chapter 38 of the Nigerian Criminal Code addresses obtaining property through false pretences and cheating and Section 418 of the Code defines "false pretences" as any claim—through words, writing, or actions—about a past or present fact that is knowingly false or misleading, Section 419 went further to focus specifically on fraudsters, stating that anyone who, with the intent to defraud, uses false pretences to obtain something that can be stolen, or persuades someone to hand over such property, commits a felony and could face up to three years in prison. This is why fraud, especially scams involving deceit, is commonly referred to as "419," though it doesn't mean these crimes are unique to Nigeria or only involve Nigerians[2].

Nigeria's Cybercrimes Prohibition and Prevention Act of 2015 sets penalties for cyber fraud, where section 14(2) stipulates that anyone who sends an electronic message with the intent to defraud by misrepresenting facts—causing the recipient or another person harm or financial loss—commits a crime and If convicted, the person could face at least five years in prison with a fine of at least N10 million, or both[3].

This study is tilted towards fraud investigations carried out by the Nigeria Security and Civil Defence Corps (NSCDC), an agency that has not received substantial intellectual and academic attention in the area of fraud investigation and its outcomes. While other agencies such as the Nigerian Police Force (NPF), the Economic and Financial Crimes Commission (EFCC), the National Financial Intelligence Unit (NFIU), and the Independent Corrupt Practices and Other Related Offences Commission (ICPC) have been the subject of

Lead City University Ibadan DO NOT COPY

numerous studies, the NSCDC's role in fraud detection and prosecution has largely been overlooked. According to Section 3 (1) (f) (iii) of the Nigeria Security and Civil Defence Corps (Amendment) Act, 2007, fraud investigation is one of its critical mandates. Understanding how the agency executes this responsibility is essential, especially considering the evolving nature of fraud and its impact on Nigeria's security and economy[4].

The NSCDC has the authority to arrest, detain, and prosecute individuals involved in fraudulent activities, making it a key player in safeguarding public trust and securing public assets. Despite its important role, the challenges and obstacles the NSCDC faces in carrying out its fraud investigation mandate remain underexplored and this study aims to fill this gap by critically examining the methods, successes, and difficulties encountered by the NSCDC in addressing fraud, and by understanding its overall contribution to Nigeria's broader anti-fraud efforts[4].

The Nigeria Security and Civil Defence Corps (NSCDC) was originally founded in 1967 during the Nigerian-Biafran Civil War as the Lagos Civil Defence Committee. It operated in Lagos, the then Federal Capital Territory, with a mission to protect and educate civilians. The Corps ran programs to raise awareness about possible attacks from the Biafran army and advised residents on staying safe, as most people in Lagos lacked knowledge about wartime dangers.

In 1984, the NSCDC evolved into a national security agency, and by 1988, it expanded further by setting up Commands across Nigeria, including in Abuja, now the Federal Capital Territory. This expansion broadened the Corps' role, and in 2003, it gained formal legal status through an Act signed by President Olusegun Obasanjo. An amendment to this Act in

Lead City University Ibadan DO NOT COPY

2007 strengthened the NSCDC's mandate to protect public infrastructure, manage crises, and address security concerns. The 2007 changes also gave the Corps authority to conduct surveillance, search properties, seize materials linked to vandalism, and prosecute suspects. Today, the NSCDC plays a crucial role in internal security, infrastructure protection, emergency response, and overseeing private security firms. It is also empowered to combat fraud—a significant addition to its duties. The Corps has proven effective in many areas, including surveillance, patrol, arrests, investigations, detaining vandals, and even prosecuting offenders[5].

On July 27, 2010, the Anti-Fraud Unit of the Nigerian Security and Civil Defence Corps (NSCDC) made a significant breakthrough in the fight against fraud by arresting 69 individuals who were falsely posing as members of the National Youth Service Corps (NYSC). These suspects were found at an unauthorized orientation camp, where they were involved in a well-organized scheme intended to deceive both authorities and the public. This operation highlighted the NSCDC's commitment to fighting fraud nationwide, showcasing the vigilance and effectiveness of its Anti-Fraud Unit. The successful raid also served as a strong warning against impersonation and fraudulent schemes in Nigeria[6].

It is worthy of mention that the formation and training of the Anti-Fraud Unit were initially supported by the EFCC, whose personnel trained NSCDC officers in key investigative skills and this early support helped the NSCDC establish a capable anti-fraud team that can operate independently. Despite its lower profile, the NSCDC Anti-Fraud Unit, Oyo State, have been handling many fraud investigations and prosecutions effectively, working as a complementary force to the EFCC, even though the EFCC seems to be facing a heavy

Lead City University Ibadan DO NOT COPY

caseload, further empowering the NSCDC's Anti-Fraud Unit could ease this burden and create a more balanced approach to fighting financial crime in Nigeria.

This study highlights the often-overlooked role of the Anti-Fraud Unit of the Nigerian Security and Civil Defence Corps (NSCDC) in fighting fraud in Nigeria and highlight the valuable contributions of the NSCDC's Anti-Fraud Unit, filling a gap in existing research and advocating for more support to unlock its full potential as a crucial partner in Nigeria's fight against fraud.

1.2 Statement of the Problem

Fraud has become a major and ongoing threat in Nigeria, affecting many sectors of society. As fraud become more complex, investigating and prosecuting this menace seems to has become more challenging. This requires not just traditional methods but also innovative and persistent efforts. While much of the focus in Nigeria's fight against fraud has been on agencies, such as EFCC, ICPC, and NPF, the role and effort of the Nigeria Security and Civil Defence Corps (NSCDC), specifically its Anti-Fraud Unit, has remained largely understudied and overlooked.

The pilot phase of this study shows that the NSCDC Anti-Fraud Unit has the capacity to make a significant impact, but its work remains largely unrecognized and underappreciated. Understanding how the unit operates, the obstacles it faces, and the effectiveness of its strategies is crucial to ensuring it can fulfil its potential in Nigeria's broader anti-fraud framework. Also, pilot studies reveal that this unit has quietly grown into a competent force that investigates and prosecutes fraud, particularly with a focus on administrative efficiency.

Lead City University Ibadan DO NOT COPY

However, despite its capacity and mandate, it operates with limited resources and little public visibility and its efforts are hindered by insufficient resources, limited public awareness, and a lack of institutional support. This lack of recognition has resulted in the unit being underutilized and underfunded, preventing it from reaching its full potential in Nigeria's fight against fraud and the over-reliance on larger agencies, has resulted in strained resources, case backlogs, and delays in prosecuting fraud cases, leaving a gap in Nigeria's overall anti-fraud efforts. Despite facing these challenges, the NSCDC Anti-Fraud Unit continues to contribute to tackling fraud, demonstrating its ability to alleviate some of the pressure on larger agencies.

1.3 Aim and Objectives of the Study

The study aims to interrogate how fraud is investigated and prosecuted by the Nigerian Security and Civil Defence Corps, Oyo State Command. Specifically, the study objectives were to:

i. investigate the dynamics of fraud prosecuted by NSCDC in Ibadan;
ii. examine the cost of fraud prosecution and how it affects investigation strategies and outcomes;
iii. interrogate the tactics and strategies utilized in perpetrating fraud;
iv. characterizes fraud perpetrators investigated by NSCDC Oyo State Command;
v. examine fraud patterns and time of occurrence.

1.4 Research Questions

To guide the research, the study seeks answers to the following questions:

Lead City University Ibadan DO NOT COPY

1. What are the dynamics of fraud occurrence within the NSCDC dataset in Ibadan, Nigeria?
2. How does the cost of prosecuting fraud cases affect the strategies and outcomes of investigations conducted by the NSCDC?
3. What tactics and strategies are commonly used in perpetrating fraud?
4. Who are the individuals or entities typically involved in committing fraud, and what are their characteristics?
5. Are there specific timeframes or patterns in the occurrence of fraudulent activities within the NSCDC dataset?

1.5 Significance of the Study

The significance of this study lies in its potential to make both practical and academic contributions to the field of fraud investigation within Nigeria's criminal justice system. While the Economic and Financial Crimes Commission (EFCC) is widely recognized for its role in tackling fraud and financial crimes, the Anti-Fraud Unit of the Nigerian Security and Civil Defence Corps (NSCDC) remains relatively unknown, especially at the state level. By focusing on the NSCDC's Anti-Fraud Unit in Ibadan, this study fills an important knowledge gap on the role, effectiveness, and challenges faced by this crucial but often overlooked part of Nigeria's anti-fraud efforts.

Beyond its practical and academic value, this study offers a unique perspective on the dynamics of fraud investigated and prosecuted in the Ibadan Command of NSCDC. While much of the research on fraud in Nigeria has focused on high-profile cases handled by the EFCC, this study highlights another important aspect of low-profile cases perpetrated by

Lead City University Ibadan DO NOT COPY

ordinary Nigerians. This approach deepens our understanding of how fraud operates at different levels in the society. The findings will inform policymakers about the critical need for better resource allocation and support for the unit, offering practical insights into how limited resources affect case outcomes and can undermine anti-fraud efforts.

As fraud tactics evolve rapidly, often outpacing the regulations designed to combat them, understanding these strategies is crucial for developing effective countermeasures and training NSCDC Anti-Fraud personnel to anticipate and respond to emerging forms of fraud. This study contributes to the broader field of criminal methodology, particularly within the Nigerian context, where regional differences in fraud tactics may reflect unique socio-economic and cultural factors.

This study also provides valuable insights into the profiles of individuals and entities involved in fraud, drawing from the NSCDC dataset. By analysing the characteristics of fraud perpetrators, such as their behaviour patterns, socio-economic backgrounds, and motivations, the research helps identify key trends that can inform risk assessment and fraud prevention efforts.

Understanding who the fraudsters are can lead to targeted interventions, educational campaigns, and preventive measures that address the underlying causes of fraud. This aspect of the study is crucial not only for improving investigations but also for empowering the public to recognize and avoid fraudulent activities.

Academically, the study enriches the understanding of fraud investigation within Nigeria's criminal justice system. By focusing on the NSCDC's Anti-Fraud Unit, it challenges the

Lead City University Ibadan DO NOT COPY

common focus on the EFCC, and highlights the importance of inter-agency collaboration in combating fraud. The study emphasizes the need for a multi-layered approach that leverages the strengths of all relevant agencies to fight fraud effectively.

The research underscores the potential for the NSCDC's Anti-Fraud Unit to play a bigger role in Nigeria's anti-fraud efforts, particularly if it receives more support and recognition. With the EFCC burdened by a large caseload, empowering the NSCDC's unit could help distribute the workload, leading to more efficient fraud detection and prosecution across the country.

This study advocates for a broader vision of anti-fraud work in Nigeria, proposing that with additional resources, strategic collaboration, and greater public awareness, the NSCDC could become a central player in the national fight against fraud. The study not only offers practical recommendations for strengthening the NSCDC's Anti-Fraud Unit but also contributes academically by exploring fraud dynamics within a multi-agency framework. By addressing both theoretical and practical aspects, this research has the potential to influence policy, improve resource allocation, and ultimately contribute to a more effective criminal justice system in Nigeria.

1.6 Scope of the Study

This study focuses on the prosecution of fraud cases by Oyo State Command of the NSCDC, Ibadan, as a major urban centre with a high incidence of diverse fraud activities, provides an ideal setting for exploring local fraud dynamics. The study covers essential aspects of fraud investigation and prosecution as managed by the NSCDC's Anti-Fraud Unit, analysing fraud

Lead City University Ibadan DO NOT COPY

patterns within the NSCDC dataset, including the types of cases handled, the profiles of offenders and victims, and the tactics employed by fraudsters. It further investigates the administrative methods used for prosecutions and the financial and resource limitations that impact the Unit's effectiveness. This study covers the investigation of fraud by the Nigerian Security and Civil Defence Corps (NSCDC) Anti-Fraud Unit, focusing on the most occurring cases handled from 2021 to 2024. It explores the contributions of seven (7) detectives who were actively involved in these investigations in the Anti-Fraud Unit, analysing their strategies, challenges, and the outcomes of the fraud cases they prosecuted during this period.

1.7 Limitation of the Study

This study has several limitations that affect its scope and depth. First, it focuses solely on the operations of the Nigerian Security and Civil Defence Corps (NSCDC) Anti-Fraud Unit in Oyo State. While this allows for a detailed analysis of their strategies and challenges, it limits the ability to apply the findings to other states in Nigeria, where fraud patterns, available resources, and institutional practices might differ. One significant challenge was the lack of existing literature on the NSCDC Anti-Fraud Unit. Unlike other prominent anti-fraud agencies in Nigeria, such as the EFCC, ICPC and NFIU, the NSCDC's Anti-Fraud Unit has received little academic attention. This lack of prior research made it difficult to build on existing knowledge and required the study to establish foundational insights. Similarly, there was a scarcity of recent and comprehensive information about the unit's activities, making it challenging to analyse current trends or outcomes in fraud investigation and prosecution. Despite these limitations, the study offers valuable insights into the NSCDC Anti-Fraud Unit's work. Future research should address these gaps by covering more geographic areas

Lead City University Ibadan DO NOT COPY

and this would provide a more comprehensive understanding of the fight against fraud in Nigeria.

1.8 Operational Definition of Terms

Anti-Fraud Unit: This refers to a specialized division within the NSCDC Oyo State Command focused on identifying, investigating, and prosecuting fraud-related activities.

Fraud: This refers to the deliberate act of deception or misrepresentation aimed at gaining financial or material benefits without authorization. It includes various forms, such as financial scams, identity theft, forgery, embezzlement, and other types of fraud documented in the Oyo State Command's investigations.

Investigation: This refers to the organized steps taken by the NSCDC Anti-Fraud Unit in Oyo State to uncover, collect, and evaluate evidence linked to suspected fraud cases.

Prosecution: This refers to the legal process the NSCDC Anti-Fraud Unit in Oyo State uses to officially charge individuals or organizations involved in fraud. This may include applying administrative penalties or pursuing court action to ensure offenders are held accountable.

Lead City University Ibadan DO NOT COPY

Endnotes

1. O. Tade & O. Adeniyi, *Dimensions of Electronic Fraud and Governance of Trust in Nigeria's Cashless Ecosystem*. **International Journal of Offender Therapy and Comparative Criminology,** 64(16) 2020, 1717-1740.

2. O. Tade, *COVID-'419': Social Context of Cybercrime in the Age of covid-19 in Nigeria.* **African Security** 14 (4), 2021, 460-483.

3. *Federal Republic of Nigeria, Cybercrimes. Prohibition, Prevention etc. Act, 2015*. https://www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__ _ Act__.pdf.2015

4. U. T. Akpoghome, & C. N. Theophilus, *The Collaboration of Investigative Authorities in Nigeria–Current Issues and Challenges*, **International Journal of Law** 3(4), 2017, 39-48.

5. H. Egodo, I. Lucky, B. B. Eyong, & A.S. Sampson, *Nigeria Security and Civil Defence Corps (NSCDC) Mandate and Infrastructural Protection in Cross River State, Nigeria*. **International Journal of Multidisciplinary Research and Growth Evaluation**, 2022

6. C. Okafor, & J. K. Ani, *The National Youth Service Corps Programme and Growing Security Threat in Nigeria,* **Africa's Public Service Delivery & Performance Review**, 2(2), 2014, 149-164.

Lead City University Ibadan DO NOT COPY

Chapter Two

Literature Review

2.1 Conceptual Review

This chapter provides an overview of existing knowledge on fraud investigation and prosecution, summarizing previous research to identify key perspectives, ongoing debates, and gaps in the field. Reviewing relevant literature is a crucial step in any research, as it helps establish a foundation for new insights and positions the study within broader academic discussions. For this study, the literature review focuses on the role of the Nigerian Security and Civil Defence Corps (NSCDC), particularly the Anti-Fraud Unit in Oyo State, in combating fraud. It examines prior research on fraud investigation and prosecution, as well as the contributions of agencies like the NSCDC, to understand the challenges, successes, and strategies involved in handling fraud cases in Nigeria. Additionally, the review looks into the administrative, legal, and operational frameworks that guide the Anti-Fraud Unit, showing how the NSCDC contributes to the broader fight against fraud in the country.

Criminologists and fraud investigators have long debated the best methods for detecting and prosecuting fraud, with some supporting comprehensive criminal procedures and others favouring quicker administrative sanctions. This literature review explores key themes relevant to the NSCDC's Anti-Fraud Unit, such as the evolution of fraud, the importance of inter-agency collaboration, the socio-economic factors that shape fraud patterns, and the theoretical frameworks guiding current investigative practices. Organized thematically, this

Lead City University Ibadan DO NOT COPY

review covers the nature of fraud in Nigeria, institutional responses, the operational roles and challenges faced by the NSCDC's Anti-Fraud Unit, and relevant criminological theories. Together, these themes provide a foundation for understanding fraud investigation and prosecution within the NSCDC's Oyo State Command.

2.1.1 Concept of Fraud

Fraud is a widespread and complex issue affecting institutions globally, cutting across cultural, economic, and geographical divides. Both public and private organizations face significant challenges in identifying and addressing these forms of fraud. It involves intentional deception aimed at securing financial or personal gain and includes activities like embezzlement, identity theft, bribery, forgery, cybercrime, and other illegal acts that disrupt the integrity of financial and operational systems[1].

Fraud has far-reaching impacts, causing significant financial losses, eroding public trust in institutions, weakening ethical standards, and hindering socio-economic progress. Globally, fraud takes on various forms, shaped by the socio-economic and technological landscape of each region. In the Global West—mainly the U.S., Canada, and Western Europe—fraud is heavily influenced by advanced digital infrastructure, complex financial networks, and globalization. These factors have led to sophisticated schemes, especially in cybercrime, securities fraud, and corporate fraud. The scale and intricacy of fraud cases in these regions highlight the weaknesses in interconnected financial systems and the role of technology in enabling cross-border crime[2].

In Western countries, the widespread use of digital transactions, online banking, and automated financial systems has increased the risk of cyber-enabled fraud[3]. This type of fraud, often executed by individuals or organized criminal networks, includes tactics like

Lead City University Ibadan DO NOT COPY

phishing, malware attacks, and ransomware. As technology advances, so do these crimes, which now employ highly sophisticated methods to evade detection and target large corporations, small businesses, and individuals alike. The dependence on technology in these economies has thus created both opportunities and challenges in fraud prevention, making it essential for cybersecurity measures to continually adapt to stay one step ahead of fraudster.

Corporate Fraud is seen as an unlawful any actions by people within a company aimed at deceiving stakeholders or gaining financial benefits. This can include practices like falsifying accounts, insider trading, and embezzlement. Recent studies suggest that corporate fraud often arises from internal problems within companies, such as weak governance or ineffective internal controls. Major corporate collapses caused by fraudulent accounting practices not only lead to huge financial losses but also erode public confidence in financial markets[4].

Securities fraud, such as Ponzi schemes and insider trading, has been particularly common in the West, largely due to the complexity of financial markets. In the U.S. and Western Europe, fraud cases have often involved high-profile schemes that mislead investors with promises of large returns. The 2008 financial crisis highlighted the far-reaching impact of securities fraud and spurred the introduction of stricter regulations, like the Dodd-Frank Act in the U.S., which aims to curb deceptive practices in financial markets[5].

Cyber fraud is especially common in the West due to widespread digital engagement. One of the most frequent forms is identity theft, where criminals steal personal information to access financial accounts or make unauthorized purchases. Identity theft is one of the fastest-growing types of fraud in the U.S., fuelled by digital advancements that make personal data more accessible and vulnerable to exploitation[6]. Healthcare and insurance fraud are also a

Lead City University Ibadan DO NOT COPY

major concern in Western economies, involving practices like billing for services that were not provided, inflating medical costs, and making fraudulent insurance claims. In the U.S. alone, healthcare fraud is estimated by the FBI to cost the nation tens of billions of dollars each year and this type of fraud not only raises expenses for patients and insurers but also harms the quality of care, as funds are siphoned away from genuine medical needs to fraudulent activities[7].

In the Global West, fraud schemes are often highly sophisticated, taking advantage of advanced technology, social manipulation, and vulnerabilities within systems and the common tactics used by fraudsters include phishing, spoofing, and ransomware attacks to gain unauthorized access to financial information. For instance, in a ransomware attack, hackers lock a victim's data through encryption and then demand a ransom to unlock it, which makes this approach to have been increasingly directed at businesses, local governments, and healthcare facilities, putting victims in a difficult position: either pay the large ransom or risk losing critical data altogether[8].

Social engineering is a tactic used by fraudsters to trick individuals into disclosing personal or sensitive information. Instead of relying on technical vulnerabilities, this approach takes advantage of human behaviour, making it harder to detect or stop and in the Western countries, where people's digital knowledge can differ greatly, these scams are particularly successful and that makes fraudsters to often pretend to be trusted figures like government agents or bank representatives to build trust and gain access to private information[2].

The main factors driving fraud in the West often include economic pressures, technological opportunities, and weaknesses within organizations**.** Financial struggles like recessions, unemployment, or personal debt can push people to commit fraud. Weaknesses within

Lead City University Ibadan DO NOT COPY

organizations, such as poor internal controls and a lack of transparency, also make it easier for fraud to take hold[1]. Gaps in regulations and weak governance structures give fraudsters further opportunities to take advantage of vulnerabilities in financial systems[5].

Fraud has significant and wide-ranging effects on Western economies, impacting individuals, businesses, and governments alike and the financial losses from fraud are estimated to be in the billions, undermining consumer confidence, reducing business profits, and destabilizing the economy. For instance, in the U.S., the Association of Certified Fraud Examiners (ACFE) reported in 2022 that occupational fraud costs organizations about 5% of their annual revenue and this highlights the urgent need for strong fraud prevention strategies and effective regulatory systems[6].

Fraud also has a significant impact on society by eroding public trust. When major fraud cases, like corporate embezzlement or healthcare scams, come to light, they can diminish people's confidence in institutions, and this loss of trust can have far-reaching effects, including reduced investor confidence in financial markets and a decline in consumers' willingness to engage in digital transactions. Studies show that high-profile fraud cases in the West often prompt regulatory changes, such as the Sarbanes-Oxley Act and the Dodd-Frank Act in the United States, which are designed to improve corporate accountability and transparency[9].

Fraud in Nigeria typically involves more opportunistic and grassroots-level scams, whereas in the West, it is often more organized and technologically advanced, taking advantage of systemic weaknesses. Despite these differences, both contexts share common drivers, such as economic pressures and the exploitation of regulatory gaps. The heavy reliance on advanced technology and complex financial systems in the West has created unique challenges,

Lead City University Ibadan DO NOT COPY

requiring specialized fraud prevention techniques, such as advanced cybersecurity and AI-driven fraud detection. On the other hand, Nigeria's approach tends to focus more on human-centred strategies, such as awareness campaigns and direct interventions by agencies like the NSCDC.

2.1.2 Historical Context: A Brief History of Fraud Issues in Nigeria's Public Sector

Fraud in Nigeria's public sector has a long and complicated history, shaped by both the country's past and its political environment. The word "fraud" comes from the Latin term *fraus*, which means deceit or trickery. In Nigeria's public sector, fraud refers to the deliberate act of deceiving others to gain financial or personal benefit, often harming the public in the process. Over the years, Nigeria's diverse political landscape has struggled with fraud, with numerous scandals exposing the depth of corruption and its negative effects on government operations, the economy, and public trust.

The origins of fraudulent practices in Nigeria's public sector can be traced back to the colonial era. During British rule, the Nigerian administration was highly centralized, with colonial officers holding almost complete control over financial and administrative matters. The lack of transparency and accountability at that time opened the door for small-scale corruption and the misappropriation of public resources. While large-scale fraud wasn't as prevalent during this period, the groundwork for systemic fraud within government structures was set, as the colonial administration often operated with little regard for the needs or interests of the local population. Colonial policies were primarily focused on resource extraction and maintaining control, rather than ensuring fair distribution of resources, which

Lead City University Ibadan DO NOT COPY

makes this approach inadvertently encouraged a culture of corruption among local administrators, who were expected to prioritize the interests of the colonial powers over those of the local population and as a result, the foundation for corrupt practices was established, as officials sought to exploit their positions for personal gain[10].

After Nigeria gained independence in 1960, the public sector saw significant expansion. The new government took over many public enterprises, and the bureaucratic system grew quickly to meet the rising demands for public services. However, this period also marked the beginning of widespread fraud. Many public officials, without strong governance structures in place, began exploiting their positions for personal benefit. As government institutions grew, the lack of effective oversight allowed embezzlement, bribery, and other fraudulent activities to flourish. The 1960s and 1970s in Nigeria were marked by political instability, particularly due to military coups in 1966, 1975, and 1983. These disruptions not only undermined the democratic process but also created an environment conducive to corruption in the public sector. The military regimes, often lacking institutional accountability, allowed public officials to engage in fraudulent activities with little fear of consequences. Frequent changes in leadership, coupled with the absence of democratic checks and balances, made public institutions more susceptible to manipulation. A prime example of this corruption was the Nigerian National Petroleum Corporation (NNPC), a state-owned entity responsible for managing the country's oil resources. During this period, billions of dollars were embezzled through fraudulent schemes, highlighting the systemic corruption within key state-owned enterprises[11].

The 1970s and 1980s were marked by an increase in fraud within Nigeria's public sector, particularly under the military leadership of General Yakubu Gowon and General Sani

Lead City University Ibadan DO NOT COPY

Abacha. During these years, large-scale financial mismanagement became widespread, with public officials embezzling funds that were meant for national development. One of the most glaring examples of this was the mismanagement of oil revenues. Instead of being used to fuel the country's economic growth, these funds were siphoned off through fraudulent schemes, benefiting a few individuals while deepening the economic disparities across the nation. This period solidified the perception of widespread corruption within the public sector and further eroded trust in government institutions[12].

Nigeria's return to civilian rule in 1999 under President Olusegun Obasanjo marked a hopeful turning point in the country's struggle against corruption in the public sector. A key step in this new phase was the establishment of the Economic and Financial Crimes Commission (EFCC) in 2003, a government agency designed to investigate and prosecute financial crimes, including fraud. The creation of the EFCC was seen as a significant move towards curbing public sector corruption. However, despite this initiative, fraud within Nigeria's public institutions persisted. It quickly became clear that the country's institutions were still hindered by weak oversight, poor governance, and deeply rooted systemic corruption, which made these challenges to underscored the difficulty of enacting real change, as public officials continued to exploit their positions for personal gain.

In the early 2000s, procurement fraud became a major issue within Nigeria's public sector. Public officials often awarded government contracts to their friends, family members, and allies, bypassing proper bidding processes. This led to inflated contract prices and the delivery of substandard work. One of the most notorious cases of procurement fraud occurred during the Obasanjo administration, where billions of naira were embezzled through fraudulent contracts in the power sector. The corrupt practices not only drained public funds

Lead City University Ibadan DO NOT COPY

but also delayed the development of critical services like electricity and infrastructure, which were essential for Nigeria's economic growth and progress[13].

In the 2000s, another major form of fraud in Nigeria's public sector was the abuse of office for personal gain. Politicians and public servants often engaged in "gatekeeping" or "kickback" schemes, where they used their positions to demand bribes or payments from contractors or businesses seeking government contracts. This practice became so widespread that it became deeply ingrained in many regions of the country. The lack of transparency in public procurement processes and the absence of a solid regulatory framework made it difficult to detect and stop such corrupt practices[5].

In the past decade, there have been some positive steps taken to fight fraud in Nigeria's public sector. The government introduced measures like the Treasury Single Account (TSA) to consolidate government revenues and minimize the risk of embezzlement. Additionally, the creation of the Nigerian Extractive Industries Transparency Initiative (NEITI) helped improve transparency in the oil and gas sector, ensuring that more of Nigeria's oil wealth was used for national development. However, despite these efforts, fraud remains a persistent problem. The increasing use of digital platforms and financial technologies in Nigeria has led to a rise in cyber fraud, which presents new challenges in the ongoing fight against corruption.

Cybercrime, especially online banking fraud, is becoming an increasingly serious issue in Nigeria's public sector. With the growing use of digital financial platforms, fraudsters are exploiting these technologies to scam government employees and public sector organizations. The widespread use of mobile phones and the internet for financial transactions has made it easier for criminals to take advantage of vulnerabilities in cybersecurity, leading to a rise in

Lead City University Ibadan DO NOT COPY

fraudulent activities within the public sector[14]. A major challenge in fighting fraud in Nigeria's public sector is the lack of coordination and resources among the agencies responsible for tackling corruption. While organizations like the EFCC and the ICPC have made progress, their efforts are often hindered by limited funding, political interference, and inefficiencies within the bureaucracy. Additionally, without a unified strategy to combat fraud, these agencies often operate independently of one another, which reduces the overall impact of anti-fraud measures. In recent years, Nigeria has received support from international organizations like the United Nations and the World Bank in its fight against fraud. These partnerships have helped improve anti-corruption frameworks and strengthen institutional capacity. However, significant challenges persist. Despite these collaborations, Nigeria still faces a need for comprehensive reforms that tackle the root causes of fraud and there is a pressing need to enhance accountability, increase transparency in public sector operations, and address systemic issues that allow fraud to thrive, which will require not only boosting the capabilities of anti-corruption agencies but also raising public awareness and cultivating a culture of responsibility and integrity within all levels of government.

2.1.3 Prosecution of Fraud

Prosecuting fraud is a complex process that aims to hold individuals or organizations accountable for fraudulent activities through the legal system. In the retributive and deterrence parlance, successful prosecution serves a dual purpose: it provides justice for victims and discourages others from engaging in similar crimes. However, prosecuting fraud presents unique challenges due to the intricate nature of the evidence involved, the need to coordinate across different jurisdictions, and the sophisticated methods often used in

Lead City University Ibadan DO NOT COPY

fraudulent schemes. Fraud cases may require extensive investigation and expert testimony to clarify complex financial or digital evidence, adding layers of difficulty for prosecutors[15].

Successful fraud prosecution relies on a well-coordinated approach that combines thorough investigations, adequate legal resources, specialized expertise, and often collaboration between different agencies. Recent research highlights the importance of enhancing prosecutorial methods and creating more efficient processes to handle fraud cases that may span multiple jurisdictions and this involves training prosecutors in complex fraud tactics, developing stronger investigative tools, and fostering communication between agencies to build solid cases against offenders[16]. A major hurdle in prosecuting fraud cases is the complexity of the evidence involved, because, in contemporary times, fraud cases often include a web of financial transactions, digital communications, and various documents that require careful analysis to prove intent and establish guilt.

Given the detailed nature of financial and cyber fraud, gathering and presenting evidence that meets the legal requirements for prosecution can be both resource-intensive and technically challenging. This complexity calls for specialized expertise and significant time and resources to build a compelling case that stands up in court[17]. In cyber fraud cases, digital forensics play a crucial role in connecting suspects to specific fraudulent activities. However, these investigations face obstacles like encrypted messages, anonymous transactions, and complex international financial systems. These challenges make it difficult to trace fraudsters and gather the concrete evidence needed for prosecution, often requiring advanced forensic techniques and international cooperation to overcome such sophisticated evasion tactics.

Jurisdictional issues add major complications to prosecuting fraud, especially in cases of cross-border or cyber fraud, because, fraudsters frequently take advantage of differences in

Lead City University Ibadan DO NOT COPY

laws and regulations across countries to avoid prosecution, using offshore accounts and international networks to hide the trail of illegal funds. This exploitation of varying legal systems makes it challenging to hold offenders accountable, often requiring international cooperation and agreements to bridge these legal gaps and pursue justice effectively. In fraud cases that span multiple countries, cooperation between prosecuting agencies is essential. However, this collaboration is often complicated by differences in legal systems and the absence of uniform procedures, especially when Extraction Treaty is at play. These disparities can slow down investigations and make it harder to gather evidence, as each country may have its own standards and protocols. This lack of alignment highlights the need for more standardized international frameworks to facilitate efficient and coordinated responses to cross-border fraud[18]. Initiatives like the European Union's Eurojust and the U.S. Department of Justice's international task forces have made significant strides in improving cross-border collaboration in fraud cases. These organizations help streamline communication and coordination between countries, making it easier to tackle complex cases that cross multiple jurisdictions. However, challenges still persist, as differences in laws, investigative methods, and resource availability can limit the effectiveness of these efforts[19].

Studies have shown that different approaches can be used to prosecute fraud, and these often vary based on the legal framework, available resources, and the type of fraud. For example, financial fraud cases may require specialized financial experts to analyse complex accounting records, while cyber fraud cases rely heavily on digital forensics to trace online transactions. In some countries, dedicated anti-fraud courts or specialized fraud divisions within the prosecution service focus exclusively on handling these cases, allowing for more streamlined processes and quicker resolutions. Additionally, plea bargaining is sometimes used to

Lead City University Ibadan DO NOT COPY

encourage suspects to cooperate with investigations, leading to reduced sentences in exchange for valuable information or recovery of stolen assets.

For Criminal Prosecution, it is the conventional method for addressing fraud, involving the trial of the accused in a criminal court where, upon a guilty verdict, they may face imprisonment, fines, or both. This approach is rigorous because it requires the prosecution to establish the defendant's guilt "beyond a reasonable doubt"—a high standard of proof that demands thorough evidence collection and a convincing presentation in court[20]. While criminal prosecution serves as a strong deterrent against fraud, it also places considerable demands on prosecutorial resources and requires extensive evidence to meet the necessary legal threshold.

Research shows that Civil prosecution provides an alternative in situations where criminal charges are challenging to prove, often because the evidence does not meet the stringent "beyond a reasonable doubt" standard required in criminal cases. In civil cases, victims—typically seeking financial restitution—must only meet the lower standard of "preponderance of the evidence," meaning it's more likely than not that the fraud occurred[21]. This approach enables victims to recover their losses without needing to prove criminal intent. Civil prosecution is especially valuable in corporate and investment fraud cases, where the primary goal is to regain financial damages rather than impose criminal penalties on the offenders. Also, Administrative prosecution has become a popular approach for handling fraud, especially within regulatory systems.

Regulatory bodies like the U.S. Securities and Exchange Commission (SEC) use administrative actions—such as fines, license suspensions, and mandatory corrective actions—to respond to fraudulent activities[22]. This method offers a faster and more resource-

Lead City University Ibadan DO NOT COPY

efficient alternative to criminal trials, particularly useful for smaller cases or regulatory violations that don't demand full court proceedings. Administrative prosecution is often preferred for corporate misconduct or regulatory breaches, where timely penalties can help prevent further issues and deter future violations.

To enhance the effectiveness and efficiency of prosecuting fraud, many countries have established specialized units dedicated to these cases. In the U.S., the Financial Fraud Enforcement Task Force combines resources from multiple agencies to address various forms of financial fraud, including mortgage, securities, and healthcare fraud. Likewise, the United Kingdom's Serious Fraud Office (SFO) is a dedicated agency focused on investigating and prosecuting serious or complex fraud. The SFO has extensive authority to handle high-profile cases of corporate and financial misconduct, enabling it to address some of the most challenging fraud cases[23, 24].

In Nigeria, the Economic and Financial Crimes Commission (EFCC) is the main agency responsible for prosecuting large-scale fraud, while the Nigerian Security and Civil Defence Corps (NSCDC) Anti-Fraud Unit targets smaller-scale, community-level fraud cases and these specialized units enhance fraud prosecution efforts by providing expertise in areas like financial systems, forensic accounting, and regulatory compliance, which increases the likelihood of successful outcomes.

Contemporary technological studies in digitalization show that Advancements in technology have greatly impacted the way fraud is prosecuted, particularly in terms of evidence collection, forensic analysis, and presenting cases in court. Digital forensics has become crucial in fraud investigations, enabling prosecutors to gather evidence from devices, networks, and cloud-based systems to reconstruct fraudulent activities. In cyber fraud cases,

Lead City University Ibadan DO NOT COPY

digital forensics helps investigators trace IP addresses, recover deleted files, and decrypt communications to build a solid chain of evidence[25]. In recent years, Artificial Intelligence (AI) and Machine Learning (ML) tools have been introduced to detect unusual patterns in financial transactions and enhance the accuracy of fraud investigations. AI-driven tools, like predictive analytics, can analyse past data to predict potentially fraudulent activities, which is especially useful in corporate and financial fraud cases[26]. For example, AI tools used by banks and financial institutions can identify red flags, offering actionable leads to prosecutors and enabling them to take pre-emptive action against potential fraud[27].

Regulatory frameworks are essential for supporting fraud prosecution by setting clear guidelines, penalties, and enforcement standards. In the United States, agencies like the Securities and Exchange Commission (SEC) and the Federal Trade Commission (FTC) establish rules for corporate governance and impose penalties for violations. Following the 2008 financial crisis, legislative changes such as the Dodd-Frank Act have strengthened the SEC's ability to pursue fraud cases, particularly in areas like securities and investment fraud[28]. In Nigeria, the Economic and Financial Crimes Commission (EFCC) Act and the Nigerian Security and Civil Defence Corps (NSCDC) Act grant these agencies the authority to prosecute various types of fraud. However, experts argue that Nigeria's regulatory frameworks need further strengthening, especially to tackle emerging forms of fraud such as cybercrime[29]. Strengthening these regulations could improve the effectiveness of agencies like the NSCDC's Anti-Fraud Unit, which often faces challenges such as jurisdictional issues and limited resources in prosecuting local fraud cases, even a more determined and streamlined regulatory frameworks would enable faster prosecutions, reduce case backlogs, and foster better collaboration between agencies[30].

Lead City University Ibadan DO NOT COPY

Plea bargaining and out-of-court settlements are increasingly used in fraud cases to resolve matters more efficiently. In countries like the U.S. and the UK, plea bargains allow defendants to plead guilty in exchange for reduced charges or lighter sentences, helping to save time and resources in the judicial process[31]. While this approach can expedite trials and ensure some level of accountability, it seems to have been leading to lighter punishments, especially in high-profile corporate fraud cases where defendants may seem to get off too easily, meanwhile, fraud prosecution is a complex and ever-evolving field within criminal justice that requires specialized expertise, resources, and collaborative efforts. The challenges involved, such as gathering evidence, dealing with jurisdictional issues, and keeping up with rapid technological changes, make it a particularly demanding area of law. Despite these hurdles, significant progress has been made in improving fraud prosecution through advances in forensic technology, the establishment of specialized prosecutorial units, and the development of stronger regulatory frameworks. In Nigeria, plea bargaining has become more common in recent years, particularly in cases involving public officials or high-profile individuals accused of embezzlement or bribery. This approach can be a practical way to resolve cases that might otherwise drag on for years. However, its use has sparked debates about fairness, with concerns that wealthier defendants may be able to negotiate more favourable deals, which could undermine the justice process[32, 33].

2.1.4 Fraud Investigation

Fraud investigation is one of the trickiest and important aspects of the criminal justice system. It goes beyond merely identifying wrongdoing—it involves methodically sorting out layers of deceit to document and prove fraudulent activities. The ultimate goal is to hold perpetrators accountable, secure justice for victims, and restore trust in affected systems.

Lead City University Ibadan DO NOT COPY

Given the complexities of fraud and its ever-evolving nature, the investigative process serves as a vital pillar in global efforts to combat financial crimes and corruption. Over the years, the range of fraud investigations has stretched out significantly. The traditional focus on straightforward embezzlement or check fraud has shifted to include sophisticated schemes like cyber fraud, financial statement manipulation, procurement fraud, and complex money laundering operations. This evolution has been fuelled by several factors, including technological advancements, the globalization of financial systems, and growing awareness of how deeply fraud impacts economies, institutions, and individuals.

In the Global West, fraud investigations often leverage cutting-edge technology and benefit from well-established legal frameworks. Investigators use artificial intelligence (AI) and machine learning tools to detect anomalies in financial transactions, while blockchain technology aids in tracking and verifying digital assets. For instance, it seems agencies like the Federal Bureau of Investigation (FBI) in the United States and the Serious Fraud Office (SFO) in the United Kingdom employ highly specialized teams trained in digital forensics and financial analysis. These teams collaborate with other governmental and private organizations, creating a multi-pronged approach to investigating fraud.

Nigeria, on the other hand seems to be facing unique challenges in fraud investigation due to systemic corruption, resource constraints, and gaps in regulatory enforcement. However, significant strides have been made in recent years. Agencies like the Economic and Financial Crimes Commission (EFCC) and the Nigerian Security and Civil Defence Corps (NSCDC) Anti-Fraud Unit play a central role in tackling various forms of fraud, from public sector embezzlement to community-level scams. The introduction of technologies such as biometric

Lead City University Ibadan DO NOT COPY

verification in banking and government transactions seems to have also enhanced investigative capacities.

Fraud investigation in Nigeria requires a delicate balance of technical expertise and local knowledge and our Investigators tends to often encounter resistance from well-connected individuals and organizations that use their influence to barricade investigations. As a result, agencies have adopted innovative strategies to uncover hidden assets, they seem to be following complex money trails, and securing critical evidence. Inter-agency collaboration, both locally and internationally, is increasingly important. For instance, Nigerian investigators frequently work with global bodies like Interpol and the United Nations to address cross-border fraud schemes. What seems to make fraud investigation particularly challenging is the sophistication of modern fraudulent schemes. Today's fraudsters are not just individuals but tends to often operate as part of organized networks that exploit loopholes in financial systems and regulatory frameworks. In cyber fraud, for example, perpetrators tend to often use encryption, anonymous transactions, and decentralized platforms to mask their activities. This seems to necessitate the use of advanced digital forensic tools and highly skilled personnel to decode encrypted communications, trace IP addresses, and uncover hidden digital footprints.

Fraud investigations in Nigeria come with a unique blend of challenges and opportunities, shaped by the nation's socio-economic realities, institutional capabilities, and legal systems. The country's fraud landscape is diverse, encompassing both traditional scams, such as identity theft and embezzlement, and more sophisticated, modern forms of fraud like cybercrime and international financial fraud and the key agency spearhead fraud investigations in Nigeria: The Economic and Financial Crimes Commission (EFCC). The

Lead City University Ibadan DO NOT COPY

EFCC is primarily tasked with addressing large-scale and high-profile financial crimes, including corruption, money laundering, and fraud involving public officials or corporate entities.

The challenges in Nigeria's fraud investigations are many-sided. Institutional constraints, such as limited funding, inadequate training, and outdated technology, often hinder the effectiveness of investigative efforts. In addition, systemic corruption can obstruct investigations, particularly when powerful individuals or entities are implicated. Modern fraud schemes, especially cybercrime, pose additional difficulties as fraudsters leverage advanced technologies, decentralized financial systems, and cross-border networks to evade detection.

Despite these obstacles, Nigeria's fraud investigation efforts have also created significant opportunities for reform and innovation. For example, advancements in digital forensics and financial intelligence have bolstered investigators' ability to track money trails, recover stolen assets, and uncover hidden networks. Collaborative efforts between local agencies and international organizations, such as Interpol and the United Nations, have strengthened Nigeria's capacity to address transnational fraud schemes.

The socio-economic context of fraud in Nigeria also shapes investigative priorities. Widespread poverty and unemployment contribute to the prevalence of "yahoo-yahoo" scams, where individuals engage in internet fraud to make quick money and addressing these underlying issues requires a holistic approach that goes beyond enforcement to include economic empowerment, education, and public awareness campaigns.

Lead City University Ibadan DO NOT COPY

The Economic and Financial Crimes Commission (EFCC) and the Nigerian Security and Civil Defence Corps (NSCDC) Anti-Fraud Unit work in tandem to combat fraud, each with distinct but complementary roles. The EFCC is primarily tasked with tackling large-scale and high-profile cases, such as money laundering, corruption, and corporate fraud. In contrast, the NSCDC Anti-Fraud Unit focuses on slighter, sophisticated community-level fraud cases that, while less prominent, have a direct and often significant impact on local communities. This division of responsibilities ensures that no case is overlooked due to its scale. The NSCDC's focus on localized fraud allows it to handle cases that may not meet the EFCC's threshold but are still crucial to maintaining trust and fairness within communities[34]. This specialization creates a more inclusive approach to fraud investigation, ensuring broader coverage across different levels of society.

Collaboration between Nigeria's anti-fraud agencies is essential for effective fraud investigations, especially since their responsibilities often overlap and fraud cases can be highly complex. Agencies like the Economic and Financial Crimes Commission (EFCC) and the Nigerian Security and Civil Defence Corps (NSCDC) frequently work together, sharing resources such as forensic labs and digital investigation tools to strengthen their efforts[35]. However, research shows that this collaboration is not always seamless. Bureaucratic bottlenecks, inadequate funding, and disputes over jurisdiction often create barriers that slow down investigations and reduce their overall impact[36]. Fraud investigations in Nigeria face significant hurdles, including limited budgets, insufficient training, and a lack of modern technology. Fraudsters take advantage of these gaps by using advanced methods to hide their actions and avoid being caught. Additionally, cultural issues like the acceptance of corruption and distrust in law enforcement make it even harder to tackle fraud effectively. To overcome

Lead City University Ibadan DO NOT COPY

these obstacles, Nigeria needs better funding and training, alongside major reforms to boost institutional accountability and rebuild public trust[37].

2.1.5 Nigerian Security and Civil Defence Corps (NSCDC)

The Nigerian Security and Civil Defence Corps (NSCDC) is a vital paramilitary organization dedicated to ensuring public safety, protecting critical infrastructure, and promoting civil stability across Nigeria. Established in 1967 and formally recognized by an Act in 2003, the NSCDC has grown to play a multidimensional role in Nigeria's security corridor. Its responsibilities include safeguarding lives, preventing crime, and protecting key national assets such as oil pipelines, power installations, and telecommunications infrastructure. Over the years, the NSCDC's mandate has expanded to include fraud investigation, the enforcement of private security regulations, and emergency management services. This evolution has positioned the NSCDC as an integral part of Nigeria's security framework. Working closely with other law enforcement and regulatory bodies, the NSCDC contributes significantly to maintaining peace and order while addressing emerging security challenges[38].

The Nigerian Security and Civil Defence Corps (NSCDC) was also established to fill security gaps and support the efforts of the Nigeria Police Force and the military in maintaining peace and order. Its responsibilities span a wide range of activities, including disaster response, riot control, and intelligence gathering, and prosecuting specific crimes such as pipeline vandalism. Empowered by the NSCDC Act, the Corps collaborates with agencies like the Department of Petroleum Resources (DPR) and the Nigeria Maritime Administration and Safety Agency (NIMASA) to investigate and prosecute cases, particularly those related to critical national infrastructure. The NSCDC's origins trace back to the Nigerian Civil War in 1967, when it was formed as the Lagos Civil Defence

Lead City University Ibadan DO NOT COPY

Committee. Initially, its primary role was to educate civilians on safety measures and provide emergency services during the war. As the nation's security needs evolved, the Corps expanded its focus beyond emergency management to address a broader spectrum of security challenges. In 1984, the NSCDC was restructured and given a national mandate, establishing its presence in states across Nigeria. The turning point came in 2003 when the Corps was officially established as a statutory body under the NSCDC Act. This legislation, later amended in 2007, expanded its mandate and enhanced its operational capacity to address emerging security threats more effectively[39].

The Nigerian Security and Civil Defence Corps (NSCDC), operating under the Federal Ministry of Interior, serves as a cornerstone of public safety and national stability in Nigeria. Its responsibilities, as defined by the NSCDC Act of 2007, encompass a wide range of critical functions aimed at safeguarding lives, protecting vital infrastructure, and responding to emergencies. At the heart of its operations is the mission to ensure civilian protection during crises. The NSCDC is equipped to provide emergency response and rescue services, playing a pivotal role in disaster management efforts across the nation. In addition to this humanitarian role, the Corps is tasked with regulating and supervising private security companies. By monitoring these firms, the NSCDC ensures compliance with national standards, promoting professionalism and accountability within the private security sector. The protection of critical infrastructure is another essential function of the NSCDC. With a mandate to maintain round-the-clock surveillance over vital national assets such as oil pipelines, power stations, and telecommunications facilities, the Corps helps to safeguard resources fundamental to Nigeria's economy and security. Collaboration is also a key aspect of the NSCDC's operations. The Corps works in cycle with other security and law

Lead City University Ibadan DO NOT COPY

enforcement agencies to tackle complex threats, including terrorism, vandalism, and other crimes that jeopardize national stability. Through these partnerships, the NSCDC enhances its ability to address multifaceted security challenges effectively.

Moreover, the Corps plays an instrumental role in the fight against economic crimes. Its authority extends to investigating and prosecuting offences such as fraud, vandalism, and the theft of public assets. By addressing these issues, the NSCDC contributes to broader anti-corruption and crime prevention initiatives, bolstering trust in Nigeria's justice system[40]. This agency also plays an important role in keeping the country safe and fighting fraud. However, it faces several difficulties that make its work harder, especially in fraud prevention and investigation. One major challenge is a lack of resources. The NSCDC often doesn't have enough money or modern tools to do its job well. For example, the Anti-Fraud Unit struggles to investigate cybercrimes because it doesn't have advanced equipment or technology needed to track digital activities[41].

Another problem is overlapping duties with other agencies, like the EFCC and the Nigerian Police. These overlaps can cause confusion about who should handle certain cases, leading to delays and wasted efforts. Clearer roles and better teamwork between these agencies could solve this issue. Many people in Nigeria don't fully understand what the NSCDC does, especially in fraud prevention. This lack of awareness means that people don't always report fraud cases to the agency. Without enough reports, it's hard for the NSCDC to act effectively. Building trust and informing the public about the agency's work could help[42].

2.1.6 Fraud Prevalence and Contributing Factors

Lead City University Ibadan DO NOT COPY

As a major problem worldwide, shaped by social, economic, and technological factors. In Nigeria, it is a significant issue that continues to grow in complexity, affecting individuals, businesses, and government institutions alike. Research shows that fraud often flourishes in places where laws are weak, enforcement is poor, and people face financial hardships[43]. Globally, the rise of digital technology has added to the problem, opening doors to cybercrimes like identity theft, phishing, and online financial scams. These crimes take advantage of the fast-paced digital world, making fraud a more urgent challenge to tackle[44].

Economic challenges like instability, unemployment, and poverty are major reasons why fraud occurs. In Nigeria, widespread poverty and joblessness push some people to commit fraud as a way to survive or earn money[45]. These tough economic conditions often make fraud seem like an easy way out for those struggling to make ends meet. The growing use of technology in financial and administrative systems has opened up new opportunities for fraud. In Nigeria, the rise of digital payment systems and online banking has made cyber fraud more common. Many of these platforms lack strong security features, making them vulnerable to advanced attacks by fraudsters[46].

Weaknesses within organizations, like poor leadership, weak internal controls, and a lack of transparency, provide fertile ground for fraud. These gaps allow fraudsters to tamper with records, steal funds, or access confidential information without authorization[47]. In Nigeria's public sector, problems such as "ghost workers" on payrolls and inflated contract costs are clear examples of how systemic flaws can enable fraudulent activities. Cultural attitudes that downplay unethical behaviour or minimize the seriousness of fraud also play a role in its widespread nature. Scholars point out that in Nigeria, certain forms of corruption are accepted by society, which weakens efforts to tackle fraud. Offenders often justify their

Lead City University Ibadan DO NOT COPY

actions by blaming perceived flaws in the system or by feeling pressure from society to go along with corrupt practices[48]. As financial systems become more connected globally, fraudsters are able to operate across borders, making it harder to detect and prosecute their activities. In Nigeria, many fraudulent schemes involve international networks, so it's crucial for local and global agencies to work together to prevent and address fraud effectively[49].

2.1.7 Patterns of Fraud

Fraud cases often rise at certain times, such as during the end of fiscal years or election periods, when economic activity and financial transactions are high. These times create opportunities for fraudsters to exploit the system. For example, records show that fraud targeting government funds is especially common during the budget implementation phase, when oversight may be less strict[50]. Fraud patterns in Nigeria seems to also differ between urban and rural areas. Cities seems to see more cases of cyber fraud and financial scams, while rural communities often face issues like land disputes, forged documents, and embezzlement of communal funds. The growth of digital technology has made fraud more complex and harder to combat and the shift to digital financial transactions has opened new doors for fraudsters while making their schemes more advanced. Common methods now include phishing, unauthorized money transfers, online impersonation, and identity theft. These tactics seems to take advantage of weaknesses in digital systems, making it harder for traditional investigation methods to catch and stop fraud and this change has pushed agencies to use more advanced tools and techniques to fight back.

2.1.8 Demographic Trends

Lead City University Ibadan DO NOT COPY

Research shows that fraud cases involve people from various socio-economic backgrounds, but young adults make up a large number of offenders. This trend highlights how unemployment and financial struggles can drive youth toward fraudulent activities, additionally, many cases involve insiders—employees within organizations who use their roles to commit or assist in fraud[51]. Fraudsters are increasingly using advanced digital tools to make their schemes more sophisticated. There seems to be a rise in cases involving encryption technologies and anonymous online transactions, which seems to make investigations more challenging. This seems to highlights the importance of the security agencies adopting modern digital forensics and data analysis techniques to stay ahead of these evolving fraud methods**.** As a serious problem worldwide, causing harm to individuals, businesses, and institutions. It can also involve acts of dishonesty done on purpose to gain unfair benefits as it can take many forms such as financial scams, identity theft, forgery, and embezzlement. These crimes weaken public trust and hurt the country's economy.

2.1.9 Types of Fraud

Fraud can generally be divided into two main types: opportunistic fraud and systemic fraud. Opportunistic fraud happens when individuals or small groups take advantage of specific weaknesses in an organization's processes, like poor oversight or weak financial controls. For example, this could involve unauthorized withdrawals or manipulating accounts for personal gain. Systemic fraud, on the other hand, is more organized and involves larger-scale efforts to exploit significant weaknesses in institutions. This type often includes activities like large-scale embezzlement or coordinated cyber fraud attacks that span multiple departments or organizations and while opportunistic fraud tends to be smaller in scale, systemic fraud has far-reaching consequences due to its organized and widespread nature[52].

Lead City University Ibadan DO NOT COPY

Research shows that social networks and insider access play a big role in enabling fraud. Insiders, such as employees or contractors with special access to an organization's data or financial systems, often use their positions to commit fraud or help others do so and many fraud cases in Nigeria involved insiders, emphasizing the importance of strict background checks and strong internal controls in organizations[53]. These cases show how fraud can be complex, as insiders often combine their knowledge of the system with technology to hide their actions and avoid detection.

2.1.10 Drivers of Fraud

To understand why persons commit fraud, it's important to look at the psychological and social factors that drive their actions. Research shows that financial stress, opportunity, and the ability to justify their actions are key reasons behind fraudulent behaviour. In Nigeria, economic hardship often pushes people to commit fraud as a way to make ends meet and cultural influences also play a role—when certain corrupt practices are seen as normal or acceptable, it becomes easier for individuals to justify their actions[54]. In some cases, societal pressure to achieve a certain lifestyle or status can encourage people to view fraud as an acceptable shortcut to success. These factors combine to create an environment where fraud thrives. Opportunities play a major role in enabling fraud and people who might not typically engage in criminal activity often exploit weak organizational controls[55]. In many fraud cases, a lack of proper monitoring and enforcement creates a sense of low risk, making it easier for individuals to take the chance without fear of being caught and the absence of strong consequences, like swift and effective prosecution, further encourages fraudulent behaviour. Without the fear of serious repercussions, individuals are more likely to take advantage of these gaps, increasing the occurrence of fraud.

Lead City University Ibadan DO NOT COPY

2.1.11 Technological Advancements and the Evolution of Fraud Tactics

Technology has significantly changed how fraud is carried out. While advancements like digital payment systems, mobile banking, and online transactions have boosted economic growth, they have also opened new doors for fraud. The widespread use of internet-connected devices has made it easier for fraudsters to operate from anywhere, targeting people and businesses with ease and the common tactics now include phishing scams, where fraudsters trick people into sharing sensitive information, identity theft, and using malware to gain unauthorized access to systems[56]. By exploiting technology, these criminals not only evade detection but also expand their reach, making it harder for individuals and organizations to protect themselves. A growing trend in fraud is the use of social engineering tactics, where fraudsters trick people into sharing sensitive information for financial gain. Scammers often pose as representatives of trusted institutions like banks or government agencies to deceive their victims into revealing personal details. This approach has been especially effective in Nigeria, where digital literacy levels vary greatly across the population and these tactics rely on exploiting trust, making them difficult to combat[57].

2.2 Theoretical Framework

The Fraud Triangle Theory (FT) and Routine Activity Theory (RAT) are useful tools for understanding how fraud occurs and the role of the Nigerian Security and Civil Defence Corps (NSCDC) Anti-Fraud Unit in tackling it. These theories provide complementary insights, helping to explore fraud as both an act driven by personal motives and a problem shaped by external circumstances. The Fraud Triangle focuses on three key elements that

Lead City University Ibadan DO NOT COPY

lead to fraud: pressure, opportunity, and rationalization. It explains why individuals commit fraud, highlighting personal and environmental factors. Meanwhile, Routine Activity Theory emphasizes the situational conditions that make fraud possible, such as the presence of motivated offenders, suitable targets, and a lack of effective security or guardianship. Together, these theories help build a clearer picture of fraud, shedding light on how it operates on both a personal and systemic level and guiding the NSCDC's efforts in investigation and prosecution.

2.2.1 Fraud Triangle Theory (FT)

The Fraud Triangle Theory, introduced by Donald Cressey in the 1950s, provides a powerful lens for understanding why individuals commit fraud, particularly in workplaces and financial systems. This theory suggests that fraud doesn't occur randomly; instead, it arises when three critical factors align: Pressure**,** Opportunity**,** and Rationalization**.** Pressure discusses the personal or financial burdens that push individuals toward fraudulent actions. These pressures can take many forms—mounting debts, family responsibilities, or even the fear of professional failure. For instance, an employee struggling with overwhelming financial obligations might feel compelled to manipulate financial records to meet those needs and Opportunity is the enabler of fraud, arising from weaknesses or gaps in an organization's controls or systems. When internal checks are lax or accountability measures are poorly implemented, individuals may perceive a low risk of detection, making fraud seem like a viable option. For example, a lack of oversight in financial reporting can provide the perfect chance for an employee to embezzle funds unnoticed while Rationalization is the psychological process that allows the fraudster to justify their actions. This could involve convincing themselves that their behaviour is not truly harmful or that they are entitled to the

Lead City University Ibadan DO NOT COPY

resources they are taking. Phrases like “I’ll pay it back later” or “The Company owes me this” are common rationalizations that enable individuals to cross ethical boundaries.

Furthermore, Pressure refers to the external or internal forces that drive an individual to commit fraud. These forces may include financial difficulties, unrealistic organizational expectations, or personal challenges such as debt or addiction. In Nigeria, socio-economic conditions such as high unemployment rates and poverty aggravate these pressures, pushing individuals toward fraudulent behaviors[58]. Opportunity arises from weaknesses in systems, such as poor internal controls, lack of oversight, or systemic loopholes. Fraudsters exploit these vulnerabilities to commit their acts without fear of immediate detection[59]. Rationalization involves the cognitive process by which fraudsters justify their actions. Common rationalizations include beliefs that their actions cause no harm, that they are entitled to compensation due to perceived injustices, or that "everyone else is doing it." In the Nigerian context, cultural normalization of corrupt practices often provides an enabling environment for such rationalizations, making it critical to address societal attitudes alongside systemic vulnerabilities[60].

The Fraud Triangle Theory is particularly useful for understanding the types of fraud cases handled by the NSCDC Anti-Fraud Unit. By focusing on the three key elements of the theory—Pressure, Opportunity, and Rationalization—the Unit can develop targeted strategies to tackle fraud more effectively. For instance, reducing financial and social pressures through broader socio-economic reforms, such as creating jobs and improving access to resources, can help address the root causes that drive people to commit fraud. Similarly, limiting opportunities by tightening internal controls, improving oversight, and addressing systemic weaknesses in organizations can make it harder for fraudsters to exploit vulnerabilities. Also,

Lead City University Ibadan DO NOT COPY

addressing rationalizations through public awareness campaigns can challenge the mindset that justifies fraudulent behaviour. Research highlights the versatility of the Fraud Triangle Theory in explaining and addressing fraud across various settings. For example, implementing strong internal controls and providing focused anti-fraud training can greatly reduce the chances of fraud occurring in Nigerian public institutions by minimizing opportunities and efforts to change cultural attitudes toward corruption have proven effective in addressing rationalization—the justifications people use to excuse fraudulent behavior[61]. Also, promoting ethical narratives and discouraging the normalization of corruption can significantly weaken the mindset that makes fraud seem acceptable.

2.2.2 Routine Activity Theory (RAT)

The Routine Activity Theory, introduced by Cohen and Felson in 1979, offers a practical way to understand how crimes occur. This theory focuses on the circumstances that make criminal activity possible, highlighting three key factors: a motivated offender who is ready to commit a crime, a suitable target that is vulnerable or appealing, and the absence of a capable guardian to prevent the crime. When these three elements come together, the likelihood of a crime increases. This approach shifts attention from the criminal alone to the environment and situational factors that create opportunities for wrongdoing, making it a valuable tool for understanding and preventing crimes like fraud.

A motivated offender is someone who has both the intention and the capability to commit fraud. Various factors can drive a person to act, including economic hardship, societal pressures, or access to insider knowledge. In Nigeria, high youth unemployment rates and the influence of peers are major reasons why some individuals turn to fraud[62]. These challenges

Lead City University Ibadan DO NOT COPY

often push people to exploit weaknesses in systems as a way to achieve financial stability or gain social acceptance.

A suitable target is anything or anyone that can be easily exploited, such as financial accounts, public resources, or digital systems. Fraudsters often look for weakly protected assets, like unmonitored payroll systems or insecure digital platforms, because they are easier to manipulate. To address this, the NSCDC works to safeguard these vulnerable targets by using surveillance, enforcing regulations, and strengthening security measures[63].

A capable guardian is someone or something that prevents crime by overseeing, regulating, or enforcing rules. When there's no strong guardian, such as weak enforcement or limited resources, fraud becomes easier to commit. The NSCDC plays a key role as a guardian by monitoring vital infrastructure, investigating fraud cases, and offering security solutions that focus on community protection[64]. Routine Activity Theory is helpful in understanding how fraud happens in situations where the NSCDC operates. By improving enforcement, increasing public involvement, and working more with other agencies, the NSCDC can prevent the three factors that allow fraud from coming together. This approach can help stop fraud before it occurs.

The Fraud Triangle Theory looks at why individuals commit fraud by focusing on their motivations and thought processes, while the Routine Activity Theory looks at the situation and weaknesses in the system that allow fraud to happen. By combining these two theories, we get a fuller picture of fraud, considering both the actions of the offender and the conditions around them that make fraud possible. The application of both the Fraud Triangle Theory and Routine Activity Theory in the context of the Nigerian Security and Civil Defence Corps (NSCDC) offers a comprehensive approach to tackling fraud and the Fraud

Lead City University Ibadan DO NOT COPY

Triangle Theory informs the NSCDC's strategies by addressing internal and external pressures, closing systemic gaps, and countering rationalizations that may justify fraudulent behaviour. Meanwhile, the Routine Activity Theory guides the NSCDC's operational measures, focusing on enhancing guardianship, reducing target vulnerability, and addressing offender motivations. This combined theoretical framework bridges individual motivations and situational factors, emphasizing the need to address both psychological and systemic elements for effective fraud prevention and investigation.

Applying these theories to the NSCDC's Anti-Fraud Unit establishes the importance of localized, community-centred strategies in complementing broader national anti-fraud initiatives, which also makes the integration of the Fraud Triangle Theory and Routine Activity Theory provides a robust foundation for understanding the dynamics of fraud. This also highlights the significance of analysing fraud as both an individual act driven by motivation and rationalization, and a systemic issue influenced by situational vulnerabilities. The dual application of these theories not only deepens the analytical perspective but also offers practical insights to enhance anti-fraud efforts in Nigeria.

2.3 Review of Empirical Studies

A study was conducted to examine e-banking fraud and the influence of trust governance on customers' decisions to adopt or avoid electronic banking in Nigeria[65]. Using qualitative methods, including in-depth and key informant interviews, 30 participants were carefully selected, with some identified through snowball and referral techniques and the findings revealed three dimensions of e-fraud: internal (fraud involving bank staff), external (fraud perpetrated by outsiders), and collaborative (fraud involving both internal and external actors), which made these fraudulent experiences deterred many bank customers from

Lead City University Ibadan DO NOT COPY

migrating to e-banking platforms. Although governance mechanisms in the banking sector were found to be weak, banks are taking steps to rebuild customer trust and these measures include sending scam alert messages, publicly shaming and dismissing compromised staff, and implementing security protocols to protect the integrity of the evolving financial ecosystem[65].

Available evidence suggests that insider's participation in the nature of fraud in Nigeria's banking sector is pertinent, with a particular focus on insider involvement and the vulnerabilities of payment platforms following the introduction of the cashless policy in 2014. A study analyses fraud and forgery data from the 2019 Nigeria Deposit Insurance Corporation (NDIC) annual report to understand the complex dynamics of banking fraud and the findings reveal a consistent increase in fraud attacks on deposit money banks over the years, though the actual monetary losses decreased in 2019 compared to 2018. Transactions mediated by technology, such as ATM usage and internet banking, were the most targeted by fraudsters. Regarding insider involvement, employees at all levels participated in fraudulent activities, but the majority were temporary staff and based on these insights, the study recommends that banks enhance their security systems and governance structures. It is worthy to mention that discontinuing the employment of temporary staff and strengthening vigilance—both online and offline—are also critical measures, which makes the research to contribute to existing knowledge by highlighting the types of fraud, the role of insiders, and the factors that make casual staff particularly susceptible to engaging in fraud[66].

While previous studies have explored the causes, participants, and impacts of cybercrimes in Nigeria, little is known about how cybercriminals adapted their activities during the COVID-19 pandemic. Using the Fraud Triangle Theory and an exploratory research design, the

Lead City University Ibadan DO NOT COPY

research analysed data from the Economic and Financial Crimes Commission (EFCC), Nigerian Police, Nigerian Communications Commission (NCC), and Central Bank of Nigeria (CBN). Also, it was noted that the partial and total lockdowns imposed by federal and state governments to contain the spread of COVID-19 disrupted government palliative interventions, weakened social support systems, and heightened the vulnerability of Nigerians to cyber scams and fraudsters, known as "COVID-419ners," exploited these vulnerabilities through schemes like fake relief packages, food and data fraud, and fraudulent cash support and loan offers. These schemes mimicked government palliative programs to deceive and defraud the public. The study recommends timely delivery of government interventions and clear public education on eligible beneficiaries to protect vulnerable Nigerians, also, anti-cybercrime agencies must adopt proactive measures to prevent fraud, dismantle fraudulent schemes, and apprehend cybercriminals to curb such activities in future crises[67].

Research to date indicates that Internet fraud is one of the fastest-growing forms of computer crime globally, and in Nigeria, hence, it has taken on a unique form with the emergence of the "yahoo-boys" subculture among students in tertiary institutions. While many studies focus on the rise of this subculture, they often overlook the structural systems that sustain it. Using a snowball sampling technique, interviews were conducted with 20 self-identified yahoo-boys and the findings reveal that internet fraud in tertiary institutions is highly organized and supported by informal networks. These networks include other fraudsters and even bank staff who provide critical support. Bank employees were reported to leak confidential customer information to yahoo-boys and facilitate payments without raising security alarms. Fellow fraudsters help each other navigate legal troubles, including

Lead City University Ibadan DO NOT COPY

arranging bail when necessary. Payments are processed through various channels, such as domiciliary accounts, cheques, credit cards, MoneyGram, and Western Union. Participants indicated that cybercrime offers tangible benefits, such as covering tuition fees, acquiring properties like cars and land, and maintaining their lifestyles, and that made this deeply rooted informal network undermines efforts to combat cybercrime in Nigeria, meanwhile, in that study, it was noted that to address the issue of fraud, the government must tackle the underlying drivers, such as unemployment and systemic corruption, while promoting moral values and ethical behaviour within society[68].

Previous research has largely overlooked the unintended consequences of ATM usage, particularly the factors that make individuals vulnerable to fraud and this address the gap by investigating victims of ATM fraud in southwest Nigeria[69]. In that study, data were gathered through in-depth interviews with 20 victims in Lagos and Oyo states and the findings revealed that victims came from diverse demographics, including young and elderly individuals of both genders. Interestingly, fraudsters were often people within the victims' social circles, such as romantic partners, friends, relatives, and even their own children. In that study, it was revealed that the common tactics used by fraudsters included card cloning, card swapping, and physical attacks at ATM locations and factors contributing to vulnerability included low literacy levels, poor health, specific routines, and the timing of cash withdrawals. To combat these issues, banks implemented various measures, such as improving staff welfare, enforcing strict penalties for employees involved in fraud, and raising customer awareness through targeted alerts. The study highlights the limitations of trust within the cashless economy and underscores the importance of robust trust governance.

Lead City University Ibadan DO NOT COPY

It also raises critical policy questions about victim compensation and the need for strengthened measures to build confidence in electronic banking systems[69].

Prior research has demonstrated that a significant drawback of the cashless policy introduced by the Central Bank of Nigeria in 2014 has been the rise of widespread ATM fraud. While fraudsters benefit financially, victims face significant disruptions to their lives. Despite this, previous research in Nigeria has largely overlooked how ATM fraud impacts victims' life chances. Using in-depth interviews with victims of ATM fraud, the empirical evidence of the study revealed that many victims experienced post-fraud trauma, often relying on friends, family, and relatives for emotional and financial support to cope[70].

As support by the literature, banks' responses to customer victimization were found to be inadequate, offering little to no support in compensating for the financial losses incurred and this study recommends that banks strengthen their internal controls and implement trust governance mechanisms to better protect customers and prevent victimization while ensuring that customer security and provision of appropriate support post-fraud are critical steps toward restoring trust in the cashless policy[70].

A survey of an extant literature sheds light on the prevalence of fraud within Nigeria's cashless financial system and explores efforts to build trust as a means of curbing this growing challenge[71]. The article addresses two key questions: Does the fear of fraud hinder financial inclusion? And how do risk governance mechanisms influence the relationship between electronic fraud and financial inclusion? Using qualitative methods to engage participants from southwestern Nigeria, the scholars in that study revealed that fear of fraud, indirect experiences with fraudulent activities, and the presence (or absence) of effective fraud governance significantly impact how individuals adopt and interact with the banking

Lead City University Ibadan DO NOT COPY

system and these factors shape both behaviour and trust, highlighting the importance of robust risk management in fostering greater financial inclusion[71].

Consistent with prior findings, Tade and Adeniyi investigated ATM fraud in southwest Nigeria, focusing on the unintended consequences of ATM usage, particularly the role of fraudsters' identities and the methods they use to commit fraud. While previous research has largely overlooked these aspects, the study employs a sequential exploratory mixed-method approach, gathering data from both ATM users and victims of ATM fraud through a multi-stage sampling process[72]. Lagos and Oyo states were purposively selected for the research. In that finding fraudsters were often individuals within the victims' social circles, including lovers, friends, relatives, and, in some cases, their own children. Common tactics included card cloning, card swapping, and physical attacks at ATM locations. However, due to the study's small sample size, the results may lack broad generalizability, emphasizing the need for more extensive research across Nigeria. The paper highlights critical policy implications for the deployment and use of payment systems like ATMs in Nigeria. It underscores the limits of trust within the cashless policy framework and raises important questions about the governance of trust to encourage broader adoption. By characterizing fraudsters and their defrauding strategies, the study provides valuable insights for policymakers aiming to enhance payment system security and public confidence[72].

In line with recent findings, another article delves into Nigeria's Whistle-Blowing Policy (WBP) and its role in the country's anti-corruption efforts between 2016 and 2017, the article explores how individuals involved in corruption have adapted their methods to conceal stolen funds in response to the policy and examines the broader implications of looting on governance and national security. This analysis is especially important given Nigeria's poor

Lead City University Ibadan DO NOT COPY

global ranking in corruption perception over the past five years, while corruption not only hinders development but also poses a significant threat to security, as public funds meant for collective progress are siphoned into private accounts. Using data from newspaper reports on corruption, the study argues that the WBP, by incentivizing patriotism, has encouraged greater citizen involvement in the fight against corruption and facilitated the recovery of stolen funds[73]. However, it has also driven looters to resort to unconventional methods of hiding money, such as storing it in private safes, septic tanks, and warehouses or abandoning it in places like airports and market stalls. The article concludes by highlighting the potential impact that the recovered funds could have had on improving governance and development. It underscores how the diversion of public funds undermines security and weakens democratic governance in Nigeria, emphasizing the need for sustained efforts to combat corruption.

A plethora of studies have focused on ATM fraud in southwest Nigeria, but a scholarly study explored ATM from the victim's standpoint, addressing a gap in research by exploring the unintended consequences of ATM use from the victims' perspective. As support by the literature, a mixed-methods approach was used, combining interviews and surveys to gather data from ATM users and fraud victims in Lagos and Oyo states. Participants were selected through a multi-stage sampling process, with victims primarily identified using the snowball method. The research included in-depth interviews with fraud victims, as well as key informant interviews with police officers and bank officials responsible for ATM security, also, questionnaires were distributed to students, business owners, civil servants, artisans, and lecturers across the two states and the findings revealed that fraudsters were often people close to the victims, such as their children, friends, relatives, or romantic partners and the

Lead City University Ibadan DO NOT COPY

consequences of ATM fraud for victims included business failures, delays in meeting housing needs, psychological distress, and financial instability, which made the study to recommend policies that take into account the unique socio-demographic characteristics of customers to promote financial inclusion and reduce the risks associated with ATM use[74].

Research on fraud in Nigeria revealed that cybercrime is predominantly carried out by young people and students in tertiary institutions, commonly referred to as "yahoo boys" and these individuals use their computer skills to deceive unsuspecting victims online. A recent development in this trend is the incorporation of spiritual practices, known as "cyber spiritualism," to enhance the success of their cybercrime activities and that study explores the factors driving the integration of spiritual elements into cybercrime and highlights the strategies employed by yahoo boys and those involved in "yahoo plus" (a variant that incorporates spiritual rituals)[75]. Using the Space Transition Theory of cybercrime, the research examines how factors like crackdowns by the Economic and Financial Crimes Commission (EFCC), conflicts within yahoo boy groups over social status, delays in achieving financial success, and increased public awareness have contributed to the adoption of spiritual practices. In that paper, the methods used by fraudsters include the use of ase (a command believed to compel obedience), enchanted rings (oruka-ere), and incisions made around the wrist, which are said to aid internet navigation and other practices involve using a tortoise (ijapa) to access profitable websites and that revealed how victims are often influenced through phone conversations where spiritual commands render them powerless to resist the fraudster's demands[75].

Cyber-enabled mass-marketing frauds, such as romance scams, investment schemes, and "419" fraud, are often associated with West Africa, particularly Nigeria and there has been

Lead City University Ibadan DO NOT COPY

significant research and debate on why this region appears to be a hotspot for such cybercrimes. A critically review of existing literature examine the extent to which cultural factors contribute to and enable these crimes, with a particular focus on the pathways Nigerians take into cyber-fraud and the findings suggest that cultural elements, such as historical and social influences, social identity, and attitudes toward these crimes, play a role in fostering cyberfraud[76]. However, the paper cautions against overly attributing the prevalence of these activities solely to "West African culture," as this risk oversimplifying the issue. Building on previous studies, the paper proposes a theoretical framework to better understand the pathways leading to cyber-fraud and outlines strategies for effective disruption and prevention. This approach aims to provide a balanced perspective while contributing to the development of targeted solutions for reducing cyber-enabled mass-marketing fraud[76].

Current research on fraud disclosed that online fraud is largely shaped by perspectives from the Global North, leaving Nigerian scholarship on the issue marginalized in academic discussions, hence, the study addresses this gap by analysing studies that focus on online fraud within the Nigerian context. The study emphasizes unique aspects of Nigerian society and culture, particularly the role of spirituality, which are often overlooked in Global North narratives and these cultural dimensions significantly influence both the discourse on online fraud and the strategies used to combat it[77]. The research argues that incorporating the insights of Nigerian scholars is essential for developing a more comprehensive and effective global approach to tackling online fraud, both within Nigeria and beyond.

The available evidence suggests that the widespread use of internet technologies has transformed modern interactions, but it also brings negative consequences, such as internet

Lead City University Ibadan DO NOT COPY

fraud, as a study explored the perception among young adults in Nigeria that internet fraud is an innovative response to economic survival rather than a criminal activity. In that study, Robert Merton's Anomie/Strain Theory (AST) was used to provide the theoretical foundation for the research using qualitative methods, data were collected through in-depth interviews with 15 participants selected through purposive and snowball sampling techniques in various locations across the Ibadan metropolis. The findings revealed that many youths engage in internet fraud as a means of financial survival in response to harsh economic conditions, framing it as a deviant but innovative strategy and also found out that internet fraudsters in Nigeria are socially organized by specialization, with wealth accumulation and the number of "clients" serving as the primary markers of hierarchy[78]. Although, Nigeria has laws prohibiting and prosecuting internet crimes, participants claimed that the state's compromised security apparatus is often manipulated to protect those involved in fraud. Successful fraudsters reportedly avoid prosecution by leveraging connections and using their illicit gains to invest in legitimate businesses, while only those without such advantages face legal consequences[78]. The study concluded with a call for youth value reorientation and the creation of job opportunities to address the underlying economic drivers of internet fraud.

The rise of the internet and the widespread use of e-payment platforms as a convenient payment method have significantly increased the prevalence of e-fraud and cyber-attacks in Nigerian banks, and an extant study examined the reasons behind and methods used in perpetrating e-fraud by employees in Nigeria's Deposit Money Banks, using a survey research design, the study collected primary data from 120 fraud investigation officers through structured questionnaires. In that study, the data analysis that was conducted using the simple percentages revealed that e-fraud was often committed by employees whose job

Lead City University Ibadan DO NOT COPY

security was threatened due to their inability to meet deposit targets, and these employees, leveraging their expertise or legitimate authority, collaborated with others to defraud the banks. The findings also showed that disruptive technologies and economic challenges led to job losses and created insecurity among employees and the fear of disengagement without adequate compensation drove some employees to commit e-fraud through methods like phishing, pharming, and bypassing internal controls[79].

The study recommended discouraging unrealistic deposit and sales targets in banks through strengthened labour laws and It also highlighted the need for human resources departments to implement whistleblowing policies, allowing employees to report supervisors who pressure them into fraudulent activities. Finally, it emphasized the importance of raising awareness about e-fraud among e-payment users and sensitizing bank employees to the consequences of fraudulent behaviour through regular education and training programs.

Another study examined how fraud and financial crimes affect the growth and development of Nigeria's economy and the data for the research were obtained exclusively from secondary sources, including the Central Bank of Nigeria (CBN) Statistical Bulletin (2022) and various editions of CBN Annual Reports. The analysis employed the Ordinary Least Squares (OLS) method, along with a series of pre-estimation and post-estimation tests. Pre-estimation tests, such as unit root and normality tests, were used to ensure the reliability of the time-series data. Post-estimation tests, including heteroscedasticity and serial correlation checks, were conducted to validate the results. The findings revealed that fraud and financial crimes significantly impact Nigeria’s economic growth rate but do not appear to affect inflation and based on these findings, the study recommended several measures to address the challenges posed by financial crimes, and these include strengthening institutional frameworks and

Lead City University Ibadan DO NOT COPY

enhancing the capacity, independence, and effectiveness of anti-fraud and financial crime organizations, such as the Economic and Financial Crimes Commission (EFCC)[80]. Additionally, the study highlighted the importance of increasing transparency and accountability in both public and private sectors and measures such as the publication of financial reports, disclosure of beneficial ownership, and implementation of whistle-blower protection policies were suggested as critical steps toward mitigating the impact of financial crimes on the economy[80].

Consistent with prior findings, a review of an extant research explained that cashless financial transactions rely on information technology to transfer funds for payments, expenditures, and local government revenues. By adopting cashless systems, the potential for fraud and corruption is significantly reduced, as these transactions offer greater transparency. As supported by literature, that study explore strategies for preventing fraud through the implementation of a cashless policy and that research was conducted systematically using an article search engine, with the keywords "Cashless" and "Fraud" entered into the Scopus journal database. Secondary data from the Publish or Perish application were also reviewed and journals and articles were carefully selected based on their relevance to the theme and the quality of their content. The findings indicate that innovations in local government payment systems have prompted a shift toward safer, more effective, and efficient non-cash transactions.

A critical review of that literature highlights that cashless payments help prevent corrupt practices such as money laundering, bribery, and the misuse of funds through commissions for services or procurement and the adoption of non-cash transactions is particularly effective when local governments enforce policies that mandate their use, supported by reliable

Lead City University Ibadan DO NOT COPY

internet access and modern technology in both urban and rural areas[81]. The study recommends that local governments not only adopt but also report on non-cash payment practices and policies should prioritize digital payment methods for initiatives like social assistance programs and the collection of fees and levies. These measures can increase local revenues while promoting transparency and efficiency in financial transactions.

Despite the implementation of the Nigerian Cybercrime Act in 2015, cyber fraud remains widespread among youths, particularly undergraduate students and an empirical evidence from the study explored the pathways leading to and the motivations behind female undergraduates' involvement in cyber fraud in selected universities across southwest Nigeria. That research adopted an exploratory, cross-sectional design and utilized Social Learning Theory as its conceptual framework. Data collected were exclusively through in-depth interviews with 17 female undergraduates, selected using the snowball sampling method and the findings in that study revealed that these students were often introduced to cyber fraud by male relatives and associates[82]. The primary motivations for their involvement included financial gain and peer pressure, which makes many viewed cyber fraud as a viable means to support their personal needs and those of their families. The study recommends a multi-dimensional approach to effectively address this issue, combining preventive strategies with education, awareness, and stricter enforcement of anti-cybercrime measures.

Lead City University Ibadan DO NOT COPY

2.4 Conceptual Model

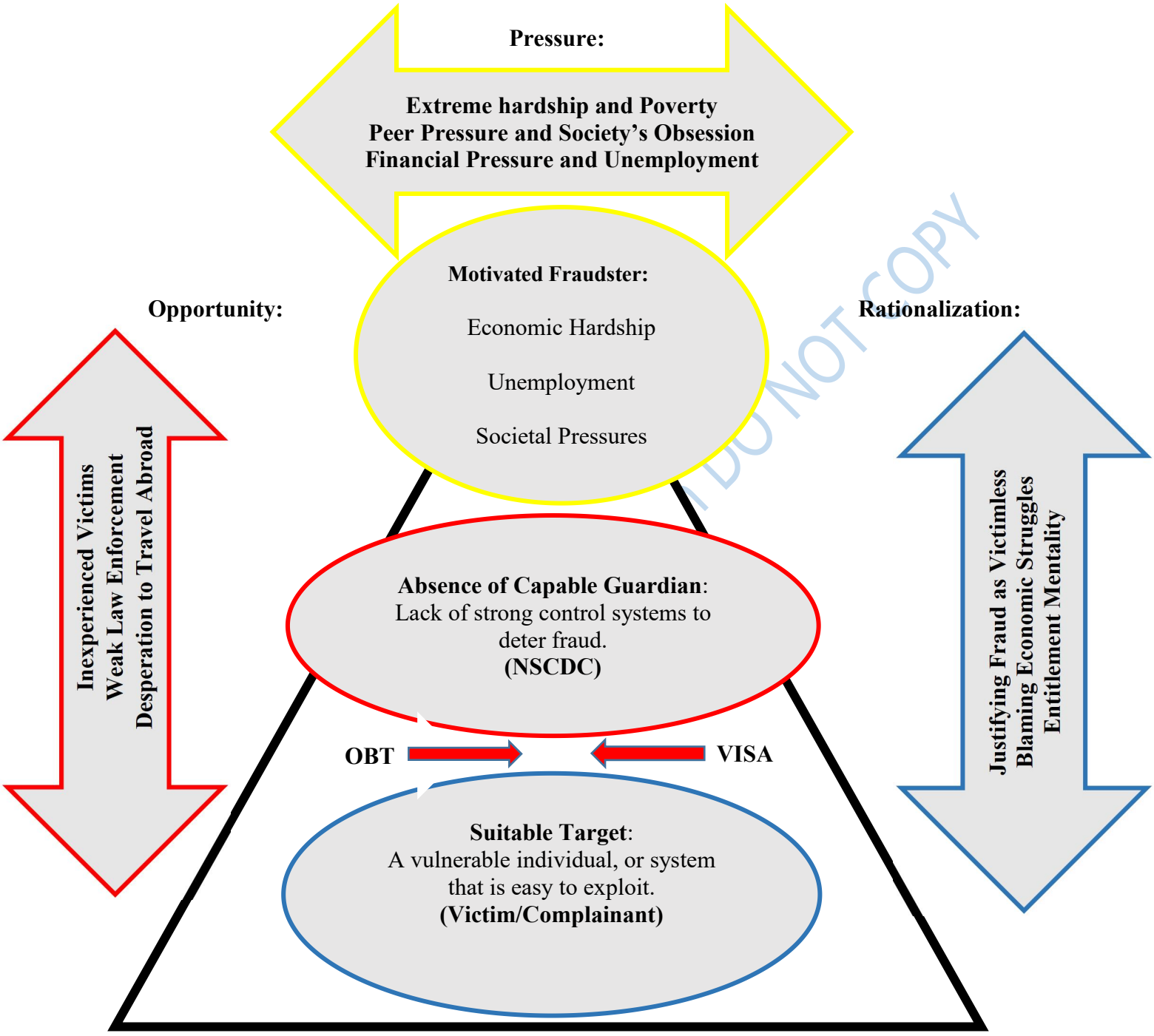


Figure 2.1: Conceptual model showing the relationship between Fraud Triangle and Routine Activity Theory.
Source: Researcher's Computation, 2025

The Fraud Triangle and Routine Activity Theories, while distinct, work together to explain how and why Obtaining by False Pretence (OBT) and Visa Racketeering (VISA) happen. Both highlight the factors that drive people to commit OBT and Visa, the opportunities that make them possible, and the systemic weaknesses that allow these crimes to thrive. Together, they offer a complete framework to understand the interactions between offenders, victims, and the systems that create an environment for OBT and Visa.

The *Fraud Triangle* provides an internal perspective, focusing on the personal motivations that lead individuals to commit fraud. It highlights three elements: *pressure, opportunity*, and *rationalization.* Pressure refers to the stresses that push individuals toward committing OBT and VISA and these pressures include *Extreme hardship and Poverty, Peer Pressure and Society's Obsession, Financial Pressure and Unemployment*. For many fraudsters, these pressures feel overwhelming, and they see fraud as their only option to meet these demands. Opportunity for OBT and VISA to happen arises when there is *Inexperienced Victims, Weak Law Enforcement and Desperation to Travel*. For example, inadequate enforcement by institutions like the NSCDC, uneducated or inexperienced victims, or gaps in identity verification systems provide fraudsters with the chance to act and without proper safeguards, individuals are more likely to exploit these opportunities. Rationalization is the mental process through which fraudsters justify their actions of OBT and VISA as *Victimless crime* while they keep *Blaming the Economic Struggles in the country and* wallowing *in* their *Entitlement Mentality.* Many convince themselves that their crimes are "harmless" or that they are entitled to the money due to their difficult circumstances. By rationalizing their actions, they reduce feelings of guilt and make it easier to proceed with fraudulent activities.

Lead City University Ibadan DO NOT COPY

The Routine Activity Theory, on the other hand, offers an external perspective on how OBT and VISA occur. It explains that these fraud types happen when three elements converge*: a motivated offender***,** a *suitable target*, and *the absence of capable guardianship***.** A motivated offender is someone willing to commit OBT and VISA, often driven by pressures similar to those outlined in the Fraud Triangle. In this study, a motivated offender is influenced by *Economic Hardship, Unemployment and Societal Pressures*, such as through fraudulent visa applications or cybercrime schemes. A suitable target are the individuals or systems that are vulnerable to exploitation. For instance, those desperate to migrate abroad or unfamiliar with digital platforms are particularly easy targets for fraudsters and the absence of capable guardianship highlights the role of weak law enforcement, poor institutional oversight, or inadequate control systems in enabling OBT and VISA. When regulatory oversight is lacking in-between a motivated fraudster and a suitable target or institutions like the NSCDC have limited resources, a motivated fraudster feels emboldened to act without fear of consequences.

When these two theories are integrated, they provide a powerful explanation of how OBT and VISA occurs. The Fraud Triangle explains why individuals are motivated to commit fraud, while the Routine Activity Theory identifies the external conditions that create opportunities for fraud to happen. For example: *When Pressure Meets Opportunity*: Someone facing *Extreme hardship and Poverty, Peer Pressure and Society's Obsession and Financial Pressure and Unemployment* (Fraud Triangle) will exploit weak systems or inexperienced victims (Routine Activity Theory), particularly during high-risk periods like festive seasons or migration waves.

Lead City University Ibadan DO NOT COPY

When Rationalization Aligns with Absence of Guardianship: Fraudsters justify their actions by blaming economic hardship or systemic failures (Fraud Triangle) and this justification is strengthened when law enforcement is ineffective or institutional safeguards are weak (Routine Activity Theory), making fraud appear low-risk and acceptable. *When Motivated Fraudster Target Vulnerable Individuals:* The Routine Activity Theory's concept of motivated offenders aligns with the Fraud Triangle's focus on pressure and rationalization. Similarly, the identification of suitable targets ties into the Fraud Triangle's concept of opportunity, demonstrating how external vulnerabilities intersect with internal motivations.

The practical implications of these interconnected theories are significant. OBT and VISA are not just about personal motivations or system failures—it is a combination of both. This framework also explains that effective law enforcement efforts will address the personal pressures and rationalizations that drive individuals to commit fraud and fixing systemic weaknesses will not create opportunities for fraud to happen. For instance, addressing unemployment and poverty can reduce the internal pressures that push people toward fraud. At the same time, strengthening institutional frameworks, such as improving enforcement by the NSCDC and educating potential victims, can close gaps that fraudsters exploit. Together, these actions create a comprehensive approach to preventing and reducing fraudulent activities like OBT and VISA.

Lead City University Ibadan DO NOT COPY

2.5 Summary of Gaps in Literature Reviewed

Existing research on fraud in Nigeria appears to have mainly focused on the roles of well-known agencies such as the Nigerian Police Force (NPF), the Economic and Financial Crimes Commission (EFCC), the National Financial Intelligence Unit (NFIU), and the

Independent Corrupt Practices and Other Related Offences Commission (ICPC). These studies have explored how these agencies operate, their strategies, and the challenges they face in tackling financial crimes. Similarly, considerable research appears to have been devoted to understanding the dynamics of fraud, its impact on society, and the prevalence of cyber-related scams such as "419." While these studies provide important insights, they seem to have overlook the roles of other key players in Nigeria's anti-fraud efforts. One major gap in the literature is the lack of attention to the Nigerian Security and Civil Defence Corps (NSCDC), particularly its Anti-Fraud Unit.

Despite having the legal mandate to arrest with or without warrant, detain, investigate and institute legal proceedings by or in the name of the Attorney General of the federation in accordance with the provisions of the constitution of the Federal Republic of Nigeria against any person who is reasonably suspected to have committed any criminal activity such as fraud and despite showing all these promises in their administrative efficiency, their contributions, especially the Anti-Fraud Unit of the NSCDC are rarely discussed in academic or policy circles. This lack of recognition has left a limited understanding of how the Unit fits into Nigeria's overall anti-fraud framework and the potential it has to complement the work of larger agencies. While much research seems to have analysed the complexities of fraud, the enforcement challenges, and the socio-economic factors driving financial crimes, little attention has been given to how less prominent agencies like the NSCDC handle these issues.

There is almost no research on the strategies the NSCDC Anti-Fraud Unit uses to investigate fraud, the specific challenges it faces, or the methods it employs to navigate institutional and resource constraints. Additionally, the challenges of the NSCDC Anti-Fraud Unit—such as limited funding, low public visibility, and insufficient institutional support—have not been

Lead City University Ibadan DO NOT COPY

adequately explored. The implications of these challenges, including how they limit the Unit's effectiveness and prevent it from easing the burden on more prominent agencies like the EFCC, remain largely unexplored. Although over-reliance on major agencies like the EFCC has been identified as a weakness in Nigeria's anti-fraud framework, the potential of the NSCDC to share this responsibility has been ignored. This study addresses these gaps by bringing the NSCDC Anti-Fraud Unit into the spotlight by highlighting the Unit's role, its challenges, and its contributions to fraud investigation and prosecution in Nigeria. By examining how the Unit operates and the obstacles it faces, the study provides new insights into Nigeria's anti-fraud efforts. it argues for more diversified approach to tackling fraud, where all available institutions, including the NSCDC, are fully supported and utilized.

Lead City University Ibadan DO NOT COPY

Endnotes

1. S. S. Simpson, *Criminology and Corporate Crime: The Art of Scientific Cross Pollination,* **Annual Review of Criminology,**8,2024, https://doi.org/10.1146/annurev-criminol-022422-121435

2. U. Bansal, S. Bharatwal, D. S. Bagiyam & E. R. Kismawadi, *Fraud Detection in The Era of AI: Harnessing Technology for A Safer Digital Economy.* In AI-Driven Decentralized Finance and the Future of Finance, **IGI Global,** 2024, 139-160.

3. M. Levi & A. Doig. *Exploring The 'Shadows' in the Implementation Processes for National Anti-Fraud Strategies at the Local Level: Aims, Ownership, and Impact*. **European Journal on Criminal Policy and Research,** 26(3), 2020,313-333.

4. M.A. Rashid, A. Al-Mamun, H. Roudaki, & Q.R. Yasser, *An Overview of Corporate Fraud and its Prevention Approach*, **Australasian Accounting, Business and Finance Journal** 16(1), 2022, 101-118.

5. J. Schwartz, D. Steffensmeier, W.J. Moser & L. Beltz*, Financial Prominence and Financial Conditions: Risk Factors for 21st Century Corporate Financial Securities Fraud in The United States***. Justice Quarterly**, 39(3), 2022, 612-641.

6. C.S. Kayser, S. Back, & M.M. Toro-Alvarez, *Identity Theft: The Importance of Prosecuting on Behalf of Victims*. *Laws***,** 13*(*6), 2024, pp. 68.

7. N. F. Stowell, C. Pacini, N. Wadlinger, J.M. Crain, & M. Schmidt, *Investigating Healthcare Fraud: its Scope, Applicable Laws, and Regulations*. **William & Mary Business Law Review**, 11(2), 2020, 479.

8. T. J. Holt, A. M. Bossler, & K. C. Seigfried-Spellar, *Cybercrime and Digital Forensics: an Introduction*. Routledge, 2022.

9. P. D. Henderson, *Organizational Leaders' Strategies to Detect and Prevent Occupational Fraud*. PhD diss., Walden University, 2024.

10. A.T. Tinuoye, *An Overview of Corruption in the Context of The Public Sector*. Management Strategies and Tools for Addressing Corruption in Public and Private Organizations**,** 2023 pp. 19-38.

11. D. S. Adeniyi*, Corruption in The Nigerian Public Sector*, **International Journal of Research and Innovation in Social Science** 6, no. 7, 2022, pp. 632-636.

Lead City University Ibadan DO NOT COPY

12. J. C., Agu, F. N., Nkwo & R. U. Eneiga. *Governance and Anti-Corruption Measures in Nigeria: Strategies for Enhancing Transparency, Accountability and Public Trust*, **International Journal of Economics and Public Policy** 8, no., 2024 pp. 1-15.

13. T.A. Abioro, *Public Procurement Corruption and Service Delivery in Nigeria and South Africa.* Public Procurement, Corruption and the Crisis of Governance in Africa, 2021 pp. 249-267, https://doi.org/10.1007/978-3-030-63857-3_13

14. A. Kuzior, I. Tiutiunyk, A. Zielińska, & R. Kelemen, "*Cybersecurity and Cybercrime: Current Trends and Threats*, **Journal of International Studies**, 17, no. 2., 2024, pp. 2071-8330

15. J. McGrath & D. Healy*, Theorizing The Drop in White-Collar Crime Prosecutions: An Ecological Model,* **Punishment & Society**, 23(2), 2021, pp.164-189, https://doi.org/10.1177/1462474520939060

16. A. C. Ozioko, *Trends in Prosecuting Financial Crimes: Successes and Failures*, **Multi-Disciplinary Research and Development Journals Int'l**, 6(1), 2024, pp.28-54.

17. R. S. Faqir, *Digital Criminal Investigations in the Era of Artificial Intelligence: A Comprehensive Overview,* **International Journal of Cyber Criminology**, 17(2), 2023, pp.77-94, https://orcid.org/0000-0002-6102-0983

18. T. Legrand, & C. Leuprecht, *Securing Cross-Border Collaboration: Transgovernmental Enforcement Networks, Organized Crime and Illicit International Political Economy*, **Policy and Society,** 40(4), 2021, pp.565-586, https://doi.org/10.1080/14494035.2021.1975216

19. A. Pântea, & S. Pantea, *Countering Fraud to The Financial Interests of The European Union Through Enhanced Cooperation*. **Acta Universitatis Danubius. Juridica,** 17(1), 2021, 167-175,

20. U. O. Felix, *Evidence Collecting Processes and Fraud Examination: The Role of an Expert Forensic Accountant***, Asian Basic and Applied Research Journal**, 4(1), 2022, pp.394-420, https://www.jofresearch.com/index.php/ABAARJ/article/view/75

21. D. A., Waterman, *A Defendant's Ability to Pay: The Key to Unlocking the Door of Restitution,* **Debt. Iowa L. Rev**., 106, 2020, pp.455.

22. L. Cadigan, & S. Nath, *Parallel Enforcement: Sec Authorities and How They Can Impact FDA's Civil and Criminal Enforcement***, Food & Drug LJ,** 78, 2023, p.235.

Lead City University Ibadan DO NOT COPY

23. K. R. Worme, *Corporate Governance–A Comparative Analysis of The Approach to Corporate Governance Regulation and Enforcement in the UK and the US*, Liverpool John Moores University (United Kingdom), 2024, pp. 15-362

24. S. Bourton, *Tax Evasion and the Law: A Comparative Analysis of the UK and US,* **Taylor & Francis**, 2024, DOI: 10.4324/9781003333227-1

25. A. A. Kazaure, M. N. Yusoff, & A. Jantan, 2023. *Digital Forensics Investigation Approaches in Mitigating Cybercrimes*, **A Review. Journal of Information Science Theory & Practice (JIStaP**), 11(4), 2023, pp. 14 DOI: 10.1633/JISTaP.2023.11.4.2

26. B. O. Adelakun, E. R. Onwubuariri, G. A. Adeniran, & A. Ntiakoh, *Enhancing Fraud Detection in Accounting Through AI: Techniques and Case Studies*, **Finance & Accounting Research Journal**, 6(6), 2024, pp.978-999, DOI: https://doi.org/10.51594/farj.v6i6.1232

27. M. Kryshtanovych, V. Lopatovskyi, O. Bondaruk, N. Datsii, R. Primush, & I. Dragan, *Accounting, Analytical and Information Support for Law Enforcement Activity in Conditions of Ensuring Economic Security in Public Administration*, **Journal of Ecohumanism**, 3(6), 2024, pp.751-759.

28. S. A. Marciniak III, *Too Big to protect: A Dodd-Frank Framework for Protecting 21st Century American Consumer Privacy Rights*. **Duq. L. Rev.,** 59, 2021, pp.329.

29. E. N. Vitus, *Cybercrime and Online Safety: Addressing the Challenges and Solutions Related to Cybercrime, Online Fraud, and Ensuring a Safe Digital Environment for All Users—A Case of African States***, Tijer-International Research Journal**, 10(9), 2023, pp.975-989, SSRN: https://ssrn.com/abstract=4589211

30. J. Kwon, J*urisdictional Overlap: The Juxtaposition of Institutional Independence and Collaboration in Police Wrongdoing Investigations*, **Regulation & Governance,** 2024, 18(2), pp.551-572, https://doi.org/10.1111/rego.12532

31. A. E. Bozbayındır, *The Role of the Judge In the European Plea Bargaining Procedures: Three Models Compared*, **The International Journal of Evidence & Proof,** 28(3), 2024, pp.203-235, https://doi.org/10.1177/13657127231217773

32. M. S. Korejo, R. Rajamanickam, R., M. H. Md. Said, E. N. Korejo, P*lea Bargain Dilemma, Financial Crime and Asset Recovery,* **Journal of Money Laundering Control**, 26(3), 2023, pp.628-639, https://doi.org/10.1108/JMLC-01-2022-0009

33. R. Subramanian, L. Digard, I.I. Melvin Washington, & S. Sorage, *In the Shadows: A Review of The Research on Plea Bargaining*, **Vera Institute of Justice**, 2020, pp.1-64.

Lead City University Ibadan DO NOT COPY

34. D. A. Yagboyaju & A. T. Simbine, *Political Finance and the 2019 General Elections in Nigeria*, **Journal of African Elections**, 19(1), 2020, pp.66-91.

35. D. Ekanem, *Artificial Intelligence as A Mechanism for Crime Control in Nigeria: A Critical Appraisal.* Lap Lambert Academic Publishing, 2020.

36. M. T. Pag, *Innovative or Ineffective? Reassessing Anti-Corruption Law Enforcement in Nigeria* Working Paper 9, Gi-Ace Project: Fighting High-Level Corruption in Africa: Learning from Effective Law Enforcement, 2021, (pp. 1-55).
37. J. Magakwe, *Curbing Corruption, Bribery, and Money Laundering in Public Procurement Processes: An International Perspective*, In Corruption, Bribery, and MoneyLaundering-GlobalIssues. IntechOpen,2024,DOI: 10.5772/intechopen.1004005

38. H. K. Ali, A. Y. Umar, & J.Y. Danga, The Role of Nigeria Security and Civil Defence Corps in Nigeria's Internal Security, **Arts and Social Science Research**, 13(1), 2023, pp.81-102, https://fassjassr.com.ng/index.php/assr/article/view/96.

39. M. B. Afolabi, I. G. Dogi, L. J. Ogunniyi, E. R. Agidigbi, & I. E. Oladipo, 2024. *Securing the Critical Infrastructure in Ondo State: Is the Nigeria Security and Civil Defence Corps up to The Task*, **African Renaissance**, 21(3), 2024, p.169.

40. U. S. Sarki, & M. Ya'u, *The Role of NSCDC in Crime Prevention in Nigeria: Conceptual and Emperical Analysis,* **International Journal of Trend in Research and Scientific Development,** 2019, www.ijtsrd.com, e-ISSN: 2456 – 6470

41. M. Egberedu, *Accessibility and Utilisation of Information and Communication Technology by the Nigeria Security and Civil Defence Corps in Southwestern Nigeria*, PhD diss., 2020, http://hdl.handle.net/123456789/1070

42. A. O. Ogunsanya, *Exploring Citizen Security in The Nigeria Federated State: Lagos State Neighbourhood Safety Agency in Perspective*, PhD diss., Walden University**,** 2021.

43. S. Ramos, J. A. Perez-Lopez, R. Abreu, S. Nunes, I*mpact of Fraud In Europe: Causes and Effects,* **Heliyon,** 2024, https://doi.org/10.1016/j.heliyon.2024.e40049

44. Q. Rossy, & O. Ribaux, *Orienting the Development of Crime Analysis Processes in Police Organisations Covering the Digital Transformations of Fraud Mechanisms.* **European Journal on Criminal Policy and Research**, *26*, 2020, pp.335-356.

45. R. Remeikienė & L. Gaspareniene*, Effects on the Economic and Sustainable Development and on the Poverty and Social Inequality.* **Economic and Financial Crime, Sustainability and Good Governance**, Cham: Springer International Publishing**,** 2023, (pp. 205-234)

Lead City University Ibadan DO NOT COPY

46. G. A. N. Ama, C. O. Onwubiko, & H. A. Nwankwo, *Cybersecurity Challenge in Nigeria Deposit Money Banks*, **Journal of Information Security,** 15(4), 2024, pp.494-523, **DOI:** 10.4236/jis.2024.154028

47. D. Medhi, P. Singh, H. Goswami, & J. Singh, *Futuristic Approach of Forensic Fraud Investigation in Money Embezzlement, Asset Misappropriation and Larceny*. **Educational Administration: Theory and Practice**, *30*(6), 2024, pp.1283-1303.

48. O. N. Okafor, F. A. Adebisi, M. Opara, & C. B. Okafor, *Deployment of whistleblowing as an accountability mechanism to curb corruption and fraud in a developing democracy*, **Accounting, Auditing & Accountability Journal**, Vol. 33 No. 6, 2020, pp. 1335-1366. https://doi.org/10.1108/AAAJ-12-2018-3780

49. M. Opara, O. N. Okafor, & F. Adebisi, F, *Whistleblowing and The Fight Against Corruption and Fraud in Nigeria: Perceptions of Anti-Corruption Agents (ACAs).* **Crime, Law and Social Change,** 73, 2020, pp.115-132.

50. H. A. Hashim, Z. Salleh, I. Shuhaimi & N.A.N Ismail, *The Risk of Financial Fraud: A Management Perspective*, **Journal of Financial Crime,** *27*(4), 2020, pp.1143-1159.

51. G. E. Odinka, J. T. Okpa, E. A. Ushie, B. E. Ekpenyong, & S. N. Echu, *Exploring the Socio-Economic Dynamics of Youths' Involvement in Internet Fraud in Nigeria,* **Journal of Public Administration, Policy and Governance Research 1**, no. 3,2023, 83-91.

52. P. Gottschalk, *Financial Crime Issues: Fraud Investigations and Social Control,* **Springer Nature**, 2022.

53. B. Blakely, J. Kurtenbach, & L. Nowak, *Exploring The Information Content of Cyber Breach Reports and The Relationship to Internal Controls*, **International Journal of Accounting Information Systems,** 46, 2022, p.100568, https://doi.org/10.1016/j.accinf.2022.100568

54. J. Kehinde Oyedeji, & H. Olamide Badmos, *Social Construction of Internet Fraud as Innovation Among Youths in Nigeria*, **International Journal of Cybersecurity Intelligence & Cybercrime**, 2022, *5*(1), pp.23-42.

55. T. A. A Koomson, G. M. Y. Owusu, R. A. Bekoe, & M. Oquaye, *Determinants of Asset Misappropriation at the Workplace: The Moderating Role of Perceived Strength of Internal Controls,* **Journal of Financial Crime**, 27(4), 2020, pp.1191-1211.

56. P. V. Falade, *Analysis of 419 Scams: The Trends and New Variants in Emerging Types,* **Int. J. Sci. Res. in Computer Science and Engineering**, Vol, 11(5), 2023

Lead City University Ibadan DO NOT COPY

57. A. Rohilla, *Strengthening Financial Resilience: A Holistic Approach to Combatting Fraud,* **Indian Journal of Economics and Finance (IJEF**), 4(1), 2024, pp.20-31.http://doi.org/10.54105/ijef.A2566.04010524

58. O. A. Ayinla, *The Impact of Crime on Economic Hardship in Oyo State, Nigeria*. ***International Journal of Social Science Research and Anthropology*****,** *4*(6), 2024, https://taapublications.com/tijssra/article/view/173

59. L. Razaq, T. Ahmad, S. Ibtasam, U. Ramzan, & S. Mare, *We Even Borrowed Money From Our Neighbor" Understanding Mobile-Based Frauds Through Victims' Experiences*, Proceedings of the ACM on human-computer interaction, *5*(CSCW1), 2021, pp.1-30, https://doi.org/10.1145/3449115

60. A. Hortal, & A. P. Martínez, *Behavioral Strategies for Reducing Corruption: From Regulation to Choice Architecture*, **Behavioural Public Policy**, 2024 pp.1-18, doi:10.1017/bpp.2024.48

61. M. K. Salawu, I. A. Oyewobi, & O. A. Adejumo, *Internal Control System, Risk Management Practice and Fraud Prevention Among Selected State Governments in Southwestern Nigeria.* **TWIST,** 18(4), 2023, pp.123-134, https://twistjournal.net/twist/article/view/86

62. A. O. Balogun, A. F. Lawal, & J. K. Ekundayo, J.K., *An Analysis of Push and Pull Factors of Internet Fraud Among Selected Residents of Ilorin Metropolis, Kwara State*, **Fuoye Journal of Criminology And Security Studies**, 2(1).

63. A. S. Brown, Nigeria *Security and Civil Defence Corps and the Protection of Critical Assets and Infrastructure: Combating Oil Theft, Vandalism and Internal Insurgency for National Development*, **Ibom Journal of Social Issues**. Vol. 9. No. 1. Afrischolar Discovery Repository (Annex).

64. J. M. C. Ogwumike*, Operational Equipment and Public Property Protection-A Study of Nigeria Security and Civil Defence Corps, Cross River State Command,* **International Journal of Democracy and Development Studies,** 5(3), 2022, pp.45-56.

65. O. Tade, & O. Adeniyi, *Dimensions of Electronic Fraud and Governance of Trust in Nigeria's Cashless Ecosystem***, International Journal of Offender Therapy and Comparative Criminology**, 64(16), 2020 1717-1740. https://doi.org/10.1177/0306624X20928028

Lead City University Ibadan DO NOT COPY

66. O. Tade, *Nature of Frauds in Nigeria's Banking Ecosystem, 2015-2019*, **Journal of Financial Crime**, Vol. 29 No. 4, 2022, pp. 1241-1248. https://doi.org/10.1108/JFC-08-2021-0185

67. O. Tade, *COVID-'419': Social Context of Cybercrime in the Age of COVID-19 in Nigeria*, **African Security**, 14(4), 2021, pp.460-483.

68. O. Tade, & I Aliyu, *Social Organization of Internet Fraud Among University Undergraduates in Nigeria.* **International Journal of Cyber Criminology**, 5(2), 2011

69. O. Tade, & O. Adeniyi, *Automated Teller Machine Fraud in South-West Nigeria: Victim Typologies, Victimisation Strategies and Fraud Prevention,* **Journal of Payments Strategy & Systems**, 11(1), 2017, pp.86-92.
70. O. Tade, & O. Adeniyi, '*They Withdrew All I Was Worth': Automated Teller Machine Fraud and Victims' Life Chances in Nigeria*, **International Review of Victimology,** 23(3), 2017, 313-324. https://doi.org/10.1177/0269758017704330

71. O. Tade, O. Adeniyi*, I Prefer to Remain Old School and Be Safe": Fear of Fraud and Governance of Risk in Nigeria's Cashless Ecosystem,* **Salus Journa**l, 11(2), 2023, pp.120-132.

72. O. Tade, O. & Adeniyi, *On the Limits of Trust: Characterising Automated Teller Machine Fraudsters in Southwest Nigeria,* **Journal of Financial Crime**, 23(4), 2016, pp.1112-1125.

73. O. Tade, *Policing Looted Funds with the Whistle,* **Africa Development/Afrique et Développement**, 44(4), 2019, pp.73-90.

74. O. Tade, & O. Adeniyi, *Automated Teller Machine Fraud in Southwest Nigeria: The Shoe Wearers' Perspectives.* **Irvine: University of California**, 2014,

75. O. Tade, *A Spiritual Dimension to Cybercrime in Nigeria: The 'Yahoo Plus' Phenomenon.* **HumanAffairs,** 23(4),2013,pp.689705,https://doi.org/10.2478/s13374-013-0158-9

76. M.T. Whitty, *419-It's Just a Game: Pathways to Cyber-Fraud Criminality Emanating from West Africa,* **International Journal of Cyber Criminology**, 12(1), 2018, pp.97-114.

77. C. Cross, *Marginalized Voices: The Absence of Nigerian Scholars in Global Examinations of Online Fraud,* The Palgrave handbook of Criminology and the Global South, 2018, pp.261-280.

78. A. Ayodele, J. Kehinde Oyedeji, & H. Olamide Badmos, *Social Construction of Internet Fraud as Innovation among Youths in Nigeria,* **International Journal of**

Leadcity University Ibadan DO NOT COPY

Cybersecurity Intelligence & Cybercrime: 5(1), 2022, 23-42, https://doi.org/10.52306/BUVC2778

79. B.M. Ololade, M. K. Salawu, & A. D. Adekanmi, *E-Fraud in Nigerian Banks: Why and How?,* **Journal of Financial Risk Management**, 9(3), 2020 pp.211-228.

80. N. O. Osmond, E. Donald, & O. J. Akamike, *Impact of Fraud and Financial Crimes on the Nigerian,* **Direct Research Journal of Social Science and Educational Studies**, 11(5), 2023, Pp: 80-87, DOI: https://doi.org/10.26765/DRJSSES042358162172023

81. R. Ridwan, S. Abdullah, & F. Yusmita, *Implementation of Cashless Policy Strategies to Minimize Fraud in The Government Sector: Systemic Revie,* **Jurnal Akuntansi**, 12(3), 2022, pp.181-201.
82. Y. O. Ogunleye, U. A. Ojedokun, A. A. & Aderinto, *Pathways and Motivations for Cyber Fraud Involvement Among Female Undergraduates of Selected Universities in South-West Nigeria,* **International Journal of Cyber Criminology**, 2019, 13(2).

Lead City University Ibadan DO NOT COPY

Chapter Three

Methodology

This chapter outlines the methodology and approach used in this study. It explains the research design, detailing the framework for gathering and analysing data. It identifies the study population and describes the sampling techniques used to select participants. Additionally, it highlights the instruments used for data collection, such as interviews and observation tools, and discusses the measures taken to ensure the validity and reliability of these instruments. The chapter also addresses the ethical considerations involved in the research, including how ethical approval was obtained before the study commenced.

3.1 Research Design

This study adopts an exploratory research design, using a case study approach to investigate the dynamics of fraud investigation within the Anti-Fraud Unit of the Nigerian Security and Civil Defence Corps (NSCDC) in Oyo State. The case study design is appropriate for this research because it allows for a detailed and contextual examination of the NSCDC's processes, practices, and challenges when handling fraud cases[1]. This approach is particularly valuable when studying an institution within its natural setting, providing insights into real-

Lead City University Ibadan DO NOT COPY

world operations and organizational structures. By using this method, the study gathered rich, qualitative data through detective interviews and an analysis of case files, offering a comprehensive understanding of the operational framework of the Anti-Fraud Unit and its role in tackling fraud within the region. This design helped to illuminate the complexities of fraud investigation in the specific context of the NSCDC.

3.2 Population of the Study

The population for this study includes all the seven (7) detectives within the Anti-Fraud Unit of the Nigerian Security and Civil Defence Corps (NSCDC) Oyo State Command. This group provided insights into the operational processes, challenges, and effectiveness of the Unit in handling fraud cases. Additionally, the study examined case files of fraud cases that have been investigated and closed by the Unit. The inclusion of both personnel and case documentation offers a well-rounded approach, allowing for a thorough understanding of both human and operational aspects of fraud investigation within the NSCDC. This combination of qualitative data from officer interviews and the analysis of case files enabled a comprehensive assessment of the Unit's performance and approach to combating fraud[2].

3.3 Sample and Sampling Techniques

This study employed a total enumeration sampling technique, meaning that all the seven (7) detectives within the Anti-Fraud Unit of the Oyo State Command of the NSCDC was included in the sample. This ensures that diverse perspectives from the officers was captured. Given the qualitative nature of the research, the focus was on detectives who have direct experience in investigating fraud cases. These officers are considered the most

Lead City University Ibadan DO NOT COPY

knowledgeable sources for understanding the practices, challenges, and operational frameworks of the Unit. In addition, purposive sampling was used to select twenty-seven (27) case files, particularly focusing on the most frequently occurring types of fraud cases handled by the Unit. This targeted approach is crucial for identifying patterns, examining common strategies, and gaining a deeper understanding of how fraud is managed within the Unit[3].

3.4 Description of the Research Instruments

For this study, two primary research instruments were used: a well-structured interview guide and a case file analysis framework. The interview guide was designed to gather detailed responses from the officers within the Anti-Fraud Unit of the Nigerian Security and Civil Defence Corps (NSCDC), and it consisted of 20 open-ended questions that were aligned with the research objectives. The guide was divided into five sections, each targeting a different aspect of fraud investigation and prosecution:

Section A explored the dynamics of fraud occurrence, delving into how fraud manifests within the NSCDC's operations.

Section B focused on the costs associated with fraud prosecution, considering both the financial and resource challenges the unit faces.

Section C investigated the tactics and strategies used by perpetrators to commit fraud, revealing common methods and approaches.

Section D analysed the characteristics of individuals who commit fraud, identifying patterns or profiles of offenders.

Lead City University Ibadan DO NOT COPY

Section E explored the time frames of fraud occurrences, investigating the duration and frequency of fraud cases.

In addition to the interview guide, the study employed a case file analysis framework, which involved a structured template to examine key elements of fraud cases handled by the NSCDC. The framework focused on critical case characteristics such as the type of fraud, file number, complainants' and suspects' statements, time frame of the case, investigation and prosecution procedures, and case outcomes and fact. This structured approach was to ensure consistency in the examination of case files and facilitate systematic data extraction and comparison.

By combining both the interview guide and case file analysis framework, this study aims to provide a comprehensive understanding of the operational dynamics within the NSCDC's Anti-Fraud Unit and the strategies used for investigating and prosecuting fraud cases. This dual approach also helped to capture insights from officers and from case records, contributing to a more holistic analysis of fraud prevention and prosecution within the organization[4].

3.5 Validity of Research Instrument

To ensure the validity of the interview guide, content validity was established through a thorough expert review process. Criminology and fraud investigation scholars were asked to evaluate the guide for its relevance, clarity, and alignment with the study's objectives and their feedback helped make necessary adjustments to ensure the questions were appropriate and comprehensive. After incorporating the required revisions, the interview guide was submitted to the project promoter for final review and approval. This process confirmed that

Lead City University Ibadan DO NOT COPY

the interview questions effectively addressed the research objectives and were suitable for eliciting insightful responses from the Anti-Fraud Unit officers[5].

3.6 Reliability of the Research Instrument

To enhance the reliability of the study, the recorded responses from the interviews, along with the field notes, undergone a thorough evaluation. The audio tapes and notes taken during the interviews were transcribed using TurboScribe and translated into written forms. These were done to ensure that no information was lost during the process. The transcription was carefully compared with the field notes to ensure consistency and accuracy in the data collected. To organize the data, responses with similar content or patterns were grouped together. When the data was transcribed using TurboScribe, it was analysed by listening to the audio recordings, then transforming and comparing the verbal responses into written text. These responses were studied in detail, identifying key points and organizing them into categories. The analysis focuses on identifying patterns and common contents within the data. Once patterns emerged, the data underwent criminological interpretation, which provided a deeper understanding of the responses in the context of the study's objectives. Additionally, consensus views, or commonly reported perspectives, were highlighted and harmonized in the findings. Content analysis was the primary method used for interpreting the qualitative data. This comprehensive approach, combining in-depth interviews and case file analysis, ensured the validity of the data and its relevance to the study's goals, allowing for a well-rounded understanding of fraud investigation within the NSCDC Anti-Fraud Unit Oyo State Command.

3.7 Method of Data Collection

Lead City University Ibadan DO NOT COPY

Data collection for this study was based on in-depth interviews with detectives of the Anti-Fraud and Case Files that have been investigate and closed.

In-Depth Interviews and Case Study: The researcher conducted interviews with all the seven (7) detectives within the Anti-Fraud Unit at the NSCDC Oyo State Command. These interviews explored their direct experiences with fraud investigations and prosecutions, available resources, and any operational challenges they face. The interviews were audio-recorded with prior consent from the participants and transcribed using the TurboScribe Software for detailed analysis. The goal was to capture diverse perspectives from respondent to better understand how fraud dynamics are handled within the Unit, providing an in-depth view of both successes and challenges in their operations. Also, the data collected from case files includes information on case characteristics, investigative methods, and fraud investigation outcomes, enabling the identification of patterns and trends.

3.8 Method of Data Analysis:

This study used content analysis for both the interview transcripts and the case files reviewed.

1. **Content Analysis for Interviews**: The interview data was analysed through content analysis by coding the transcripts to identify recurring contents and patterns. The data was categorized based on the research objectives, such as the common challenges faced by the officers, the investigative strategies they use, and their personal experiences in fraud investigation and prosecution. This method allowed for an in-depth exploration of the officers' insights, providing a nuanced understanding of both individual experiences and shared patterns that emerge across the interviews.

Lead City University Ibadan DO NOT COPY

2. **Content Analysis for Case Files**: A similar approach was applied to the case files. The analysis focused on identifying patterns in case characteristics, investigative methods, and the outcomes of fraud investigations. A coding framework aligned with specific fraud types and case outcomes was used to extract relevant data from the case files. This structured approach summarizes trends in fraud cases, highlighting investigative practices and offering insights into how fraud cases are handled by the Anti-Fraud Unit.

   The combination of content analysis from the interview data and content analysis of case files provides a comprehensive view of both the narrative perspectives of the officers and the structured data from the case files. This holistic approach deepens the study's understanding of fraud investigation and prosecution practices within the NSCDC's Anti-Fraud Unit.

3.9 Ethical Considerations

Ethical considerations were based on the principles of respect for persons, beneficence, and justice, as outlined by the American Psychological Association (APA). In practice, informed consent was obtained verbally and in writing, and participants were assured that no personal identifiable information would be disclosed. During case file reviews, data was accessed under supervision, and names, addresses, and any other personal identifiers of suspects, victims, or personnel mentioned in the records were excluded from the data analysis to maintain confidentiality. Digital and physical data storage adhered to strict security protocols, with sensitive files stored in encrypted formats and accessed only by the researcher.

Lead City University Ibadan DO NOT COPY

An official letter was submitted to the Commandant of the NSCDC Oyo State Command, outlining the study's objectives and requesting permission to conduct interviews and review relevant records. Following approval, informed consent was obtained from all the seven (7) detectives, before their involvement in interviews and the provision of access to documents. The detectives were informed about the purpose of the research, how the data would be used, and their right to withdraw at any point. Confidentiality was strictly maintained by ensuring that no names or photographs of participants appeared in the research.

For the review of case files, access was granted following approval by the Commandant, and the records were reviewed physically under the supervision of authorized personnel. Data extraction focused solely on non-identifiable details relevant to the study's objectives, ensuring anonymity. The files reviewed were purposively selected based on their relevance to the types of fraud being investigated. Data was recorded securely without taking any original files out of the NSCDC premises. Additionally, physical and digital copies of the records were handled securely, and access was limited strictly to the researcher.

Challenges During Data Collection

Several challenges arose during the research process. First, navigating bureaucratic protocols to secure approval for accessing NSCDC records caused initial delays. These delays were mitigated by submitting the researcher’s personal details for background checks and presenting an oral proposal of what the research is all about and also maintaining regular communication with the Commandant’s office.

Lead City University Ibadan DO NOT COPY

Additionally, some case files were heavily restricted due to their sensitive nature and to address this, physical supervision and alternative data sources, such as detective interviews, were used to gather relevant insights. Participant hesitation was another challenge, as some detectives were initially reluctant to share information due to concerns about confidentiality. This was addressed by reiterating assurances of confidentiality, providing clear explanations of the study's objectives, and emphasizing the academic nature of the research. Lastly, logistical constraints, such as restrictions on using digital devices of all sort or writing materials within the NSCDC office, required careful planning to ensure accurate data recording. Secure storage systems were employed to manage all digital and physical data, and encrypted files ensured data security.

Lead City University Ibadan DO NOT COPY

Endnotes

1. R. K. Yin, *Case Study Research and Applications*, Sage Publication, Inc**,** 2018, pp 319.
2. B. Dierckx de Casterlé, K. De Vliegher, C. Gastmans, & E. Mertens, E., C*omplex Qualitative Data Analysis: Lessons Learned from the Experiences with the Qualitative Analysis Guide of Leuven,* **Qualitative Health Research,** 31(6), 2021, pp.1083-1093.
3. G. K. Mweshi, & K. Sakyi, *Application of Sampling Methods for the Research Design,* **Archives of Business Review**–Vol, 8(11), 2020, pp.180-193.
4. E. Knott, A. H. Rao, K. Summers, & C. Teeger, *Interviews in the Social Sciences,* Nature Reviews Methods Primers, 2(1), 2022, p.73.
5. A. Gani, N. Imtiaz, M. Rathakrishnan, & H.N. Krishnasamy, *A Pilot Test for Establishing Validity and Reliability of Qualitative Interview in the Blended Learning English Proficiency Course.* **Journal of Critical Reviews**, 7(05), 2020, pp.140-143

Chapter Four

Results and Discussion of Findings

4.1 Demographic Data Analysis

This chapter presents the findings from the data collected during the study, which involved both interviews and case file analysis. The study drew insights from two main sources: interviews with all the seven (7) detectives from the Anti-Fraud Unit of the Nigerian Security and Civil Defence Corps (NSCDC) and a detailed review of twenty-seven (27) case files handled by the Unit. The seven (7) detectives who participated in this study are currently serving in the NSCDC Anti-Fraud Unit in Oyo State Command. They were purposively selected based on their direct involvement in investigating fraud cases and their experience handling complex investigations.

Collectively, the seven (7) detectives in the Anti-Fraud Unit have served an average of 8 to 10 years, demonstrating extensive experience in investigating fraud-related cases. Their ranks within the Unit highlight a well-defined hierarchy, ensuring effective distribution of roles and responsibilities. Among them, one detective holds the rank of Assistant Commandant of Corps (ACC), while another serves as a Superintendent of Corps. The team also includes a Deputy Superintendent of Corps (DSC), two Assistant Superintendents of Corps I (ASC I), an Assistant Superintendent of Corps II (ASC II), and an Inspector of Corps (IC). This diverse range of ranks underscores the Unit's organizational structure, which combines strategic leadership with operational expertise to combat fraud effectively. This diversity in ranks reflects a hierarchical structure within the Unit, where roles and responsibilities are distributed based on rank and expertise. The combination of senior officers and mid-level detectives ensures that the Unit benefits from both strategic oversight and operational

Lead City University Ibadan DO NOT COPY

capabilities. Additionally, the seven detectives of the Unit comprise of two (2) females and five (5) males, further contributing to its diversity, balance**.** This composition enhances collaboration by integrating different perspectives and experiences, strengthening the Unit's ability to tackle fraud investigations effectively.

A total of twenty-seven (27) case files were thoroughly reviewed during the study, with a focus on the two most prevalent types of fraud handled by the Anti-Fraud Unit. Obtaining by False Pretence (OBT) emerged as the most common type of fraud, accounting for 16 cases, which represents 80% of the reviewed files. Visa Racketeering (VR) was the second most frequent, comprising 11 cases, representing 55% of the total. The case files provided crucial insights into the strategies employed by fraudsters and the investigative practices of the Unit. The review focused on patterns such as the nature of the fraud, the profiles of perpetrators, and the outcomes of investigations.

The interview guide was carefully crafted to align with the study's research questions and objectives. It explored several critical aspects of fraud investigation, including the dynamics of fraud occurrence within the NSCDC dataset in Ibadan, Nigeria, the cost of prosecuting fraud cases and how it influences investigation strategies and outcomes, the tactics and strategies commonly employed by fraud perpetrators, the characteristics of individuals or entities typically involved in fraudulent activities, and specific timeframes or patterns in the occurrence of fraudulent cases.

The data collected were analysed using content analysis**,** which provided a systematic understanding of the findings. This method allowed for a comprehensive examination of the NSCDC Anti-Fraud Unit's investigative practices, shedding light on the nature of the cases

Lead City University Ibadan DO NOT COPY

handled, the strategies employed in fraud detection and prosecution, and the challenges encountered in executing their mandate.

4.2 Presentation of Data

4.2.1 Research Questions

Research Question One:

Dynamics of Fraud Occurrence in Oyo State

In the data collected, the detectives were asked to provide detailed insights based on their experience in the Antifraud Unit into the types of fraud commonly investigated within the Anti-Fraud Unit in Ibadan. The most frequently mentioned fraud type was Obtaining by False Pretences (OBT) and Visa Racketeering, where victims are deceived into paying for fake visas or false promises of job opportunities. For instance, OBT was described as a dominant issue within the Unit's caseload due to its prevalence in the region, which also involves the use of digital platforms to defraud individuals or organizations. The respondents who are detectives in the Unit highlighted OBT activities such as phishing, fake alert, email scams, and ATM-relate frauds, reflecting the increasing reliance on technology by criminals. In addition, respondents also discussed cases of economic sabotage and this includes fraudulent land sales, where one piece of land is sold to multiple buyers, and cases where individuals fail to deliver goods or refund payments as promised. These cases were seen as affecting not only individual victims but also contributing to broader economic instability. A senior detective disclosed:

> The most prominent ones I have investigated are known as OBT and VR, that is Obtaining under False Pretences and Visa Racketeering. Those are the major ones we have in this office. **29/07/24. IDI. ANTIFRAUD. NSCDC. Male. ASSISTANT COMMANDANT OF CORPS**

Lead City University Ibadan DO NOT COPY

Furthermore, another respondent who has investigated cases of obtaining money, assets, or property under false pretences explained that the most common offences encountered by the NSCDC Anti-Fraud Unit include Obtaining by False Pretences (OBT) (Cybercrime), and Visa Racketeering. He gives examples which include but not limited to misusing funds meant for a specific purpose, absconding with entrusted assets like vehicles or land, and failing to fulfil agreed obligations. He explains:

> The common offences we see here in Antifraud include OBT, which stands for Obtaining by False Pretence, which can be a cybercrime, as well as visa racketeering. OBT involves situations where someone collects money or assets under the guise of using them for a specific purpose but diverts them for personal gain. For example, they may promise to buy something or provide a service but fail to deliver, or they may abscond with entrusted property like vehicles or land. Essentially, it's about obtaining money or assets through deceit. **29/07/24. IDI. ANTIFRAUD. NSCDC. Male. SUPRINTENDENT OF CORPS**

Building on the discussion of common types of fraud, the detectives emphasized the prevalence of Obtaining by False Pretences (OBT**)** in Ibadan, Oyo State. A detective highlighted that OBT cases involving visa-related fraud are becoming increasingly common in the city of Ibadan. He averred thus:

> OBT is very rampant in Ibadan. When it comes to traveling, everyone wants to 'JAPA' (travel abroad). We have many agents in town, both legitimate and fraudulent, and everyone is trying to find a way to leave the country. The number of fraudulent agents is increasing. Most of them are not genuine. We've investigated cases where people lost their money to these agents. We've also investigated fake visas being issued. So, in Ibadan, OBT remains the major type of fraud, and its occurrence is on the rise. **29/07/24. IDI. ANTIFRAUD. NSCDC. Male. ASSISTANT COMMANDANT OF CORPS**

Lead City University Ibadan DO NOT COPY

Apart from the Assistant Commandant, an Assistant Superintendent highlighted that fraud in Ibadan takes various forms, with Obtaining by False Pretences (OBT) being the most prevalent. In particular, it often involves phone theft, where fraudsters exploit stolen SIM cards to access victims' bank accounts, siphon money, or borrow funds in their name and these incidents are especially common in areas like Bodija and Mokola, Gate and Agbowo typically during late hours. He explains:

> So, the trend that is very common in Ibadan involves more than one type of fraud. The first one is OBT, which is very prevalent and easy to notice and which is often carried out through the theft of victims' phones. Fraudsters use stolen SIM cards to siphon money from accounts, borrow money, or gain unauthorized access to bank accounts if the victim is not careful. This type of fraud is especially common in areas like Bodija, Mokola, Gate and Agbowo, particularly during closing hours when phone theft incidents are frequent. For instance, fraudsters may use the victim's phone to borrow money or perform unauthorized transactions in the victim's name. This type of fraud has become increasingly common in these areas. **29/07/24. IDI. ANTIFRAUD. NSCDC. Male. ASSISTANT SUPERINTENDENT OF CORPS I**

When asked about the factors contributing to the occurrence of fraud in cases they have investigated, the detectives explained that it is influenced by several interconnected factors, including those related to the victims. They highlighted the role of internet acquaintances, which can be shaped by issues such as illiteracy and the economic situation of the country, leading to desperation and a desire to leave the system. Each of these factors contributes uniquely to the prevalence of fraud, with some working in combination to create an environment where fraud thrives. One of the most significant factors contributing to fraud is the limited knowledge of ICT and cybersecurity practices, particularly among older

Lead City University Ibadan DO NOT COPY

generations and many victims fall prey to scams involving One-Time Passwords (OTPs) or other digital exploits because they are not familiar with how to secure their banking and personal information. Fraudsters exploit this lack of awareness by deceiving victims into compromising their accounts. This gap in knowledge creates a vulnerability that is easily exploited, especially as digital platforms become more central to financial transactions. As one detective noted:

> You see, one of the key factors is that people have limited knowledge of the ICT world. For instance, the "Gen Z" generation is very proficient when it comes to gadgets, whereas people of my generation are not as knowledgeable. For example, when they send OTP codes to people, fraudsters trick them into sending those codes, and before you know it, their accounts are wiped out. ***(29/07/24, IDI, ANTIFRAUD. Male, ASSISTANT COMMANDANT OF CORPS)***

Furthermore, another female detective explains how financial destitution has created an environment where individuals, particularly youths, see fraud as a means of survival. She emphasized that many people resort to fraudulent activities as a way to escape financial struggles, economic hardship or meet societal expectations for wealth. She remarked:

> Poverty, Unemployment. Poverty is the major thing because there is no job, there is no money. In Nigeria today, things are very difficult, and many people want to be rich without working. ***(29/07/24, IDI, ANTIFRAUD, Female, ASSISTANT SUPERINTENDENT OF CORPS I)***

Lead City University Ibadan - NOT COPY

Desperation, particularly the desire to migrate abroad for better opportunities (popularly referred to as the "Japa syndrome"), is a key driver of fraud. Fraudsters exploit this desperation by making enticing promises of cheap visas or travel arrangements, preying on individuals who are eager to leave the country but lack sufficient funds or knowledge. A senior detective shared:

> Many victims of fraud fall prey because they are desperate to travel abroad. These fraudsters take advantage of this desperation by making enticing promises. For example, they might tell someone, 'If you have ₦100,000 don't worry, we'll help you do American Visa.' In the end, the fraudsters collect money from multiple victims but never follow through. ***(29/07/24, IDI, ANTIFRAUD, Male, DEPUTY SUPERINTENDENT OF CORPS)***

Fraud has undergone significant changes over the years, evolving from basic scheme like Obtaining by False Pretences (OBT) to highly sophisticated digital and cybercrime methods. Detectives of the NSCDC Anti-Fraud Unit emphasized that technological advancements, particularly in artificial intelligence (AI) and digital banking systems, have contributed to this transformation and these developments have not only expanded the scope of fraudulent activities but have also made them harder to detect and prevent. The advent of technology, particularly AI, has introduced new tools for fraudsters to exploit unsuspecting victims and there were cases where fraudsters used AI to manipulate voice and video, creating a false sense of trust among their targets. This level of sophistication marks a departure from traditional fraud methods and underscores the importance of enhancing technological literacy among the general public. A detective explained:

Lead City University Ibadan DO NOT COPY

> Fraud is evolving with the rise of technology, especially with this AI thing. We recently handled a case where AI was used to manipulate both voice and video, making it hard for people to detect the fraud. Technology is only making things worse, and many people fall victim to these types of scams ***(29/07/24, IDI, ANTIFRAUD, Male, SUPERINTENDENT OF CORPS)***

The shift from physical transactions to cashless systems has simplified fraudulent activities. Cyber fraud, such as account hacking and unauthorized transfers, has become more prevalent but fraudsters now bypass traditional theft methods by exploiting digital banking systems and cashless policies. For instance, money is often transferred to Point-of-Sale (POS) machines and converted to cash within minutes, leaving little trace for investigators to follow. A junior detective avers:

> Fraud has evolved significantly because it's much easier now. Once money is transferred from one account to another, fraudsters can take it to a POS, exchange it for cash, and it's done. This method is far easier than physically breaking into someone's home to steal money. ***(29/07/24, IDI, ANTIFRAUD, Male, INSPECTOR OF CORPS)***

Furthermore, fraud has not only evolved in complexity but has also increased in frequency and this rise is attributed to the growing accessibility of technology and the lack of productive engagement for many youths. Despite efforts to combat fraud, societal issues such as unemployment and the normalization of a "get-rich-quick" mentality continue to drive individuals toward fraudulent practices. As one detective puts it:

> The efforts we've made here to combat crime, especially fraud, should have led to a significant reduction. But instead, the problem is growing daily. The lack of positive and productive engagement for the youth is a major issue we're facing. ***(29/07/24, IDI, ANTIFRAUD, Male, ASSISTANT SUPERINTENDENT OF CORPS I)***

Lead City University Ibadan DO NOT COPY

ICT advancements, artificial intelligence, and socio-economic factors are interconnected in the evolvement of fraud as technologies has not only made fraud easier and faster but has also created new vulnerabilities for victims who lack the necessary knowledge to protect themselves. At the same time, societal pressures, such as unemployment and the glorification of wealth, drive individuals to exploit these vulnerabilities and there is a need for increased public awareness and enhanced technological literacy to mitigate the risks posed by evolving fraud tactics.

Case Review on Dynamics of Fraud Occurrence

Fraudulent activities investigated by the NSCDC Antifraud Unit in Ibadan reflect a dynamic interplay of socio-economic pressures, technological gaps, and systemic vulnerabilities. Among the most prevalent forms of fraud are Obtaining by False Pretences (OBT) and Visa Racketeering (VR), both of which exploit trust and desperation. For instance, **File No. 492 (2021)** highlights how trust can be weaponized in OBT cases. In this case, the suspect diverted ₦1,050,000 entrusted for a financial transfer to family members abroad. Weak accountability systems, compounded by socio-economic pressures, provided the opportunity and rationalization for this fraudulent act. This aligns with the Fraud Triangle, where the "opportunity" created by poor monitoring systems enabled the crime.

Similarly, cases such as **File No. 729 (2022)** emphasize how migration desperation is exploited in Visa Racketeering. Fraudsters often lure victims through false promises of visas, leveraging deceptive advertisements to target those eager to migrate. As described in this case, the victim lost ₦500,000 to a fraudulent agent offering a Canadian visa, only discovering the fraud at the airport. The Routine Activity Theory underscores this

Lead City University Ibadan DO NOT COPY

vulnerability, where a motivated offender exploits suitable targets in the absence of capable guardianship.

The following table summarizes key cases from the NSCDC dataset, illustrating the types of fraud, their contributing factors, and theoretical underpinnings.

Table 4.1: Dynamics of Fraud Occurrence within the NSCDC Dataset

Case Type	File. No. & Year	Key Fact of the Case	Contributing Factors	Theoretical Link	Outcome/Prosecution Details
(OBT)	F.N. 492 (2021)	Suspect diverted ₦1,050,000 entrusted for transfer to family members in the USA for personal use.	-Weak accountability systems - Socio-economic pressure (financial strain)	**Fraud Triangle:** Opportunity due to low monitoring **Routine Activity Theory:** Absence of capable guardianship in entrusted fund management	Suspect confessed and Payment schedule created after ADR and money was recovered
(VR)	F.N. 729 (2022)	Victim paid ₦500,000 for a Canadian Visa based on a fraudulent radio ad. Visa was revealed to be fake at the airport	- Economic hardship (migration desperation) - Deceptive advertising targeting vulnerable individuals	**Fraud Triangle:** Pressure from financial/economic desperation and Opportunity due to lack of oversight in Visa service providers	Suspect confessed; restitution of ₦500,000 via legal undertaking and money was recovered through a payment schedule

Source: Researcher's Computation, 2025

Lead City University Ibadan DO NOT COPY

4.2.2 Research Question Two:

Cost of Prosecuting Fraud Case and Investigation Strategies and Outcomes

The cost of prosecuting fraud poses significant challenges for the Anti-Fraud Unit, directly influencing their strategies and the outcomes of investigations. Although, fraud investigation

is one of the core mandates of the NSCDC, financial constraints significantly hinder their operations and these constraints affect logistics, inter-agency collaborations, and the ability to pursue cases beyond local jurisdictions. Furthermore, the burden of prosecution costs is often shifted to complainants, who may abandon cases due to financial and emotional strain. Detectives highlighted that the government does not cover the expenses for essential processes such as obtaining court orders, conducting tracking operations, or handling inter-state logistics. As a result, complainants are often required to bear these costs, which can discourage them from pursuing their cases to resolution. A female detective explains:

> When the complainant brings a case to us, we will tell them the cost. For instance, visa racketeering costs differ from OBT phone tracking. The government is not covering most of the costs for us, so complainants must pay for things like court orders and other expenses. I cannot use my salary to pay for them**.** For some complainants, they say, 'Please help us!' But we cannot use our salaries to finance them. Some people pay willingly, but others simply cannot afford it, leaving us with no choice but to abandon the case ***(29/07/24, IDI, ANTIFRAUD Female, ASSISTANT SUPERINTENDENT OF CORPS I)***

While some wealthier complainants are willing and able to fund their cases, lower-income individuals often abandon their claims due to financial constraints. This creates inequality in access to justice, where only those who can afford the associated costs can pursue cases to their conclusion. The financial burden of investigations significantly affects case outcomes, with many promising cases abandoned due to lack of funds. For instance, tracking a suspect to another state or securing advanced documentation (e.g., KYC information from banks) often becomes financially prohibitive when there is no finance.

Furthermore, a senior detective lamented on how financial constraints have forced the Unit to adapt its strategies, prioritizing cases that are feasible within their budget or referring cases to

Lead City University Ibadan DO NOT COPY

other NSCDC offices in the relevant jurisdictions. For example, investigations that require travel to other states often depend on the financial capability of the complainant to cover transportation and logistics costs. Without such support, cases may be shelved or delayed indefinitely and in cases where complainants cannot afford these costs, investigations are either delayed, referred to another jurisdiction, or abandoned altogether and these has created a disparity in outcomes, with wealthier complainants having better chances of seeing their cases pursued. The detective shared an illustrative example:

> I handled a case involving a church with over 100 million naira at stake. The church could afford to cover the expenses for us to travel to Ilorin and Lagos to pursue the case. However, in another instance, a complainant couldn't foot the bill for inter-state logistics, and we had to refer the case to our colleagues in that other state. ***(29/07/24, IDI, ANTIFRAUD, Male, ASSISTANT COMMANDANT OF CORPS)***

Another significant issue is the abandonment of cases when the cost of investigation outweighs the value of the fraud involved and the logistical costs of apprehending suspects across multiple locations exceed the amount of money lost by the complainant. In such cases, investigations are often terminated prematurely. More often than not, complainants often abandon cases due to the prolonged financial and emotional strain associated with the justice process. Delays in obtaining results, coupled with the high costs of pursuing cases, frustrate complainants and lead to disinterest over time. One detective explained:

> I've seen cases where complainants initially pursued fraud cases but eventually dropped them due to delays in the justice system. They lose interest, feeling the financial and emotional burden isn't worth it anymore. ***(29/07/24, IDI, ANTIFRAUD, Male, DEPUTY SUPERINTENDENT OF CORPS)***

Lead City University Ibadan DO NOT COPY

A Justice that is delayed can be said to be a justice that might be denied because of finance. Financial limitations are compounded by inefficiencies in the justice system, such as delays in court processes and the limited availability of judges. These delays discourage complainants, who often withdraw their cases after prolonged periods of waiting. A detective avers:

> You see, if funds are released as appropriate, it will send you to pursue cases to the letter. There have been financing issue, I will not lie to you, but I will still go back to the delay in our justice system. We still have cases from three years ago stuck in court because of delays and awaiting cases, we don't have much judges to even decide most of them. Complainants often lose interest and stop following up because the process is too slow and costly, like federal high court now, the whole of Oyo State, they have only two judges in federal high court, you can imagine, and two judges that look at all the federal cases that is what they have, their complaint is that they have so numerous cases in front of them, so it delays the prosecution of those cases, even after we have investigated *(***29/07/24, IDI, ANTIFRAUD, Male, DEPUTY SUPERINTENDENT OF CORPS)**

Due to inflation and resource allocation challenges, budgetary provisions often fail to account for inflation, reducing the real value of funds available for investigations. This leads to logistical inefficiencies, such as the unavailability of patrol vehicles or fuel, which further hinder operations and a lack of immediate resources can delay responses to fraud cases, making it harder to apprehend suspects in real-time. A junior detective emphasized:

> If resources are allocated to us, inflation over time will reduce their value. I think this needs to be considered, and allocations should be substantial. Additionally, comparing last year's expenses to this year's needs is important. Since budgets are planned in advance, they are not adjusted afterward. By the time the allocated funds become available, inflation may have increased costs, affecting the resources budgeted for fighting fraud. If logistics and resources are provided immediately, investigations would

Lead City University Ibadan DO NOT COPY

be faster and more efficient. **(29/07/24, IDI, ANTIFRAUD, Male, INSPECTOR OF CORPS)**

Case Review on the Cost of Prosecuting Fraud Case and Investigation Strategies and Outcomes

Investigating and prosecuting fraud cases within the NSCDC often involve substantial financial and logistical challenges. These constraints directly impact case outcomes and the strategies employed by investigators. The cost of fraud investigations is often transferred to complainants, many of whom lack the financial capacity to fund extensive processes such as interstate tracking or obtaining court orders. **File No. 851 (2022)** highlights a case where the complainant, defrauded of ₦1,380,000 through a fake financial platform, could not afford the logistics for investigators to track the suspect to Lagos. As a result, the investigation was stalled, and the case was abandoned. Similarly, **File No. 731 (2023)** involved an elderly woman who fell victim to a Visa scam, losing ₦ 2,546,258 ($3991). The cost of tracking the fraudster across multiple states exceeded her capacity, leaving the suspect untraceable. These cases highlight systemic inequities, as victims with limited financial resources are more likely to experience delays or case abandonment, resulting in unequal access to justice. Additionally, the financial and logistical challenges faced by the NSCDC Anti-Fraud Unit expose systemic gaps that hinder the effectiveness of fraud investigations and prosecutions. These challenges align with the Routine Activity Theory, where the absence of capable guardianship (due to resource constraints) creates opportunities for offenders to exploit.

Lead City University Ibadan DO NOT COPY

The following table summarizes specific cases that illustrate the financial and logistical challenges faced by the NSCDC in investigating and prosecuting fraud cases.

Table 4.2: Challenges in the Cost of Fraud Investigations and Prosecutions

Case Type	File. No & Year	Key Fact of the Case	Contributing Factors	Theoretical Link	Outcome/Prosecution Details
(OBT)	F.N. 851 (2022)	The suspect used a fake financial platform to defraud the complainant of ₦1,380,000, then relocated to Lagos, leaving the complainant unable to recover funds.	Complainant couldn't fund interstate travel expenses for investigators to track the fraudster to Lagos.)	**Routine Activity Theory:** Absence of capable guardianship (due to resource constraints)	Investigation stalled, and case eventually abandoned.
(VR)	F.N. 731 (2023)	Victim paid ₦ 2,546,258 ($3991) for admission. Visa was denied because suspect refused to disburse the ($3991) to the school account.	Case delayed for several months because funds for bank tracking not readily available. Suspect transferred money to cryptocurrency wallet.	**Routine Activity Theory:** Absence of capable guardianship (due to resource constraints)	Investigation stalled, and case eventually abandoned.

Source: Researcher's Computation, 2025

4.2.3 Research Question Three:

Tactics and Strategies Commonly used in Perpetrating Fraud

Lead City University Ibadan DO NOT COPY

Fraudsters frequently capitalize on victims' limited knowledge of digital security and financial systems. Many individuals remain unaware of basic cybersecurity protocols, such as safeguarding OTP codes, PINs, or passwords. This lack of awareness creates an entry point for fraudsters, enabling them to exploit victims with minimal effort. For instance, fraudsters often send deceptive messages posing as financial institutions or service providers. These messages trick victims into revealing sensitive information, such as their banking credentials, under the guise of resolving account issues or offering rewards. A detective emphasized:

> Fraudsters capitalize on people's ignorance. For instance, they send OTP codes or fake alerts to individuals. Many people unknowingly share these details, allowing fraudsters to gain unauthorized access to their accounts. With new technologies like AI, they can even mimic the voices of familiar individuals to deceive their victims. **(29/07/24, IDI, ANTIFRAUD, NSCDC, Male, ASSISTANT COMMANDANT OF CORPS)**

When asked, he further provided a case study involving a fraudulent app that mimicked a popular financial service:

> Fraudsters create fake versions of banking apps that are almost identical to the real ones. When users unknowingly log in, their credentials are captured, enabling fraudsters to access and wipe their accounts. In one case, we apprehended a suspect who falsified apps and targeted customers of a fintech company. **(29/07/24, IDI, ANTIFRAUD, NSCDC, Male, ASSISTANT COMMANDANT OF CORPS)**

Fraudsters also use impersonation and psychological manipulation to exploit victims' trust as it remains one of the oldest yet most effective fraud strategies. Fraudsters pose as friends, family members, or even trusted officials to manipulate victims into transferring money or sharing sensitive information. In some cases, they target victims at ATMs or public spaces,

Lead City University Ibadan DO NOT COPY

posing as security personnel offering assistance. By exploiting interpersonal relationships and psychological vulnerabilities, they manipulate victims into providing sensitive information or transferring funds. A detective explained:

> The thing is that hackers often create deceptive emails or messages that they send to devices, such as computers or phones. If you are not very careful, you might think the email originated from a trusted site. Once you respond or click on the link, they gain access to your device, making it easy for them to steal all your information. For example, a woman was working on her computer and saw a link from her husband. She thought it was from a reliable source and clicked on it. After that, her Facebook account was hijacked. The hacker then sent messages to all her contacts, demanding money from them. A similar thing always happens with WhatsApp. **(29/07/24, IDI, ANTIFRAUD, NSCDC, Male, DEPUTY SUPERINTENDENT OF CORPS)**

Fraudsters often rely on intermediaries, such as POS operators or individuals who unknowingly facilitate their schemes. By using accounts and devices not directly linked to them, fraudsters create layers of anonymity, complicating investigations. Also, the use of cryptocurrency wallets and gift cards is a growing trend among fraudsters, as these methods provide anonymity and are difficult to trace. Fraudsters convert stolen funds into cryptocurrency and then use untraceable platforms to exchange them for gift cards, bypassing traditional banking systems. A detective shared:

> Fraudsters have moved away from using traditional banking systems and now rely on methods like cryptocurrency and gift cards to avoid being caught. In one case, a fraudster stole 1.2 million Naira, converted it into cryptocurrency, and then into gift cards tied to foreign countries like in Mexico and New Zealand. This made it nearly impossible to track the funds. **(29/07/24, IDI, ANTIFRAUD, NSCDC, Male, ASSISTANT SUPERINTENDENT OF CORPS I)**

Lead City University Ibadan DO NOT COPY

Fraudsters often prey on individuals who are desperate or in unfamiliar situations. Schemes like visa racketeering take advantage of victims' eagerness to migrate abroad, promising fake visas or work permits in exchange for money. Similarly, lost or stolen phones provide opportunities for fraudsters to access linked accounts and steal funds. A detective explains:

> Fraudsters capitalize on lost phones, especially if the device is linked to a bank account. Once a phone is lost, quick action is critical—such as reporting the loss to us or the police, blocking the SIM, and notifying the bank to secure linked accounts. If not promptly addressed, fraudsters can bypass also, many people desperate to travel abroad are lured into scams where fraudsters promise them visas for a fee. These victims often lose significant amounts of money without receiving any assistance. **(29/07/24, IDI, ANTIFRAUD, NSCDC, Male, INSPECTOR OF CORPS)**

Case Review on Tactics and Strategies commonly used in perpetrating fraud

The NSCDC Anti-Fraud Unit has identified a wide range of sophisticated tactics and strategies used by fraudsters in Oyo State. These methods leverage technological advancements, psychological manipulation, and systemic vulnerabilities to exploit unsuspecting victims. Fraudsters frequently use advanced technology, such as fake apps and artificial intelligence (AI), to deceive their victims. **File No. 837 (2022)** involved a case where a victim logged into a fake banking app that mirrored a legitimate one, unknowingly sharing their credentials. The fraudster used these details to access and empty the victim's account. Similarly, **File No. 792 (2023)** highlights how AI-powered voice manipulation was employed to mimic a trusted relative's voice, convincing the victim to transfer ₦5.5 million. These cases emphasize the increasing sophistication of fraud schemes, which challenge investigators to keep pace with technological developments. Similarly, **File No. 731 (2023)**

Lead City University Ibadan DO NOT COPY

highlights the use of cryptocurrency to launder stolen funds, a tactic that exploits the anonymity of digital currencies and the lack of regulatory oversight.

Fraudsters rely heavily on psychological manipulation to exploit their victims' trust. **File No. 837 (2022)** also involved ATM card swapping, where the suspect used distraction techniques to replace the victim's card with a similar-looking one. These strategies prey on victims' lack of awareness and urgency in public spaces. These findings align with the **Routine Activity Theory**, which emphasizes how motivated offenders exploit suitable targets in the absence of capable guardianship. The table below summarizes specific cases illustrating the diverse tactics and strategies employed by fraudsters in Oyo State, as investigated by the NSCDC.

Lead City University Ibadan DO NOT COPY

Table 4.3: Fraud Tactics and Strategies Identified in NSCDC Cases

Case Type	File. No & Year	Key Fact of the Case	Contributing Factors/ Tactics/Strategies	Theoretical Link	Outcome/Prosecution Details
(OBT)	F.N. 837 (2022)	Fraudster developed a fake app resembling a legitimate financial app. Victim logged in, unknowingly sharing credentials, which were used to empty the account.	Creation of fake banking apps to collect victims' credentials.	**Routine Activity Theory:** motivated offenders exploit suitable targets in the absence when guardianship is low.	Suspect apprehended and charged to court.
(OBT)	F.N. 792 (2023)	Victim fell prey to voice manipulation scam and transferred ₦5.5 million. Suspect posed as a family member.	Use of AI-powered voice manipulation to mimic trusted individuals and demand funds.	**Routine Activity Theory:** motivated offenders exploit suitable targets in the absence when guardianship is low	Investigation delayed due to lack of advanced tracking tools; suspect remains at large.
(OBT)	F.N. 837 (2022)	Victim lost ₦300,000 via ATM card swapping and the suspect Denied involvement, claiming the card was sold to them by someone else.	Suspect swapped the victim's card at an ATM using sleight of hand during a staged "helpful gesture."	**Routine Activity Theory:** motivated offenders exploit suitable targets in the absence when guardianship is low.	Suspect apprehended; funds partially recovered.
(VR)	F.N. 731 (2023)	Victim lost ₦ 2,546,258 ($3991)	Use of cryptocurrency to	**Routine Activity Theory:**	Case stalled as funds were converted into

Lead City University Ibadan DO NOT COPY

	admission scam. and suspect used anonymous wallets to launder money.	launder stolen funds; conversion of fiat currency to crypto for untraceable transactions.	motivated offenders exploit suitable targets in the absence when guardianship is low	cryptocurrency and gift cards, making tracking difficult due to a lack of advanced tools.

Source: Researcher's Computation, 2025

4.2.4 Research Question Four:

Characteristics of Individuals typically involved in committing fraud

Fraud perpetrators exhibit diverse characteristics influenced by their socio-economic circumstances, motivations, and operational strategies. Common traits, behavioural patterns, and environmental factors were associated with fraudulent activities. This underscores the complex interplay between individual, systemic, and societal factors in facilitating fraudulent behaviour. Also, recurring patterns in their behaviour, appearance, and methods of operation, reveal distinct profiles that aid law enforcement in identifying and addressing them. Many fraudsters rationalize their actions as a response to systemic inequities, seeing fraud as a survival strategy rather than a crime.

Fraud perpetrators often share a common desire for financial gain, driven by socio-economic hardships, poverty, and unemployment. Many are young individuals, predominantly in their late teens and early adulthood, who resort to fraudulent activities as a means of attaining quick wealth and social validation. A senior detective noted that these individuals are typically driven by societal pressures to achieve financial success, which is glorified within their communities. He described the obsession with "fast money":

> Fraudsters don't want to work but they want quick money; they are driven by greed and the hunger for wealth. They

Lead City University Ibadan DO NOT COPY

> want to chill with the big boys, drive big cars, and wear flashy clothes without working for it. Poverty and unemployment also play a significant role. People feel frustrated because there are no opportunities, so they justify fraud as a way to survive. People say, 'I'm a graduate without a job; how do I survive? **(29/07/24, IDI, ANTIFRAUD, NSCDC, Male, ASSISTANT COMMANDANT OF CORPS)**

Fraudsters are often identifiable by their ostentatious lifestyles and distinct appearances, which serve as red flags for law enforcement. A detective described them as flashy individuals who prefer luxurious cars, designer clothing, and high-profile social engagements. This behaviour aligns with the Fraud Triangle Theory's concept of rationalization, where perpetrators justify their actions by blaming systemic inequality or societal neglect. Additionally, they tend to cluster in shared apartments and form social groups that amplify their operations. He described these characteristics:

> We've noticed that many fraudsters prefer living in quiet, less conspicuous areas, such as around new development sites. In Ibadan, we see them—young men living together in flats, sharing apartments where rent is unusually high. They dress flamboyantly, with extravagant hairdos and outfits, and spend money lavishly on clubbing and big hotels. It's easy to identify them; they stand out like goldfish in an aquarium. **(29/07/24, IDI, ANTIFRAUD, Male, ASSISTANT SUPERINTENDENT OF CORPS I)**

He further specified the age range. He continued:

> Most of them are youths, often aged 18 to 30, including university students and even secondary school pupils. They cluster in places where they can blend into the environment and avoid scrutiny. These areas are hotspots for fraud, and accessing them requires strategic measures. Their outfits, their hairdos, their lifestyle—it's all excessive. They live in expensive apartments and frequent clubs. They're easy to profile, **(29/07/24, IDI, ANTIFRAUD, Male, ASSISTANT SUPERINTENDENT OF CORPS I)**

Lead City University Ibadan DO NOT COPY

Most fraud cases are facilitated by bank staff or employees within organizations, particularly in financial institutions. Employees in sensitive roles, such as cash handling or account management, are sometimes manipulated by fraudsters who offer financial incentives or exploit weak internal controls. Most banks manipulate their internal controls and regular audits which often lead to risk of compromise. A detective explains:

> Insiders in financial institutions especially those occupying the roles at the Forex table. They are very philanthropic—they give out money easily, creating a bond. In banks, some insiders assist fraudsters by providing account details or facilitating unauthorized transactions, they're like the collaborators. Without their aid, all these things we are talking about wouldn't really be as widespread as they are. For instance, a bank manager was involved in draining a customer's account through fraudulent transfers. Junior staff often find it hard to challenge their superiors, allowing such schemes to persist. **(29/07/24, IDI, ANTIFRAUD, NSCDC, Male, INSPECTOR OF CORPS)**

Case Review on Characteristics of Individuals typically involved in committing fraud

Fraudsters are predominantly young males aged 18 to 35, often driven by economic hardships and societal pressures. They are typically unemployed or underemployed, seeking quick financial success. **File No. 749 (2022)** highlights a suspect who displayed a flamboyant lifestyle, including luxury vehicles and high-end fashion, without a verifiable source of income. These individuals often rationalize their actions, citing systemic inequities or lack of job opportunities, aligning with the **Fraud Triangle Theory's** pressure element.

Insider involvement in financial institutions remains a significant enabler of fraud. **File No. 1052 (2024)** and **File No. 969 (2023)** illustrate cases where technology savvy individuals through social media and bank employees provided fraudsters with unauthorized access to customer accounts, highlighting systemic vulnerabilities. High-ranking officials and junior staff alike exploit their positions, often collaborating with external fraud networks to execute

Lead City University Ibadan DO NOT COPY

sophisticated schemes. The findings reveal that fraudsters are opportunistic, resourceful, and driven by socio-economic pressures.

The table below provides a summary of specific cases highlighting the characteristics of fraud perpetrators, as investigated by the NSCDC in Oyo State.

Table 4.4: Characteristics of Fraud Perpetrators Identified by NSCDC

Case Type	File. No & Year	Key Fact of the Case	Contributing Factors/Perpetrator Characteristics	Theoretical Link	Outcome/Prosecution Details
(VR)	F.N. 749 (2022)	Suspect was living a flamboyant lifestyle with no clear source of income and denied allegations of fraud.	Young males (aged 18-35), flashy lifestyle (luxury cars, designer clothes). He purchased high-end vehicles and living in luxury apartments.	**Fraud Triangle Theory's** rationality of their actions, citing lack of job opportunities.	Suspect claimed to be a visa agent and was apprehended in a luxury apartment and his assets were confiscated.
(OBT)	File No. 1052 (2024)	Fraudster gained access to victims' banking details via SIM card cloning and claimed SIM card manipulation was unintentional.	Highly skilled in ICT; young, technologically savvy individuals exploiting weak security measures.	**Fraud Triangle Theory's** rationality of their actions, citing lack of job opportunities.	Suspect apprehended; victims educated on digital security.
(OBT)	File No. 969 (2023)	Senior bank officer exploited their access to customer accounts,	Involvement of high-ranking officials; insider fraud exploiting trust in institutional frameworks.	**Fraud Triangle Theory's** of the opportunistic nature of	Investigation stalled due to lack of cooperation from the bank.

Leadcity University Ibadan DO NOT COPY

transferring funds without detection.		fraudster

Source: Researcher's Computation, 2025

4.2.5 Research Question Five:

Specific timeframes or patterns in the occurrence of fraudulent activities

Fraudulent activities often exhibit clear temporal patterns, with peaks during festive periods and high-demand seasons. The EMBER months (September to December) stand out as particularly active periods for fraud, influenced by increased economic activity, societal expectations, and financial pressures. Festive seasons, characterized by heightened consumer spending and financial transactions, create opportunities for fraudsters to exploit vulnerable individuals and systems, which makes the Fraud Triangle and Routine Activity Theories offer insightful frameworks for understanding these patterns. The "pressure" element of the Fraud Triangle aligns with financial strain during festive periods, driving both offenders and victims into situations of increased risk. Similarly, the Routine Activity Theory highlights how the absence of capable guardianship (e.g., reduced banking hours during weekends) and the availability of suitable targets amplify the likelihood of fraud during these periods. Detectives consistently reported that fraudulent activities peak during festive seasons like Christmas and "Ileya". These periods are associated with societal pressures to showcase success, financial strain from holiday spending, and increased financial transactions. A senior detective avers:

> Of course, fraudulent activities tend to spike during the EMBER Months, from September to December. This is when everyone wants to cash out and take stock of what they've achieved. During this time, fraudsters are all out,

Lead City University Ibadan DO NOT COPY

> reaching people through deceptive SMS messages. If you click on these messages, they can infiltrate your phone. This end-of-year urgency underscores the need for heightened vigilance to avoid being scammed. **(29/07/24, IDI, ANTIFRAUD, NSCDC, Male, ASSISTANT COMMANDANT OF CORPS)**

Another female detective noted the connection between festive demands and fraud, particularly in rural areas where theft and scams are rampant during religious celebrations. She stated:

> December, festival time during Christmas and Ileya. For example, during Ileya just few months ago, we saw an increased rate of people running fake alert to buy goat, ram and cow. It's that period where people are desperate to meet their demands, and they turn to theft. A lot of crimes happen during that period because it's a time when these activities increase significantly. **(29/07/24, IDI, ANTIFRAUD Female, ASSISTANT SUPERINTENDENT OF CORPS I)**

Festive periods also heighten societal pressures, with individuals engaging in fraud to "keep up" with perceived social standards, and people want to leave big because of the celebration that comes with it. A detective shared:

> Festive periods are a time when crimes tend to increase significantly, driven by people's desire to 'live large' and indulge in the celebrations. During these times, individuals are often motivated by greed or peer pressure. For example, someone might think, 'My friend is already driving a Benz, so why am I still walking?' These societal pressures, coupled with the heightened expectations of festive seasons, create an environment where fraudulent activities thrive. **(29/07/24, IDI, ANTIFRAUD, NSCDC, Male, INSPECTOR OF CORPS)**

Lead City University Ibadan DO NOT COPY

Additionally, fraudsters seek to outshine returning diaspora members during festive celebrations like Christmas when they come home for visit their families. A detective explains:

> During Christmas, people from the diaspora often return to Nigeria to celebrate with their families and friends. Those in Nigeria, especially those involved in fraudulent acts, don't want to feel overshadowed or oppressed by their returning counterparts. They go to great lengths to perpetrate fraud, finding any means possible to secure money and project an image of success. **(29/07/24, IDI, ANTIFRAUD, Male, ASSISTANT SUPERINTENDENT OF CORPS I)**

Just like how the biblical analogy of "when men sleep, the enemy came and sowed tares among the wheat" explains how the devil works, fraudsters are also deliberate in timing their activities to exploit gaps in institutional operations or security and integrity, often striking when vigilance is very low and defence are down. They sow seeds of deception, hiding their malicious activities among the legitimate transactions and processes. For example, internet fraud often occurs over weekends and during late-night hours, because fraudsters want to exploit better internet connectivity and reduced alertness among victims and their protector. A detective highlighted:

> Fraudsters usually strike on Friday evenings, knowing that if they start draining your bank account, you won't be able to resolve it until Monday since banks are closed over the weekend. This deliberate timing allows fraudsters to maximize their window of opportunity, often emptying victims' accounts before any action can be taken. **(29/07/24, IDI, ANTIFRAUD, NSCDC, Male, DEPUTY SUPERINTENDENT OF CORPS)**

Like a winter storm that brings unexpected challenges, temporal patterns also significantly influence the Anti-Fraud Unit's approach to investigations. During peak periods like Christmas, Easter and Ileya, the unit anticipates a surge in fraud cases, which requires

Lead City University Ibadan DO NOT COPY

proactive planning but resource constraints often hinder effective responses. One detective asserts:

> During peak periods like Christmas, temporal patterns play a significant role in shaping investigations, as many people fall victim to fraudulent travel schemes. Fraudsters take advantage of the increased demand for travel services to Mecca or Median for Hajj by posing as legitimate agents, advertising fake businesses, while given out ram, groundnut oil, rice and issuing false documents. **(29/07/24, IDI, ANTIFRAUD Female, ASSISTANT SUPERINTENDENT OF CORPS I)**

Furthermore, another detective explained the challenge that hamper fraud investigation, particularly during high-risk periods such as the festive time. He explained how outdated tools severely impede the ability to effectively detect, investigate and prosecute fraudulent activities. The lack of modern investigative tools, such as drones and real-time surveillance systems, further complicates efforts during high-risk periods. He avers:

> We don't have enough gadgets for proper investigation and when we go out for an operation during Christmas, we rely solely on our mindset and the passion we have for the job. Even something as basic as a drone isn't available to us. Ordinary radio communication? We don't have that either. Instead, we depend on our mobile phones for telecommunication support. **(29/07/24, IDI, ANTIFRAUD Male, ASSISTANT SUPERINTENDENT OF CORPS I)**

The Fraud Triangle and Routine Activity Theories collectively illuminate the dynamics of temporal patterns in fraud. The "pressure" element of the Fraud Triangle is evident during festive periods when financial and social demands increase, motivating offenders to act. Simultaneously, the Routine Activity Theory explains how the absence of capable guardianship (e.g., limited banking operations during weekends) and the availability of suitable targets (e.g., individuals distracted by holiday activities) facilitate fraud. Meanwhile,

Lead City University Ibadan DO NOT COPY

temporal patterns in fraudulent activities reflect the interplay of societal pressures, financial strain, and systemic vulnerabilities. Festive periods, particularly the EMBER months, emerge as high-risk times for fraud, requiring targeted interventions and resource optimization.

Case Review on Specific timeframes or patterns in the occurrence of fraudulent activities

Festive seasons, particularly during the September–December months and religious celebrations like Ileya, Christmas and Easter are characterized by heightened economic activity and financial transactions. These periods create opportunities for fraudsters to exploit societal pressures and financial desperation. **File No. 722 (2022)** and **File No. 797 (2022)** highlights a livestock scam during Ileya celebrations, where fraudsters issued fake payment alerts to purchase rams, reselling them for profit and a purchase of 13 bags of rice which the suspect refused to deliver or refund the money. Similarly, fraudsters often target victims during weekends (Fridays) and late-night hours, when institutional oversight is reduced. **File No. 859 (2022)** illustrates a case where fraudulent withdrawals were conducted late on a Friday evening, taking advantage of banking closures over the weekend. This delay in institutional response allowed the fraudster to withdraw substantial amounts before detection. These cases reflect the **Routine Activity Theory's** emphasis on the absence of capable guardianship. Reduced oversight during weekends and at night creates vulnerabilities that fraudsters exploit, emphasizing the need for round-the-clock institutional monitoring.

Lead City University Ibadan DO NOT COPY

The table below summarizes specific cases highlighting the temporal patterns observed in fraudulent activities within Oyo State, as investigated by the NSCDC.

Table 4.5: Temporal Patterns in Fraudulent Activities Identified by NSCDC

Case Type	File. No & Year	Key Fact of the Case	Contributing Factors/ Timeframe/Period	Theoretical Link	Outcome/Prosecution Details
(OBT)	F.N. 722 (2022)	Fraudster used fake payment alerts to purchase livestock during the festive period and resell them for profit.	Religious Festive Periods (Ileya)	**Routine Activity Theory's** emphasis on the absence of capable guardianship.	Suspect apprehended; victims recovered partial funds.
(OBT)	File No. 797 (2022)	Fraudster exploited victims' negligence during Christmas with a purchase of 13 bags of rice.	Festive Shopping Season (December)	**Routine Activity Theory's** emphasis on the absence of capable guardianship.	Suspect apprehended, and funds were recovered.
(OBT)	File No. 859 (2022)	Fraudster swapped victim's ATM	Friday late Nights and Weekends	**Routine Activity Theory's** emphasis on the absence of	Suspect arrested after tracing transactions to a secondary account.

Lead City University Ibadan DO NOT COPY

	card late on a Friday night and conducted multiple transactions over the weekend to avoid immediate detection.	capable guardianship.

Source: Researcher's Computation, 2025

4.2.6 Investigation and Prosecution Process

The review of case files from the NSCDC Anti-Fraud Unit provides valuable insights into the dynamics of fraud cases and their resolution in Oyo State. Investigations typically begin with the complainant writing a detailed statement and this statement introduces the complainant, provides their professional background, and recounts the events that led to the fraudulent activity. It includes information about how the complainant encountered the suspect, the amount of money transferred, the purpose of the transfer, and supporting evidence such as bank transaction records. Detectives also require key details like the suspect's phone number to track and monitor their location. Once the suspect is located, detectives proceed by either sending an official invitation or obtaining a warrant of arrest if necessary. Suspects who cooperate are treated respectfully, with their rights fully upheld. Upon arrival at the Anti-Fraud Unit, detectives conduct a calm and non-threatening interrogation, ensuring a comfortable environment to encourage honest communication. During this process, suspects

Lead City University Ibadan DO NOT COPY

are asked to explain their version of events, which is then compared to the allegations made by the complainant.

If the suspect admits guilt, detectives explain the charges—most commonly obtaining by false pretence (OBT) or Visa Racketeering (VR)—and provide two options: refund the defrauded money or face court proceedings. In cases where the suspect denies the allegations, detectives rely on collected evidence such as bank statements to corroborate the complainant's claims. If the evidence reveals misuse of funds, detectives confront the suspect with the findings. When suspects are willing to resolve the matter amicably, the unit facilitates mediation between both parties. A Memorandum of Understanding (MOU) accompanied with a Payment Schedule, is signed to establish repayment terms. However, if the suspect remains uncooperative or attempts further deception, the case is escalated to court. At this stage, the legal department of the NSCDC Oyo State Command takes over prosecution responsibilities with the assistance of the detailed evidence provided by the Anti-Fraud Unit, leaving the judiciary to deliver the final verdict.

After a victim reports a fraudulent case to the NSCDC Anti-Fraud Unit and details of proof have been supplied, a Banker's Order is first obtained from the court by the detective. This allows detectives to analyse transactions in the suspect's bank statement. Simultaneously, a Court Order is secured and taken to the telecommunications provider to access the suspect's call logs, enabling detectives to gather evidence, including details of the suspect's contacts and movements. An invitation is then sent to the suspect. If the suspect honours the invitation, a statement of witness and an accused statement are recorded. However, if the suspect fails to respond, a warrant of arrest, also referred to as Criminal Form 5 & 6, is obtained from the court. Alongside this, an Armed Squad Request Form is submitted by the unit and approved

Lead City University Ibadan DO NOT COPY

by the Commandant. At the point of arrest, Miranda Warnings will be said by the senior detective and once arrested, the suspect is brought to the command for interrogation, and their statement is recorded using the NSCDC Form (003). If the suspect is unable to write in English, an Illiterate Jurat form is used to document their statement.

Following the statement, detectives begin interrogating the suspect based on the information provided. Suspects can be held in custody for a maximum of 48 hours but If they fail to cooperate or do not provide sufficient evidence to support further investigation, a Motion Ex-Parte is requested from the court to extend custody for an additional 14 days. However, if the suspect shows signs of cooperation, they may be granted bail under an Acknowledgment of Bail Conditions (Bail Bond), with the understanding that they can be recalled for further interrogation if necessary. If it is determined that the suspect has defrauded the complainant, the unit may explore the possibility of an Out-of-Court Settlement. In such cases, both parties are issued a Consent of Parties (ADR) Form, and an undertaking is documented.

The unit mediates between the suspect and the complainant, arranging for the suspect to compensate the victim for the damages or funds defrauded. A payment schedule is agreed upon and recorded. Finally, a Preliminary Report detailing the case records, processes, and outcomes is prepared and sent to the Commandant's Office for proper documentation. This report is maintained in the Office of the Commandant, which is accountable to the President for cases handled by the Anti-Fraud Unit. This thorough approach ensures that investigations are handled professionally while respecting the rights of both complainants and suspects.

4.3. Discussion of Findings

Lead City University Ibadan DO NOT COPY

This study explores the prosecution of fraud cases by the Nigerian Security and Civil Defence Corps (NSCDC) in Oyo State Command, with a focus on the dynamics of fraud occurrence in Ibadan**.** In research question one**,** findings reveal that the most prevalent types of fraud within the NSCDC dataset are Obtaining by False Pretence (OBT) and Visa Racketeering (VR). These fraud typologies share key characteristics, including strategic deception, manipulation of victims' trust, and a primary focus on financial gain. OBT cases typically involve fraudsters making false promises or misrepresentations to extract money or assets from their victims, while VR schemes often prey on individuals desperate to travel abroad, offering them fake documents or fraudulent opportunities. Both types highlight the opportunistic and calculated nature of fraudsters, who exploit societal vulnerabilities and personal aspirations for financial advantage. This understanding of the patterns and dynamics of fraud in Oyo State provides a foundation for targeted interventions, emphasizing the need for increased vigilance, public awareness, and enhanced investigative strategies within the NSCDC Anti-Fraud Unit. The dominance of OBT in the fraud landscape aligns with previous research, where OBT remains one of the most persistent forms of fraud in Nigeria and it is characterized by the misuse of funds or assets under false claims[1]**.** These cases involve individuals being tricked into transferring money or assets to fraudsters who present themselves as legitimate. Common examples include fraudulent land sales, fake contracts, and unauthorized financial transactions. In one instance, a suspect disappeared with over ₦1,050,000 that a victim had entrusted to them for transferring to a family member. Instead of completing the transaction, the suspect diverted the funds for personal use. These examples highlight how fraudsters exploit trust-based relationships, leaving victims financially and emotionally devastated. Similarly, the rise in cybercrime reflects global

Lead City University Ibadan DO NOT COPY

trends, as the growing use of the internet across Africa, combined with weak regulatory systems, has made digital fraud more widespread[2].

Visa racketeering, highlighted in this study, also shows how fraudsters take advantage of people's economic struggles and desire to migrate abroad. Cases like File Nos. 729, 731 and 749 reveal how fraudulent agents deceive victims' eager to relocate under the "Japa" trend—a term describing the growing number of Nigerians leaving the country for better opportunities. This type of fraud has become common, preying on individuals who are desperate to improve their lives by moving abroad.

Extant literature has recorded that Visa fraud is also a growing issue in Sub-Saharan Africa whereby fraudsters will promise victims job placements, academic admissions, or travel visas, charging exorbitant fees for services that are never delivered and these schemes capitalize on the desperation of individuals eager to escape Nigeria's economic challenges[3]. The Fraud Triangle theory helps explain why fraud happens by looking at three key factors: opportunity, pressure, and rationalization. Economic pressures like poverty, unemployment, and society's obsession with wealth make fraud more likely. Opportunities come from weak systems in areas like law enforcement, banking, telecommunications, and real estate, which fraudsters take advantage of. Rationalization happens when offenders justify their actions, saying they had to do it to survive or because of the pressure to meet societal expectations.

This work show that economic hardship and unemployment play a significant role in driving fraud in Oyo State. Several respondents pointed out that fraudsters often justify their actions as a way to cope with poverty and a lack of opportunities. This aligns with the Fraud Triangle Theory, which highlights financial pressure as a major cause of fraudulent behaviour. In a

Lead City University Ibadan DO NOT COPY

society where wealth is celebrated without concern for how it is acquired, people feel pressured to engage in fraud to gain social acceptance. The obsession with material success further encourages this behaviour. Several respondents also highlighted the role of societal pressures, where individuals feel compelled to display wealth to gain social standing. This dynamic encourages youth to abandon traditional employment or skill acquisition in favour of quick money-making schemes such as OBT or visa racketeering and that has made societal glorification of wealth often rationalizes fraudulent behaviours, particularly among young people[4]. The Routine Activity Theory helps explain why fraud happens, showing that it occurs when offenders take advantage of situations where there is no one to stop them, targeting people who are vulnerable. This is clear in the NSCDC's case files, which highlight fraud types like Obtaining by False Pretence (OBT), Visa Racketeering, and ATM card swapping. By recognizing these patterns, the NSCDC has been able to anticipate and prepare for increases in fraud during periods when risks are higher.

For the second research question, which looks at how the cost of prosecuting fraud cases affects the NSCDC's investigations, findings from interviews and case analyses show that limited funds have a significant impact on both strategies and outcomes. Detectives explained that investigations are often delayed because there isn't enough money to gather evidence quickly. For example, obtaining a Banker's Order, Court Order or a Motion Ex-parte to keep a suspect in custody for longer requires court fees and other logistical expenses, which often exceed the unit's budget. As reported in literature, many anti-corruption and fraud-related agencies in Nigeria face chronic underfunding, limiting their capacity to effectively pursue cases and without adequate financial backing, investigations are prone to delays and incomplete evidence gathering, which can compromise case outcomes[5].

Lead City University Ibadan DO NOT COPY

Interviews and case files reveal that financial constraints frequently delay or disrupt investigations. Acquiring court orders, accessing telecommunications records, and carrying out surveillance require significant funding, which is often unavailable. For instance, in Case Nos. 851, 731 and 969, investigations were stalled due to limited resources, forcing the complainant to withdraw the case prematurely. The Routine Activity Theory sheds light on this issue by highlighting the importance of capable guardianship in preventing and addressing fraud. When resources are scarce, the NSCDC's ability to act as a capable guardian weakens, giving offenders more room to operate without fear of prosecution. This lack of sufficient resources undermines the agency's efforts to deter fraud and hold offenders accountable effectively.

The reliance on traditional methods, like manual tracking and basic communication tools, makes investigations even more challenging for the NSCDC. Detectives highlighted that the lack of advanced tools, such as digital forensics equipment, real-time surveillance systems, and secure communication devices, significantly hampers their work. Much of their investigations rely on outdated processes and basic technology, like mobile phones, which are often unreliable. For instance, tracking suspects using GPS data is frequently disrupted by network issues, leaving investigators to rely on less effective methods. This inability to invest in modern investigative technology puts the NSCDC at a disadvantage, especially in cybercrime cases where fraudsters use advanced and sophisticated techniques. The gap between the agency's resources and the evolving tactics of fraudsters exacerbates the challenges faced by investigators, making it harder to keep pace with the criminals. Extant studies revealed that the increasing complexity of fraud schemes necessitates investment in digital forensics and data analytics to enhance the capacity of investigative agencies and the

Lead City University Ibadan DO NOT COPY

lack of such tools within the NSCDC not only slows down investigations but also reduces the likelihood of successfully prosecuting fraudsters[6].

Existing literature highlights inadequate funding as a critical barrier to effective crime prevention in Nigeria and the financial cost of fraud prosecution significantly impacts investigative strategies and outcomes, because resource constraints, including limited funding and logistical challenges, hinder the Unit's ability to sustain prolonged investigations[7]**.** This work found that complainants often bear the cost of investigations, which introduces inequities in access to justice. Additionally, the lengthy process of obtaining court orders delays investigations and gives suspects time to evade justice. Findings revealed that in cases where the complainant cannot provide financial support, investigations are either delayed or abandoned and this reflects findings by a literature which argue that the cost of accessing critical evidence often becomes a barrier to justice in low-resource settings and this resulting delays can erode public trust in the NSCDC and discourage victims from reporting fraud in the future[8].

The findings in this work highlight the urgent need for faster legal processes to help deter fraud. According to the Fraud Triangle Theory, reducing opportunities for fraud can be an effective prevention strategy. However, the financial challenges faced by the NSCDC often result in delays in resolving fraud cases. Respondents pointed out that investigations frequently exceed the standard 48-hour custody limit because of delays in securing court orders or gathering necessary evidence. These setbacks not only slow down the process but also make it harder to achieve timely justice.

Literature explains that delays in prosecution often result in the loss of evidence or witness cooperation, reducing the likelihood of securing convictions and fraudsters may use the

Lead City University Ibadan DO NOT COPY

extended timelines to abscond or tamper with evidence, undermining the integrity of the investigative process[9].

Research question three explores the tactics and strategies commonly used by fraudsters, and investigations reveal a variety of evolving methods designed to exploit victims through technology and personal vulnerabilities. Fraudsters frequently use online platforms to pose as legitimate vendors or service providers. For example, in File No. 969, a complainant was defrauded by a fraudulent social media vendor which was also aided by a top bank official. Another strategy involves forging documents, such as fake admission letters or employment offers, to gain victims' trust. This was evident in File No. 749, where victims were tricked into parting with their money based on false promises. Fraudsters also capitalize on personal or professional relationships to access funds or assets under false pretences. In cases of Obtaining by False Pretence (OBT), fraudsters persuade victims to transfer money or hand over valuable assets for fabricated purposes. Interviews revealed several cases where fraudsters posed as real estate agents, offering land or property sales, only to disappear with the victims' funds. These findings emphasize the adaptive nature of fraud and the importance of robust investigative strategies to counter these evolving tactics.

Interpersonal relationships play a big role in fraud, as trust exploitation is a common strategy in financial crimes, especially in places with weak regulations where fraudsters take advantage of their victims' lack of knowledge and their willingness to trust, making it one of the easiest and most effective ways to steal from someone close to them.[10]. Social engineering is also key tactic employed by fraudsters, as they manipulate victims into sharing sensitive information or transferring funds. The Routine Activity Theory highlights how motivated offenders exploit vulnerable individuals, especially those unaware of new fraud

Lead City University Ibadan DO NOT COPY

schemes. The lack of strong detection and enforcement mechanisms, like the underutilized NSCDC Anti-Fraud Unit in Oyo State Command, makes it easier for these fraudsters to succeed.

This study also found that inadequate public awareness and the absence of advanced surveillance technologies further facilitate fraudulent activities. This underscores the urgent need for continuous education and technological improvements to counteract the ever-evolving tactics used by fraudsters. Among these tactics are phishing, ATM card swapping, SIM card manipulation, and identity theft, all of which target unsuspecting victims and capitalize on systemic gaps. Fraudsters take advantage of technological advancements and societal trust to carry out their schemes. They use tools like artificial intelligence and untraceable platforms, such as cryptocurrency and gift cards, to avoid being traced. To counter these tactics, the NSCDC employs methods like monitoring bank transactions and analysing call logs, showing their commitment to adapting to these challenges.

The work also reveal that fraudsters often work in clusters or networks, sharing information and resources to strengthen their operations. These networks give them an edge, providing access to insider information, logistical support, and a broader pool of potential victims. Some respondents highlighted that fraudsters even collaborate with bank employees or telecommunication agents to bypass security systems, making unauthorized transactions easier to execute. This collaboration adds another layer of complexity to the fight against fraud. The Routine Activity Theory emphasizes the role of offender networks in creating a conducive environment for crime and previous studies highlight that these collaborations often involve a division of labour, with different members specializing in tasks such as phishing, document forgery, or fund diversion and disrupting these networks requires

Lead City University Ibadan DO NOT COPY

targeted surveillance and intelligence-sharing between law enforcement agencies and financial institutions[11].

To discuss the findings on research question four on identifying individuals or entities involved in committing fraud, this study highlights distinct demographic and behavioural traits among perpetrators. Most fraudsters are young, male, and technologically skilled, often operating within tightly organized networks. These groups thrive in urban areas like Molete, Mokola, Agbowo, and Bodija in Ibadan, where they benefit from the anonymity and easy access to digital tools that these environments provide. Fraudsters rarely act alone; they collaborate in hierarchical networks with clearly defined roles. Leaders typically plan and oversee schemes, while lower-ranking members carry out specific tasks. The involvement of institutional insiders, such as bank employees or telecommunications agents, further exposes systemic vulnerabilities that facilitate fraud. These findings emphasize the need for targeted interventions to address both individual and systemic factors enabling fraudulent activities. A detective highlighted that breaking these fraud networks requires focused surveillance, intelligence-sharing, and coordinated enforcement efforts. Most fraudsters are young, tech-savvy males, typically from Generation Z. Respondents noted that a large number of these perpetrators fall within the 18 to 35 age range, mirroring national patterns in cybercrime and financial fraud.

This demographic is often drawn to fraudulent activities due to unemployment, economic hardship, and societal pressure to achieve quick financial success. These findings align with the Fraud Triangle Theory, which emphasizes financial pressure as a major factor driving fraudulent behaviour. In the context of Nigeria, where youth unemployment was estimated at 42.5% which buttresses the fact that economic hardship will create a fertile ground for young

Lead City University Ibadan DO NOT COPY

people to rationalize fraudulent activities as a means of survival or social mobility[12]. Interviews with NSCDC officials in the Anti-Fraud Unit show that fraudsters often live flashy lifestyles, which act as warning signs for investigators. The NSCDC data also reveals that fraudsters range from opportunistic individuals to well-organized groups. These groups often have members who specialize in specific tasks like document forgery, phishing, or social engineering. Detectives pointed out that these fraudsters' displays of wealth usually don't match their actual income, making it easier to spot them as potential suspects. Fraudsters also tend to operate discreetly in their day-to-day interactions, masking their illicit activities to avoid suspicion and this duality in behaviour also aligns with findings of a literature which observed that fraudsters use their wealth as both a status symbol and a cover for their activities[13].

This study found that fraudsters often target people who are not very familiar with technology, taking advantage of their lack of knowledge about how to protect personal information. However, for a victim or complainant to hold a fraudster accountable, they need to prove that the fraudster knowingly lied about something, understood that the victim was likely to trust them, and that the victim relied on this false information and suffered harm as a result. Interviews also revealed that fraudsters exploit the desperation of their victims, using clever tactics to manipulate them. Additionally, many fraudsters justify their actions by blaming economic struggles or societal issues, which aligns with the concept of rationalization from the Fraud Triangle Theory.

The findings also suggest that certain institutional roles, such as banking staff or telecommunication agents, act as enablers in fraud schemes. For example, insider involvement in facilitating unauthorized transactions or document falsification was

Lead City University Ibadan DO NOT COPY

highlighted in multiple interviews and case files. This study found that fraudsters come from a wide range of socio-economic and educational backgrounds. Some have little formal education and commit small-scale fraud, while others are highly educated and use their technical skills to carry out more advanced crimes like cyber fraud or money laundering. Respondents pointed out that these highly skilled fraudsters often justify their actions by claiming they are simply using their expertise in a system that doesn't offer enough legitimate opportunities. The range of educational levels among fraudsters shows how adaptable they can be. Those with technical knowledge are increasingly using advanced tools like blockchain and artificial intelligence to hide their activities. This highlights the urgent need for specialized training and advanced digital forensic tools in the NSCDC Anti-Fraud Unit to effectively tackle these more complex schemes.

For research question five, which examines fraud patterns and timing, the findings show that fraudulent activities tend to peak during specific periods. These include the end of the fiscal year, when there's an increase in financial transactions, and admission seasons, when visa-related fraud cases rise. For example, in File Nos. 722, 749,797 and 859 clearly aligns with these seasonal trends. This study revealed that fraudsters carefully plan their activities to take advantage of high-stakes times, such as academic admissions and festive shopping periods. This shows the opportunistic nature of fraud and highlights the need for proactive measures during these high-risk times. The Fraud Triangle supports this idea by showing how external pressures, like increased spending during the holidays or migration demands, create more opportunities for fraud. Additionally, the study found that fraudsters also take advantage of societal and economic challenges during certain seasons. For instance, during economic

Lead City University Ibadan DO NOT COPY

downturns or currency devaluation, fraudsters exploit people's financial desperation by offering fake investment opportunities or schemes promising high returns.

Participates shared cases where fraudsters lured victims with promises of high returns from foreign exchange trading or cryptocurrency investments but then disappeared with their money[14]. Victims, often desperate to regain financial stability, become more vulnerable to these risky and fraudulent offers, making them easy targets. In some cases, these individuals are re-victimized, as their desperation leads them to fall for similar scams again. Cyber fraud, on the other hand, follows a specific pattern, often happening late at night when internet traffic is lower. During these hours, fraudsters can take advantage of network vulnerabilities, making it harder for their activities to be detected. Detectives in the NSCDC Anti-Fraud Unit observed that many cyber fraudsters work overnight, using time zone differences to target international victims. Phishing scams and fake online store transactions often happen during these late hours to avoid immediate detection. Cybercriminals strategically plan their activities to exploit gaps in digital monitoring and take advantage of people's reduced alertness. They also use advanced tools like automated phishing bots, which allow them to run their scams for long periods and target multiple victims at once.

Additionally, this study found that visa racketeering tends to follow a seasonal pattern, with cases peaking during academic admissions and migration waves. One respondent explained how fraudsters prey on people's aspirations for foreign education, jobs, or residency by offering fake visas, admission letters, or work permits, often charging large sums for these fraudulent services. These schemes are especially common between June and September, which aligns with university application deadlines and the migration season. During this time,

Lead City University Ibadan DO NOT COPY

when migration demand is high, visa racketeering becomes more widespread, particularly given the current economic challenges in the country.

Fraudsters take advantage of individuals who are unfamiliar with legitimate application processes, preying on their desperation and charging them extremely high fees for fake services. The timing of fraud presents significant challenges for law enforcement agencies like the NSCDC Anti-Fraud Unit. Respondents explained that during peak periods, such as the end-of-year festive season, the surge in fraud cases often overwhelms resources. This leads to delays in investigations and prosecutions, as manpower and financial resources are stretched thin. For example, financial fraud cases spike during the festive season when consumer spending increases, making it difficult for investigators to keep up with the demand.

Understanding the timing of fraud is crucial for the Anti-Fraud Unit to optimize its resources. By identifying periods when fraud activity is likely to increase, the NSCDC can better allocate personnel and tools to manage these surges. This approach is supported by the Routine Activity Theory, which highlights the importance of capable guardianship in preventing crime. Strengthening guardianship—such as increasing surveillance and proactive measures during high-risk times—can disrupt fraudsters' operations and protect potential victims. The theory also explains how fraud is more likely to occur when motivated offenders, vulnerable victims, and a lack of protective measures converge. By understanding these patterns, the NSCDC can focus its efforts during critical periods, improving its ability to prevent and respond to fraudulent activities effectively.

Lead City University Ibadan DO NOT COPY

Lead City University Ibadan DO NOT COPY

Endnotes

1. J. Ugoani, *Pyramidal Public Corruption: Public Policy and Bad Governance--Nigerian Perspective*, **American Journal of Economics, Finance and Management**, 1(5), 2015, pp.404-413

2. A. Kuzior, I. Tiutiunyk, A. Zielińska, & R. Kelemen, *Cybersecurity and Cybercrime: Current Trends and Threats*, **Journal of International Studies (2071-8330),** 17(2), 2024

3. N. Smith, *The Blind Eye in Sino-African Relations: Social Trust and Business Scams,* **Rising Asia Journal** 4(2), 2024.

4. A. H. Bhat & D. Kolhe, *Crime and Fraud at the Community Level: Social Networking Understanding into Economic Crimes and Psychology Motivations.* **Journal of Social Sciences and Economics**, 3(2),2024, pp.127-146.

5. M. E. Akokuwebe & E. S. Idemudia, *Fraud Within the Nigerian Health System, A Double Threat for Resilience of a Health System and the Response to the COVID-19 Pandemic: A Review.* **Pan African Medical Journal**, 45(1), 2023

6. R. E. Daraojimba, O. A. Farayola, F. O. Olatoye, N. Mhlongo, & T.T. Oke, *Forensic Accounting in the Digital Age: A Us Perspective: Scrutinizing Methods and Challenges in Digital Financial Fraud Prevention*, **Finance & Accounting Research Journal**, 5(11), 2023, pp.342-360.

7. E.C. Nwokaeze, T. D. Ikiriko, & S.W. Johnbull, *Urban Security Challenges: A Review of Crime Prevention Strategies Adopted by Residents in Greater Port Harcourt City, Rivers State, Nigeria***. International Journal of Research and Review**, 9(3), 2022 pp.60-74.

8. S. Belshaw, & B. Nodeland, *Digital Evidence Experts in the Law Enforcement Community: Understanding the Use of Forensics Examiners by Police Agencies,* **Security Journal**, 35(1), 2022, pp.248-262.

9. L. M. Ouziel, *Prosecution in Public, Prosecution in Private*, **Notre Dame L. Rev**., 97, 2021, p.1071.

10. N. M. Zin, S. Muda, E. S. Kasim,, N. Ismail, H. M. Padil, & R. Ramli, *Understanding the Vulnerabilities Contributing to Investor Victimization in Scams*, **Pakistan Journal of Criminology**, 16(3), 2024

11. C. Cretu-Adatte, J. W. Azi, O. Beaudet-Labrecque, H. Bunning, L. Brunoni, & R. Zbinden, *Unravelling the Organisation of Ivorian Cyberfraudsters: Criminal Networks or Organised Crime?*. **Journal of Economic Criminology**, 2024, 3, p.100056.

12. H. Achimugu, D. O. A. Adamu, & D. Ojonugwa,, N*ational Social Investment Programme and Youth Unemployment in Kogi State, Nigeria,* **International Journal of Public Administration and Management Research,** 10(4), 2024, pp.30-39.

13. P. Manning, *A Novel Understanding of Fraudsters*, **Journal of Financial Crime**, *30*(5), 2023, pp.1117-1129.

14. E. Esoimeme, *Examining the Potential Misuse of Artificial Intelligence to Circumvent Technology-Based Processes for AML/CFT Compliance in the Cryptocurrency Ecosysyem*. CFT Compliance in The Cryptocurrency Ecosysyem *22, 2024)*, https://ssrn.com/abstract=4964272 or http://dx.doi.org/10.2139/ssrn.4964272

Lead City University Ibadan DO NOT COPY

Lead City University Ibadan DO NOT COPY

Chapter Five

Conclusion

5.1 Summary of Findings

This study investigated the understudied role and effort of the Nigerian Security and Civil Defence Corps (NSCDC) in fraud investigation and prosecution within Oyo State in the academic and policy circle. It focused on the dynamics of fraud occurrence, challenges in investigative processes, and strategies employed to combat fraudulent activities. Because of the underrated role and effort of the Anti-Fraud Unit of the NSCDC, the findings provide critical insights into the nature of fraud in the region, highlighting socio-economic drivers, technological advancements, and institutional challenges, as well as the need for enhanced prevention and prosecution measures. These findings are based on interview data, case file reviews, and theoretical frameworks such as the Fraud Triangle Theory and Routine Activity Theory. This study was introduced by highlighting the increasing prevalence of fraud in Oyo State and its socio-economic implications. It underscored the critical role of the NSCDC in addressing this challenge and set the stage for exploring fraud dynamics, investigative strategies, and systemic constraints.

The chapter two provided a detailed review of relevant literature and theoretical frameworks which served as lenses for understanding fraud's underlying drivers and the conditions that enable it and the next chapter outlined the research methodology, emphasizing the use of interviews, case file reviews, and content analysis to collect and analyse data. This approach ensured a robust examination of fraud patterns, investigative processes, and institutional challenges. Afterwards, the findings were presented, offering insights into the types of fraud prevalent in Oyo State, the socio-economic and systemic factors influencing these crimes,

Lead City University Ibadan DO NOT COPY

and the strategies employed by the NSCDC to combat them. The study revealed that fraud in Oyo State takes various forms, with the most prevalent being Obtaining by False Pretence (OBT) and Visa Racketeering (VR). These crimes share common characteristics, such as deception, exploitation of trust, and financial motives. Fraudsters often leverage socio-economic desperation, technological tools, and systemic vulnerabilities to perpetrate their schemes. For example, OBT cases frequently involve trust exploitation, where victims are deceived into transferring money for fake contracts, land sales, or fabricated business deals. Similarly, Visa Racketeering thrives during periods of high migration activity, with fraudsters targeting individuals seeking opportunities abroad by offering fraudulent travel documents.

These findings align with the Fraud Triangle Theory, which highlights the interplay of pressure, opportunity, and rationalization in driving fraudulent behaviour. The study highlighted that financial constraints significantly hinder the NSCDC's ability to investigate and prosecute fraud cases effectively. Detectives often face delays in obtaining essential court orders, accessing banking and telecommunication records, and conducting surveillance due to insufficient funding. These delays not only prolong investigations but also lead to the premature withdrawal of cases by complainants who cannot bear the financial burden of pursuing justice. During high-demand periods, such as the festive season, the surge in fraud cases overwhelms the NSCDC's limited resources, stretching manpower and investigative tools thin. This aligns with the Routine Activity Theory, which emphasizes the importance of capable guardianship in preventing crime. Without adequate funding, the NSCDC struggles to act as an effective guardian, allowing fraudsters to exploit systemic gaps. These findings

Lead City University Ibadan DO NOT COPY

underscore the need for improved resource allocation and funding to enhance the investigative and prosecutorial capacity of the Anti-Fraud Unit.

This study explained that fraudsters employ a wide range of sophisticated tactics to execute their schemes. These include phishing emails, ATM card swapping, SIM card manipulation, document forgery, and social engineering. Fraudsters leverage advanced technologies, such as artificial intelligence and cryptocurrency, to conceal their activities and evade detection. For instance, untraceable platforms like cryptocurrency and gift cards are increasingly used to launder stolen funds. Organized fraud networks, often hierarchical in structure, provide operational support and insider information, making it difficult for investigators to dismantle their operations.

Fraudsters also strategically time their activities to coincide with high-risk periods, such as academic admissions and festive seasons, exploiting societal pressures and financial vulnerabilities. These findings highlight the adaptability and sophistication of fraud schemes, emphasizing the need for continuous public awareness campaigns and specialized training for investigators. The study identified distinct characteristics of fraud perpetrators, who are predominantly young, technologically skilled males aged between 18 and 35. Many perpetrators are motivated by economic hardship, unemployment, and societal pressures to achieve financial success. They often operate in urban centres such as Bodija, Mokola, and Agbowo, where anonymity and access to digital tools enable their fraudulent activities. Respondents noted that fraudsters frequently display outward signs of wealth disproportionate to their legitimate income, such as luxury vehicles and extravagant lifestyles, which serve as red flags for investigators and this demographic trend reflects broader national patterns in cybercrime and financial fraud, where young people, often referred to as

Lead City University Ibadan DO NOT COPY

"Yahoo Boys," dominate the landscape. Insider complicity within institutions, including banks and telecommunications companies, was also highlighted as a significant enabler of fraud. Employees in these sectors provide fraudsters with access to sensitive information, facilitating unauthorized transactions. These findings underscore the need for stricter internal controls, regular audits, and enhanced whistle-blower protections to address insider involvement.

Fraud activities in Oyo State exhibit clear temporal patterns, peaking during high-risk periods such as the end of the fiscal year, festive seasons, and migration waves. For example, visa racketeering surges during academic admissions, while cyber fraud spikes during festive shopping periods when consumer spending increases. Fraudsters exploit these periods to target individuals under financial pressure or those eager to meet year-end obligations.

The opportunistic nature of fraud aligns with the Routine Activity Theory, which explains how motivated offenders exploit suitable targets in the absence of capable guardianship. Understanding these temporal patterns enables the NSCDC to allocate resources more effectively, prioritizing high-risk periods for heightened surveillance and proactive measures.

The findings underscore the need for strategic interventions to enhance the NSCDC's capacity to combat fraud. Addressing socio-economic drivers, such as unemployment and poverty, is crucial to reducing the pressures that lead individuals into fraudulent activities. Strengthening regulatory frameworks and investing in advanced investigative technology, such as digital forensics and predictive analytics, can significantly improve the NSCDC's efficiency. Public awareness campaigns are also crucial for educating citizens about common fraud tactics and how to protect themselves. Collaboration with financial institutions, telecommunications providers, and international anti-fraud organizations is vital for

Lead City University Ibadan DO NOT COPY

intelligence-sharing and operational efficiency. Additionally, fostering community engagement and promoting ethical values can help address the cultural normalization of fraud. These measures are necessary to empower the NSCDC to effectively combat fraud and deliver justice to victims.

5.2 Conclusion

This study has provided valuable insights into the role of the Nigerian Security and Civil Defence Corps (NSCDC) in combating fraud within Oyo State. It has revealed the complex nature of fraud, driven by socio-economic pressures, technological advancements, and systemic weaknesses. The findings highlight the diverse forms of fraud, such as Obtaining by False Pretence (OBT), cybercrime, and visa racketeering, which exploit victims' trust, desperation, and lack of awareness. Fraudsters employ sophisticated tactics and leverage digital tools to carry out their schemes, often during periods of heightened financial activity, such as festive seasons and academic admissions.

One of the key challenges identified is the limited resources available to the NSCDC Anti-Fraud Unit. Financial constraints, lack of advanced investigative tools, and insufficient manpower hinder the timely and effective prosecution of fraud cases. These resource limitations not only delay investigations but also allow fraudsters to operate with reduced risk of detection. Despite these challenges, the NSCDC has shown commitment in addressing fraud through strategic interventions, public education, and inter-agency collaboration.

The study also underscored the importance of understanding the characteristics of fraudsters, who often come from diverse backgrounds but share common motivations such as economic hardship and societal pressure. By identifying these patterns, the NSCDC can better anticipate and disrupt fraudulent activities and the need for a holistic approach to combating

Lead City University Ibadan DO NOT COPY

fraud in Oyo State should be emphasized. Addressing the root causes of fraud, such as poverty and unemployment, while strengthening institutional capacity, regulatory frameworks, and public awareness efforts, is essential. By investing in advanced technology and fostering collaboration with stakeholders, the NSCDC can enhance its ability to prevent fraud, protect victims, and bring offenders to justice. Ultimately, these efforts will contribute to building a more secure and trustworthy environment for the people of Oyo State.

5.3 Recommendations

Based on the findings of this work anchored on the objectives and aim of the research, this work recommends the following:

1. The NSCDC Anti-Fraud Unit requires adequate financial and material resources to carry out its mandate effectively in accordance with Section 3 (1) (f) (iii) of the Nigeria Security and Civil Defence Corps (Amendment) Act, 2007. The government should prioritize increased budgetary allocation to the unit to support critical activities such as obtaining court orders, accessing banking and telecommunication data, conducting surveillance, advanced investigative tools, and logistics. These funds should also cover the recruitment of additional personnel to reduce the strain on existing manpower during peak periods and a dedicated budget for the Anti-Fraud Unit will reduce delays, improve operational efficiency, and encourage victims to pursue justice without the fear of financial burden.
2. The NSCDC should intensify efforts to educate the public about common fraud tactics, such as phishing scams, visa racketeering, and fake investment schemes. Public awareness campaigns should be conducted through television, radio, social media, and community outreach programs to equip citizens with the knowledge to

Lead City University Ibadan DO NOT COPY

identify and avoid fraudulent activities. These campaigns should educate citizens on common fraud tactics, preventive measures, and the importance of reporting fraud and special focus should be placed on digital literacy to help individuals protect themselves in an increasingly online world because a well-informed public is less likely to fall victim to fraud. should collaborate with media outlets, community organizations, and educational institutions to conduct regular awareness campaigns.

3. Effective fraud prosecution requires seamless collaboration between the NSCDC and other stakeholders, such as financial institutions, telecommunications providers, and international anti-fraud organizations. Establishing frameworks for intelligence-sharing and joint operations will enhance the ability to track and apprehend fraudsters with investigative tools such as digital forensics technology, blockchain analysis, and artificial intelligence. These tools will also enhance the ability to track and analyse digital transactions, detect patterns, and gather evidence effectively. Additionally, the introduction of GPS tracking devices and real-time surveillance systems will improve operational efficiency. Also, these partnerships will enable better intelligence-sharing, faster access to critical data, and joint operations to dismantle fraud networks. Memorandums of Understanding (MoUs) should be established to streamline these collaborations and ensure timely support.
4. Fraud is often fuelled by unemployment, poverty, and societal pressures. The government should intensify their efforts in implementing targeted socio-economic interventions, such as job creation programs, entrepreneurship training, and financial literacy initiatives, to address the root causes of fraud and reduce the number of individuals turning to criminal activities. Empowering the youth through education

Lead City University Ibadan DO NOT COPY

and economic opportunities will reduce their vulnerability to engaging in fraudulent activities.

5. To address the societal normalization of fraud, cultural reorientation programs should be introduced to promote ethical values and integrity. Schools, religious institutions, and community organizations can play a critical role in reshaping societal attitudes toward wealth acquisition and emphasizing the importance of hard work and honesty. Community leaders and local organizations can play a vital role in fraud prevention by promoting ethical values and reporting suspicious activities. The NSCDC should engage communities in its anti-fraud initiatives to create a collective sense of responsibility in combating fraud.

5.4 Contribution to Knowledge

This study has made important contributions to understanding how fraud occurs and is tackled within Oyo State, Nigeria, particularly focusing on the role of the Nigerian Security and Civil Defence Corps (NSCDC). It provides a detailed look at the nature of fraud, the challenges faced in investigating and prosecuting it, and practical ways to improve prevention and enforcement efforts. By addressing gaps in knowledge, this research has created a better understanding of fraud and how it affects individuals, institutions, and society as a whole.

One of the key contributions is the detailed exploration of the types of fraud prevalent in Oyo State. This includes Obtaining by False Pretence (OBT), cybercrime, visa racketeering, and ATM card swapping. By outlining how fraudsters operate, such as through phishing scams, fake documents, or social engineering, the study helps identify the tactics that need to be

Lead City University Ibadan DO NOT COPY

addressed. This knowledge is essential for law enforcement and policymakers to develop targeted strategies to combat these crimes.

The research also uncovered patterns in when fraud is most likely to occur. For instance, fraud peaks during festive seasons, academic admission cycles, and migration periods. By identifying these high-risk times, this study equips the NSCDC and other stakeholders with the ability to anticipate fraud trends and prepare their resources accordingly. This insight supports a more proactive approach to preventing fraud.

Additionally, this study has applied established theories, such as the Fraud Triangle and Routine Activity Theory, to the Nigerian context. It demonstrates how pressures like poverty and unemployment, combined with opportunities created by weak regulations and insider complicity, drive fraudulent behaviour. This adaptation helps deepen the understanding of fraud in developing economies and provides a basis for future research.

The findings also highlight the role of insiders, such as bank staff and telecom employees, who often help facilitate fraud. By exposing these vulnerabilities, the study stresses the importance of internal controls, regular audits, and whistle-blower protections to reduce insider involvement. This aspect is particularly valuable for institutions aiming to tighten their security.

Another key contribution is the emphasis on public awareness and education. The study shows that many victims fall for scams because of a lack of knowledge or technological literacy. This insight highlights the importance of running awareness campaigns and offering digital literacy programs to help individuals recognize and avoid fraud.

The research further sheds light on the challenges faced by the NSCDC, particularly in terms of limited funding and outdated tools. It calls attention to the need for more resources, such

Lead City University Ibadan DO NOT COPY

as digital forensic tools and better-trained personnel, to enhance the agency's ability to investigate and prosecute fraud effectively. These recommendations serve as a call to action for government and institutional support.

Lastly, the study provides practical solutions, including the need for a centralized fraud database, stronger collaboration between agencies and institutions. These recommendations offer clear steps that can be taken to improve how fraud is handled, both in the short and long term.

5.5 Suggested Areas of Further Studies

One important area for further study is how fraud trends and investigative challenges differ across states in Nigeria. A comparative analysis could provide a broader understanding of how factors such as socio-economic conditions, cultural differences, and levels of institutional support affect fraud patterns and enforcement strategies. This would help identify regional best practices that can be adopted nationwide. Another area worth exploring is the role of advanced technology in fraud prevention and investigation. Future research could assess how tools like blockchain analytics, artificial intelligence, and digital forensics can improve the efficiency and success of fraud detection efforts. This would guide law enforcement agencies on which technologies to prioritize and invest in.

The effectiveness of public awareness campaigns and digital literacy programs is another area that requires further study. Research could focus on how different types of education impact people's ability to identify and avoid fraud, helping to design more targeted and impactful outreach initiatives. The role of insider complicity in fraud also warrants deeper exploration. While this study highlights how insiders such as bank employees and telecom staff enable fraud, further research could investigate the specific motivations and

Lead City University Ibadan DO NOT COPY

organizational weaknesses that allow this to happen. Understanding this would help develop stronger internal controls and accountability mechanisms.

Additionally, future research could examine the long-term socio-economic impacts of fraud on individuals, families, and communities. This would provide policymakers with a clearer picture of how fraud undermines financial stability and trust in institutions, reinforcing the urgency of combating it. As fraud tactics evolve, there is also a need to study emerging schemes such as cryptocurrency scams, deep fake technology, and artificial intelligence-powered fraud. Research in this area would ensure that law enforcement agencies stay ahead of these trends and remain effective in preventing new forms of fraud.

Cross-border fraud and international collaboration present another avenue for future research. Many fraud cases, especially cybercrime and visa racketeering, involve perpetrators and victims in different countries. Examining how Nigeria can strengthen its partnerships with international organizations and improve legal frameworks for handling cross-border fraud would be highly beneficial. Behavioural studies on fraudsters could also provide new insights. Understanding the psychological and social factors that drive individuals to commit fraud could help develop targeted interventions and improve profiling techniques.

Lastly, future research could focus on improving Nigeria's judicial processes and legal frameworks for handling fraud cases. Examining the bottlenecks in prosecuting fraud cases and delivering justice to victims would provide actionable recommendations for streamlining the system and making it more effective. Additionally, victim-centred approaches, such as strategies to reduce re-victimization and provide better psychological support, could further enhance the fight against fraud. In summary, these areas of further study would provide a

Lead City University Ibadan DO NOT COPY

deeper understanding of fraud dynamics and help strengthen the strategies used to combat fraudulent activities, both in Nigeria and beyond.

Lead City University Ibadan DO NOT COPY

Bibliography

Books

Bourton S., *Tax Evasion and the Law: A Comparative Analysis of the UK and US,* Taylor & Francis, 2024, DOI: 10.4324/9781003333227-1

Cross, C., *Marginalized Voices: The Absence of Nigerian Scholars in Global Examinations of Online Fraud,* The Palgrave Handbook of Criminology and the Global South, 2018, pp.261-280.

Ekanem D., *Artificial Intelligence as a Mechanism for Crime Control in Nigeria: A Critical Appraisal.* Lap Lambert Academic Publishing, 2020.

Fraud, A.F., Other Fraud Related Offences Act, 2006. *Laws of the Federation of Nigeria*, *2*.2005

Gottschalk P., *Financial Crime Issues: Fraud Investigations and Social Control,* Springer Nature, 2022.

Holt T.J., Bossler A.M., & Seigfried-Spellar K.C., *Cybercrime and Digital Forensics: An Introduction*. Routledge, 2022, https://doi.org/10.4324/9780429343223

Page, M. T, *Innovative or Ineffective? Reassessing Anti-Corruption Law Enforcement in Nigeria* Working Paper 9, Gi-Ace Project: Fighting High-Level Corruption in Africa: Learning from Effective Law Enforcement, 2021, pp. 1-55.

Remeikienė, R., & Gaspareniene, L., *Effects on the Economic and Sustainable Development and on the Poverty and Social Inequality.In Economic and Financial Crime, Sustainability and Good Governance, Cham:* Springer International Publishing, 2023, 205-234

Internets

Corrupt Practices and Other Related Offences Act, https://www.icpc.gov.ng/wp-content/uploads/downloads/2012/09/Corrupt-Practices-Act.pdf, 2010

Criminal code act arrangement of sections criminal code cap 1955 "C38", https://lawsofnigeria.placng.org/laws/C38.pdf, L.N. 47 of 1955

Economic and Financial Crimes Commission (Establishment) Act https://www.efcc.gov.ng/efcc/images/pdfs/establishment_act_pdf, 2004

Lead City University Ibadan DO NOT COPY

Federal Republic of Nigeria, Cybercrimes. Prohibition, Prevention etc Act, https://www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc Act_pdf, 2015.

Nigeria Security and Civil Defence Corps (Amendment) Act, 2007, 2007 Act No.6 https://nscdc.gov.ng/nscdc-act/, 2007

Journals

Abioro T.A., *Public Procurement Corruption and Service Delivery in Nigeria And South Africa.* **Public Procurement, Corruption and the Crisis Of Governance In Africa**, 2021 pp. 249-267, https://doi.org/10.1007/978-3-030-63857-3_13

Adelakun B. O., Onwubuariri E. R., Adeniran G. A., & Ntiakoh A., *Enhancing Fraud Detection in Accounting Through AI: Techniques and Case Studies*, **Finance & Accounting Research Journal**, 6(6), 2024, pp.978-999, DOI: https://doi.org/10.51594/farj.v6i6.1232

Adeniyi D. S., *Corruption in the Nigerian Public Sector*, **International Journal of Research and Innovation in Social Science** 6, no. 7, 2022, pp. 632-636.

Afolabi, M. B., Dogi, I. G., Ogunniyi, L. J., Agidigbi, E. R., & Oladipo, I. E., *Securing the Critical Infrastructure in Ondo State: Is the Nigeria Security and Civil Defence Corps up to the Task*, **African Renaissance**, 21(3), 2024, p.169.

Agu J. C., Nkwo F. N., & Eneiga R. U. *Governance and Anti-Corruption Measures in Nigeria: Strategies for Enhancing Transparency, Accountability and Public Trust*, **International Journal of Economics and Public Policy** 8, no., 2024 pp. 1-15.

Akpoghome U. T., & Theophilus C. N., *The Collaboration of Investigative Authorities in Nigeria–Current Issues and Challenges.* **International Journal of Law 3**, no. 4, 2017, 39-48.

Ali, H. K., Umar, A. Y., & Danga, J. Y., *The Role of Nigeria Security and Civil Defence Corps In Nigeria's Internal Security*, **Arts and Social Science Research**, 13(1), 2023, pp.81-102, https://fassjassr.com.ng/index.php/assr/article/view/96.

Ama, G. A. N., Onwubiko, C. O., & Nwankwo, H. A., *Cybersecurity Challenge in Nigeria Deposit Money Banks***, Journal of Information Security,** 15(4), 2024, pp.494-523, DOI: 10.4236/jis.2024.154028

Ayinla O. A., *The Impact of Crime On Economic Hardship In Oyo State, Nigeria*. **International Journal of Social Science Research and Anthropology,** 4(6), 2024, https://taapublications.com/tijssra/article/view/173

Lead City University Ibadan DO NOT COPY

Balogun, A. O., Lawal, A. F., & Ekundayo, J. K., *An Analysis of Push and Pull Factors of Internet Fraud Among Selected Residents Of Ilorin Metropolis, Kwara State*, **Fuoye Journal Of Criminology And Security Studies**, 2(1), 2023

Bansal U., Bharatwal S., Bagiyam DS. & Kismawadi E. R., *Fraud Detection in the Era of AI: Harnessing Technology for a Safer Digital Economy.* In AI-Driven Decentralized Finance and the Future of Finance, **IGI Global**, 2024, pp. 139-160

Blakely, B., Kurtenbach, J., & Nowak, L., *Exploring The Information Content of Cyber Breach Reports and The Relationship To Internal Controls*, **International Journal of Accounting Information Systems,** 46, 2022, p.100568, https://doi.org/10.1016/j.accinf.2022.100568

Bozbayındır A. E., *The Role Of the Judge In the European Plea Bargaining Procedures: Three Models Compared*, **The International Journal of Evidence & Proof,** 28(3), 2024, pp.203-235, https://doi.org/10.1177/13657127231217773

Brown, A. S., Nigeria *Security and Civil Defence Corps and the Protection of Critical Assets and Infrastructure: Combating Oil Theft, Vandalism and Internal Insurgency for National Development*, **Ibom Journal of Social Issues**. Vol. 9. No. 1,2024, Afrischolar Discovery Repository (Annex).

Cadigan L., & Nath S., *Parallel Enforcement: SEC Authorities and How They Can Impact FDA's Civil and Criminal Enforcement*. **Food & Drug LJ,** 78, 2023, p.235.

Egodo H., Lucky I., Eyong B. B., & Sampson A.S., *Nigeria Security and Civil Defence Corps (Nscdc) Mandate and Infrastructural Protection in Cross River State, Nigeria*. **International Journal of Multidisciplinary Research and Growth Evaluation**, 2022

Falade P. V., *Analysis of 419 Scams: The Trends and New Variants in Emerging Types,* **Int. J. Sci. Res. in Computer Science and Engineering**, Vol, 11(5), 2023

Faqir R. S., *Digital Criminal Investigations in The Era of Artificial Intelligence: A Comprehensive Overview,* **International Journal of Cyber Criminology**, 17(2), 2023, pp.77-94, https://orcid.org/0000-0002-6102-0983

Felix U. O., *Evidence Collecting Processes and Fraud Examination: The Role Of an Expert Forensic Accountant***, Asian Basic and Applied Research Journal**, 4(1), 2022, pp.394-420, https://www.jofresearch.com/index.php/ ABAARJ/article/view/75

Hashim, H. A., Salleh, Z., Shuhaimi, I., & Ismail, N. A. N., *The Risk of Financial Fraud: A Management Perspective*, **Journal of Financial Crime,** 27(4), 2020, pp.1143-1159.

Lead City University Ibadan DO NOT COPY

Hortal, A., & Martínez, A. P., *Behavioral Strategies for Reducing Corruption: From Regulation to Choice Architecture*. **Behavioural Public Policy**, 2024, pp.1-18, doi:10.1017/bpp.2024.48

Kayser C.S., Back S., & Toro-Alvarez M.M., *Identity Theft: The Importance of Prosecuting on Behalf of Victims*." **Laws,** *13*(6), 2024, pp. 68, https://doi.org/10.3390/laws13060068

Kazaure A. A., Yusoff M. N., & Jantan A., *Digital Forensics Investigation Approaches in Mitigating Cybercrimes*, **A Review. Journal of Information Science Theory & Practice (JIStaP**), 11(4), 2023, pp. 14 DOI: 10.1633/JISTaP.2023.11.4.2

Kehinde Oyedeji, J., & Olamide Badmos, H., *Social Construction of Internet Fraud as Innovation among Youths in Nigeria,* **International Journal of Cybersecurity Intelligence & Cybercrime:** 5(1), 2022, 23-42, https://doi.org/10.52306/BUVC2778

Koomson, T. A. A., Owusu, G. M. Y., Bekoe, R. A., & Oquaye, M., *Determinants of Asset Misappropriation at The Workplace: The Moderating Role of Perceived Strength of Internal Controls,* **Journal of Financial Crime**, 27(4), 2020, pp.1191-1211.

Korejo, M. S., Rajamanickam, R., Md. Said, M. H., & Korejo, E. N., P*lea Bargain Dilemma, Financial Crime and Asset Recovery,* **Journal of Money Laundering Control**, 26(3), 2023, pp.628-639, https://doi.org/10.1108/JMLC-01-2022-0009

Kryshtanovych M., Lopatovskyi V., Bondaruk O., Datsii N., Primush R., & Dragan I., *Accounting, Analytical and Information Support for Law Enforcement Activity in Conditions of Ensuring Economic Security in Public Administration*. **Journal of Ecohumanism**, 3(6), 2024, pp.751-759.

Kwon J., J*urisdictional Overlap: The Juxtaposition of Institutional Independence and Collaboration in Police Wrongdoing Investigations*. **Regulation & Governance,** 18(2), 2024, pp.551-572, https://doi.org/10.1111/rego.12532

Legrand T., & Leuprecht C., *Securing Cross-Border Collaboration: Trans governmental Enforcement Networks, Organized Crime And Illicit International Political Economy*, **Policy and Society,** 40(4), 2021, pp.565-586, https://doi.org/10.1080/14494035.2021.1975216

Levi M. & Doig A, *Exploring The 'Shadows' in The Implementation Processes for National Anti-Fraud Strategies at The Local Level: Aims, Ownership, And Impact*. **European Journal on Criminal Policy and Research,** 26, no. 3, 2020, pp. 313-333.

Magakwe, J., *Curbing Corruption, Bribery, and Money Laundering in Public Procurement Processes: An International Perspective*, In Corruption, Bribery, and MoneyLaundering-GlobalIssues,IntechOpen,2024,DOI:10.5772/intechopen.1004005

Lead City University Ibadan DO NOT COPY

Marciniak III S. A., *Too Big to Protect: A Dodd-Frank Framework for Protecting 21st Century American Consumer Privacy Rights*. **Duq. L. Rev.,** 59, 2021, pp.329.

McGrath J. & Healy D*., Theorizing The Drop In White-Collar Crime Prosecutions: An Ecological Model,* **Punishment & Society**, 23(2), 2021, pp.164-189, https://doi.org/10.1177/1462474520939060

Medhi, D., Singh, P., Goswami, H., & Singh, J., *Futuristic Approach of Forensic Fraud Investigation in Money Embezzlement, Asset Misappropriation and Larceny*. **Educational Administration: Theory and Practice**, 30(6), 2024, pp.1283-1303.

Odinka, G. E., Okpa, J. T., Ushie, E. A., Ekpenyong, B. E., & Echu, S. N., *Exploring the Socio-Economic Dynamics of Youths' Involvement in Internet Fraud In Nigeria,* **Journal of Public Administration, Policy and Governance Research 1**, no. 3,2023, 83-91.

Ogunleye, Y. O., Ojedokun, U. A., & Aderinto, A. A., *Pathways and Motivations for Cyber Fraud Involvement among Female Undergraduates of Selected Universities in South-West Nigeria,* **International Journal of Cyber Criminology**, 13(2), 2019

Ogwumike, J. H. C*., Operational Equipment and Public Property Protection-A Study of Nigeria Security and Civil Defence Corps, Cross River State Command.* **International Journal of Democracy and Development Studies,** 5(3), 2022, pp.45-56.

Okafor, C. and Ani, J.K., *The National Youth Service Corps Programme and Growing Security Threat in Nigeria*. **Africa's Public Service Delivery & Performance Review,** 2(2), 2014, pp.149-164.: **https://doi.org/10.4102/apsdpr.v2i2.56**

Okafor, O. N., Adebisi, F. A., Opara, M., & Okafor, C. B., *Deployment of Whistleblowing as an Accountability Mechanism To Curb Corruption And Fraud In A Developing Democracy*, **Accounting, Auditing & Accountability Journal**, Vol. 33 No. 6, 2020, pp. 1335-1366. https://doi.org/10.1108/AAAJ-12-2018-3780

Okafor, O. N., Opara, M., & Adebisi, F., *Whistleblowing and The Fight Against Corruption and Fraud in Nigeria: Perceptions Of Anti-Corruption Agents (ACAs).* **Crime, Law and Social Change,** 73, 2020, pp.115-132.

Ololade, B. M., Salawu, M. K., & Adekanmi, A. D., *E-Fraud In Nigerian Banks: Why And How?*. **Journal of Financial Risk Management**, *9*(3), 2020 pp.211-228.

Osmond, N. O., Donald, E., & Akamike, O. J., *Impact of Fraud and Financial Crimes on the Nigerian*, **Direct Research Journal of Social Science and Educational Studies**, 11(5), 2023, Pp: 80-87, DOI: https://doi.org/10.26765/DRJSSES042358162172023

Lead City University Ibadan DO NOT COPY

Ozioko A. C., *Trends in Prosecuting Financial Crimes: Successes and Failures*, **Multi-Disciplinary Research and Development Journals Int'l**, 6(1), 2024, pp.28-54.

Pântea A., & Pantea S., *Countering Fraud to the Financial Interests of the European Union through Enhanced Cooperation*. **Acta Universitatis Danubius. Juridica,** 17(1), 2021, 167-175,

Ramos, S., Perez-Lopez, J. A., Abreu, R., & Nunes, S., I*mpact Of Fraud In Europe: Causes and Effects,* **Heliyon,** 2024, https://doi.org/10.1016/j.heliyon.2024.e40049

Rashid M.A., Al-Mamun A., Roudaki H., & Yasser Q.R., *An Overview of Corporate Fraud and Its Prevention Approach*, **Australasian Accounting, Business and Finance Journal** 16, no. 1, 2022, pp. 101-118, http://dx.doi.org/10.14453/aabfj.v16i1.7

Razaq, L., Ahmad, T., Ibtasam, S., Ramzan, U., & Mare, S., *We Even Borrowed Money From Our Neighbor" Understanding Mobile-based Frauds Through Victims' Experiences*, Proceedings of the ACM on human-computer interaction, **5(CSCW1),** 2021, pp.1-30, https://doi.org/10.1145/3449115

Ridwan, R., Abdullah, S., & Yusmita, F., *Implementation of Cashless Policy Strategies to Minimize Fraud in the Government Sector: Systemic Revie,* **Jurnal Akuntansi**, 12(3), 2022, pp.181-201.

Rohilla A., *Strengthening Financial Resilience: A Holistic Approach to Combatting Fraud,* **Indian Journal of Economics and Finance (IJEF**), 4(1), 2024, pp.20-31, http://doi.org/10.54105/ijef.A2566.04010524

Rossy, Q., & Ribaux, O., *Orienting the Development of Crime Analysis Processes In Police Organisations Covering The Digital Transformations Of Fraud Mechanisms.* **European Journal on Criminal Policy and Research**, 26, 2020, pp.335-356.

Salawu, M. K., Oyewobi, I. A., & Adejumo, O. A., *Internal Control System, Risk Management Practice and Fraud Prevention Among Selected State Governments in Southwestern Nigeria.* **TWIST,** 18(4), 2023, pp.123-134, https://twistjournal.net/twist/article/view/86

Sarki, U. S., & Ya'u, M., *The Role of NSCDC in Crime Prevention in Nigeria: Conceptual and Emperical Analysis.* **International Journal of Trend in Research and Scientific Development,** 2019, www.ijtsrd.com, e-ISSN: 2456 – 6470

Schwartz J., Steffensmeier D., Moser W.J. & Beltz L.*, Financial prominence and financial conditions: Risk factors for 21st century corporate financial securities fraud in the United States***. Justice Quarterly**, 39, no. 3, 2022, pp. 612-641, https://doi.org/10.1080/07418825.2020.1853799

Lead City University Ibadan DO NOT COPY

Simpson S. S., *Criminology and Corporate Crime: The Art of Scientific Cross Pollination,* **Annual Review of Criminology,**8,2024, https://doi.org/10.1146/annurev-criminol-022422-121435

Stowell N.F., Pacini C., Wadlinger N., Crain J.M., & Schmidt M., *Investigating Healthcare Fraud: Its Scope, Applicable Laws, And Regulations*. **William & Mary Business Law Review**, 11, no. 2, 2020, pp. 479.

Subramanian, R., Digard, L., Melvin Washington, I. I., & Sorage, S., *In the Shadows: A Review of The Research on Plea Bargaining*, **Vera Institute of Justice**, 2020, pp.1-64.

Tade, O., *A Spiritual Dimension to Cybercrime in Nigeria: The 'Yahoo Plus' Phenomenon.* **HumanAffairs,** 23(4),2013,pp.689705,https://doi.org/10.2478/s13374-013-0158-9

Tade O., *COVID-'419': Social Context of Cybercrime in the Age of COVID-19 in Nigeria.* **African Security** 14 (4), 2021, 460-483.

Tade, O., & Adeniyi O., *Automated Teller Machine Fraud in South-West Nigeria: Victim Typologies, Victimisation Strategies and Fraud Prevention,* **Journal of Payments Strategy & Systems**, 11(1), 2017, pp.86-92.

Tade, O., & Adeniyi, O., *Dimensions of Electronic Fraud and Governance of Trust in Nigeria's Cashless Ecosystem***, International Journal of Offender Therapy and Comparative Criminology**, 64(16), 2020 1717-1740. https://doi.org/10.1177/0306624X20928028

Tade, O., & Adeniyi O*., Automated Teller Machine Fraud in Southwest Nigeria: The Shoe Wearers' Perspectives.* **Irvine: University of California**, 2014,

Tade, O., & Adeniyi O*., I Prefer to Remain Old School and Be Safe": Fear of Fraud and Governance of Risk In Nigeria's Cashless Ecosystem,* **Salus Journa**l, 11(2), 2023, pp.120-132.

Tade, O., & Adeniyi O., *On the Limits of Trust: Characterising Automated Teller Machine Fraudsters in Southwest Nigeria,* **Journal of Financial Crime**, 23(4), 2016, pp.1112-1125.

Tade, O., & Adeniyi O., '*They Withdrew All I Was Worth': Automated Teller Machine Fraud and Victims' Life Chances in Nigeria*, **International Review of Victimology,** 23(3), 2017, 313-324. https://doi.org/10.1177/0269758017704330

Tade, O., & Aliyu I., *Social Organization of Internet Fraud Among University Undergraduates in Nigeria.* **International Journal of Cyber Criminology**, 2011, 5(2).

Lead City University Ibadan DO NOT COPY

Tade, O., *Nature of Frauds in Nigeria's Banking Ecosystem, 2015-2019*, **Journal of Financial Crime**, Vol. 29 No. 4, 2022, pp. 1241-1248. https://doi.org/10.1108/JFC-08-2021-0185

Tade, O, *Policing Looted Funds with The Whistle,* **Africa Development/Afrique et Développement**, 44(4), 2019, pp.73-90.

Tinuoye A.T., *An Overview of Corruption in The Context of The Public Sector*. Management Strategies and Tools for Addressing Corruption in Public and Private Organizations, 2023 pp. 19-38. DOI: 10.4018/978-1-6684-8536-1.ch002

Tiutiunyk A. Kuzior, I., Zielińska A., & Kelemen R., "*Cybersecurity and Cybercrime: Current Trends and Threats*, **Journal of International Studies,** 17, no. 2., 2024, pp. 2071-8330

Vitus E. N., *Cybercrime and Online Safety: Addressing the Challenges and Solutions Related to Cybercrime, Online Fraud, and Ensuring A Safe Digital Environment for All Users—A Case of African States***. Tijer-International Research Journal**, 10(9), 2023, pp.975-989, SSRN: https://ssrn.com/abstract=4589211

Waterman D. A., *A Defendant's Ability to Pay: The Key to Unlocking the Door of Restitution* **Debt. Iowa L. Rev**., 106, 2020, pp.455.

Whitty, M. T., *419-It's Just A Game: Pathways to Cyber-Fraud Criminality Emanating from West Africa.* **International Journal of Cyber Criminology**, 12(1), 2018, pp.97-114.

Yagboyaju, D. A., & Simbine, A. T., *Political Finance and the 2019 General Elections in Nigeria.* **Journal of African Elections,** 19(1), 2020, pp.66-91.

Theses / Dissertations

Egberedu, M., *Accessibility and Utilisation of Information and Communication Technology by The Nigeria Security and Civil Defence Corps in Southwestern Nigeria*, PhD diss., 2020, http://hdl.handle.net/123456789/1070

Henderson P.D., *Organizational Leaders' Strategies to Detect and Prevent Occupational Fraud*. PhD diss., Walden University, 2024.

Ogunsanya, A. O., *Exploring Citizen Security in the Nigeria Federated State: Lagos State Neighbourhood Safety Agency in Perspective*, PhD diss., Walden University**,** 2021.

Worme K. R., *Corporate Governance–A Comparative Analysis of The Approach to Corporate Governance Regulation and Enforcement in the UK and the US*, Liverpool John Moores University (United Kingdom)**,** 2024, pp. 15-362

Lead City University Ibadan DO NOT COPY

Appendix 1

Interview Questions

Objective One: Dynamics of fraud prosecuted by NSCDC in Ibadan: Probe for;

IDI for Detectives

1. Based on your experience, what are the common types of fraud you have encountered within the NSCDC dataset?
2. Can you describe any specific incidents or trends of fraud that you have observed in Ibadan?
3. What factors do you believe contribute to the occurrence of fraud within the NSCDC dataset?
4. How has the nature of fraud evolved over the time you have been working in this field?

Objective Two: Cost of fraud prosecution and how it affects investigation strategies and outcomes: Probe for;

IDI for Detectives

1. How does the financial cost of prosecuting fraud cases impact the strategies you employ in investigations?

Lead City University Ibadan DO NOT COPY

2. Can you provide examples where the cost of prosecution has influenced the decision to pursue or drop a case?
3. In what ways do budget constraints affect the resources allocated for fraud investigations?
4. How do financial considerations impact the overall effectiveness of fraud investigations and prosecutions?

Objective Three: Tactics and strategies utilized in perpetrating fraud: Probe for;

IDI for Detectives

1. What are the most common tactics and strategies you have identified that fraudsters use to perpetrate fraud?
2. Can you provide specific examples or case studies of successful fraud tactics?
3. How do fraudsters adapt their strategies in response to new security measures or investigations?
4. What emerging trends or new methods of fraud have you observed recently?

Objective Four: Characterizes fraud perpetrators investigated by NSCDC Oyo State Command: Probe for;

IDI for Detectives

1. Based on your investigations, what are the typical characteristics of individuals who commit fraud within the NSCDC?

Lead City University Ibadan DO NOT COPY

2. Are there particular demographic or socio-economic profiles that are more commonly associated with fraud perpetrators?
3. What organisational roles or positions are most frequently involved in fraudulent activities?
4. Can you discuss any common motives or incentives that drive individuals or entities to commit fraud?

Objective Five: Fraud patterns and time of occurrence: Probe for;

IDI for Detectives

1. Have you noticed any specific timeframes or periods when fraudulent activities are more prevalent?
2. Are there particular seasons, months, or events that coincide with spikes in fraud occurrences?
3. How do temporal patterns of fraud affect your investigation strategies and resource allocation?
4. Can you provide examples of how understanding these patterns has helped in preventing or mitigating fraud?

Lead City University Ibadan DO NOT COPY

Lead City University Ibadan DO NOT COPY

Bio-data

A. Personal Data

1. **Full Name:** Olalekan Olawale TAIWO

   (Cathedral of St. James The Great Oke-Bola Ibadan, tunmixee@gmail.com 08072016751 ,08164176352)

2. **Date and Place of Birth:** 24th June, 1993, Ibadan
3. **Nationality:** Nigeria
4. **Marital Status:** Single
5. **No. of Children & their age: Nil**
6. **Name and Address of Spouse: Nil**

   (Including E-mail address & Phone no)

7. **Name and Address of Next of Kin:** Mr. Sunday Samuel Taiwo

   (Cathedral of St. James The Great Oke-Bola Ibadan)

B. Educational Background

1. **Educational Institutions Attended with Dates and Qualifications:**

   i. Adventist nursery/primary school, Oke-Bola Ibadan. (1996-2003) (PSLC)

   ii. Oke-Bola Comprehensive High School, Ibadan (2003- 2009) (SSCE)

   iii. National Open University of Nigeria, Abuja (2013-2017) (B.Sc.)

   iv. Lead City University, Ibadan, Nigeria (2023) (M.Sc. in-view)

C. Work Experience with Date

Graduate Assistant: Department of Criminology and Security Studies, Lead City University, Ibadan, Nigeria (Sept 2023 – Present)

|Police Detective College (NPF), General Detective Course |(2016)

Lead City University Ibadan DO NOT COPY

Ibadan Diocese Team for the Church of Nigeria ACADI Team (Dec 2023-Present)

Administrative Officer | Chrisland University Registry | (May 2021 – Feb 2023)

Team Member; WideGates Initiatives (Aug 2019-Present)

Mentor at Tony Elumelu Foundation (Jul 2024)

D. Awards and Fellowships:

i. Rotary Youth Leadership Award (2013)

ii. Scholarship Aid Initiative Award (2013)

iii. NHIP Early Bird Trainee Award (2018)

iv. Ison BPO Best Agent Award (2021)

E. Membership of Academic Professional Bodies

i. Nigeria Society for Criminology

F. Publications:

1. Thesis/Dissertation

2. Books/Monographs

(a) Authored Books: Nil

(b) Edited Books: Nil

(c) Contribution to Books: Nil

3. Published Referred Conference Proceedings: Nil

4. Paper Accepted for Publication: Nil

5. Book Reviews and Commentaries in Scholarly Journals: Nil

6. Technical Reports: Nil

7. Technical Reports: Nil

8. Creative Work: Nil

Lead City University Ibadan DO NOT COPY

9. **Notable Scholarly or Professional Accomplishment:** Nil

G. Major Conference/Workshops Attended:

1. Transformation Leadership for Academic Excellence Enhancing Quality and Innovation **(2025)**
2. Faculty of Management and Social Sciences International Conference **(2024)**
3. Postgraduate College Multidiscipline International Academic Conference **(2023)**

H. Names and Addresses of Referees

Professor Babajide Owoeye
Council Chamber, Lead City University, Ibadan, Nigeria
+2348037250417
chairman@lcu.edu.ng

Professor Tade Oludayo
Department of Sociology, Criminology and Security Studies Unit, University of Ibadan,
+2348116164291
dotad2003@yahoo.com

Lead City University Ibadan DO NOT COPY

Signature **Date**

The University Compliance Certification

This is to certify that, this thesis was written by **Olalekan Olawale TAIWO** with matriculation number **LCU/PG005233** in the Department of Criminology and Security Studies, Faculty of Management and Social Sciences, Lead City University, Ibadan in full compliance with the approved University format and style.

_____ _____

Signature **Date**

Lead City University Ibadan DO NOT COPY