Love, Lies, and Larceny: One Hundred Convicted Case Files of Cybercriminals with Eighty Involving Online Romance Fraud

{ACCEPTED COPY}

Cite as:

- Soares, A. B., Lazarus, S., & Button, M. (2025). Love, Lies, and Larceny: One Hundred Convicted Case Files of Cybercriminals with Eighty Involving Online Romance Fraud. *Deviant Behavior*, 1–24. https://doi.org/10.1080/01639625.2025.2482824

Abstract

This article examines 100 convicted case files of cybercriminals, 80 of which concern online romance fraud. While all were prosecuted by the Economic and Financial Crimes Commission in Nigeria, many involve multiple offenses, including crypto investment fraud and hacking. The study provides critical insights into offender profiles and the criminal justice system's approach to cybercrime enforcement. Drawing on the Space Transition Theory (STT), the study highlights the transient and intermittent nature of criminal activities in cyberspace. The findings reveal that most offenders are young males aged 18–28, predominantly university undergraduates or graduates. Notably, 96% of offenders hail from southern Nigeria, and 80% of crimes involve romance fraud. While perceptions of leniency in cybercrime punishments persist, 96% of offenders acted as primary perpetrators, with 2% serving as mules or accomplices and another 2% adopting dual roles. By relying on actual case files of online offenders rather than online profiles, which are often fake, this study offers unique insights that can inform future research and support evidence-based strategies to address cybercrime in Nigeria and beyond

1. Introduction

This article examines one hundred case files of cybercrime offenders in a Nigerian context. It offers an in-depth understanding of offender profiles and the criminal justice system's strategies for addressing cybercrime. The study is particularly relevant given Nigeria's prominence as a major hub for cybercrime, with a well-documented history of fraud schemes targeting victims worldwide (Lazarus and Okolorie 2019; Lazarus 2024). A qualitative study commissioned by the UK Home Office identified West African nations, including Nigeria, as high-risk jurisdictions for fraud, particularly in scams directed at Western countries (Button et al. 2024). The World Cybercrime Index ranks Nigeria as the leading country in Africa for cybercrime and fifth globally. This ranking is based on key factors such as technical expertise, operational impact, and cash-out mechanisms (Bruce et al. 2024). These rankings highlight the sophistication and global reach of cybercriminal networks in the region. A key driver of Nigeria's cybercrime notoriety is the so-called "Yahoo Boys," who engage in various forms of online fraud, commonly referred to as "Yahoo Yahoo" (Aborisade 2023; Lazarus et al. 2023a). Their activities range from traditional advanced fee fraud, or 419 scams, to more complex operations. These include romance fraud (Aborisade, Ocheja, and Okuneye 2024), sextortion (Button et al. 2024), and business e-mail compromise (Lazarus 2024). Over time, these networks have also expanded their operations to include cryptocurrency fraud (Garba, Lazarus, and Button 2024). This shift reflects the evolving nature of financial cybercrime in Nigeria.

Research on offender profiles in West Africa and the diaspora provides a crucial empirical context for understanding the regional nature of online fraud. Ghana and Nigeria remain dominant actors in online romance fraud (Lazarus and Soares 2025; Lazarus et al. 2025; Lazarus et al. 2025). Existing studies highlight the demographic characteristics, motivations, and operational structures of offenders, offering insight into the factors that drive engagement in cyber-enabled financial crimes (Abubakari 2023; Abubakari and Amponsah 2024; Garba, Lazarus, and Button 2024). Yet, while existing research has explored the perspectives of fraudsters in West Africa, specifically in Nigeria (Aransiola and Asindemade 2011) and Ghana (Lazarus et al. 2025), empirical studies drawing insights from convicted online fraudsters remain limited. To date, only two empirical studies, Garba, Lazarus, and Button (2024) on convicted cryptocurrency-fraud offenders and Soares and Lazarus (2024) on convicted dating-fraud perpetrators, have analyzed case files of convicted cybercriminals to under- stand economic cybercrime. This study seeks to fill this gap by examining one hundred case files of convicted cybercriminals, most of whom are online romance fraudsters.

Online romance "scams"[1] exploit intimate relationships for financial gain (Lazarus et al., 2023b; Lazarus et al. 2025; Yushawu and Jaishankar 2025). Offenders create fraudulent dating profiles to deceive and manipulate victims. The primary objective of this research is to investigate these case files to better understand the profiles of convicted offenders, victim-targeting strategies, and sentencing patterns. By doing so, the study aims to enrich the empirical literature on cybercrime. It offers critical insights for both regional and international stakeholders seeking to combat online fraud.

2. Literature review

The literature on romance fraud issues originating from West Africa highlights that scammers are not mere impersonators but skilled manipulators who adapt their narratives to victims' responses, enhancing the emotional effectiveness of their deception (Aborisade, Ocheja, and Okuneye 2024; Abubakari 2024; Lazarus et al. 2025; Soares and Lazarus 2024). Along similar lines, findings from Abubakari's (2024) ethnographic study in Ghana show that offenders create multiple fake profiles using images of Western military personnel, models, and businessmen to target specific victim demographics, often categorized into formats such as "Military" and "Business." Similarly, studies that rely exclusively on online data sources have reported comparable findings. These include analyses of music lyrics (Lazarus, 2018), dating profiles (Kopp et al., 2015), offenders' messages (Anesa, 2020), and scammer profiles (Suarez-Tangil et al., 2020). Kopp et al. (2015) revealed that

[1] This article uses "scam" and "fraud," as well as "scammers" and "fraudsters," interchangeably. While "scam" is widely used by the media, financial institutions, and the public, organizations such as the Global Anti-Scam Alliance (GASA), Scamwatch, Scam Survivors, and Scam Baiters incorporate this term in their names. In academic discourse, "fraud" is often preferred to emphasize the legal and financial dimensions of these crimes (Lazarus et al. 2025a).

scammers design profiles with evolving narratives that align with victim interactions, increasing their credibility and impact. In parallel, Anesa (2020) noted that scammers use structured message patterns to foster emotional dependency, aligning with Kopp et al. (2015) findings. Suarez-Tangil et al. (2020) demonstrated how scammers mimic authentic user profiles to evade detection on dating platforms. Collectively, these studies illustrate how scammers leverage technological and social cues to craft convincing deceptions, showcasing their strategic and manipulative abilities.

In a comparable manner, Lazarus et al. (2023a: 8) analysis of 33 Nigerian hip–hop lyrics shows that romance scam victims are routinely dehumanized, depicted as cognitively deficient "maga" (a term connoting game animals or fools) or as "cash cows." This lyrical framing reinforces a blend of victim– blaming and dehumanization that primarily functions to shield online fraudsters from remorse (see also Lazarus 2018: 70). This dehumanization is especially evident in many songs that use irony and double entendre to mock victims while portraying dating fraudsters as superior "hunters" in the digital domain (Lazarus et al. 2023a: 10; Lazarus 2018: 70). Collectively, these studies illustrate how cultural artifacts, such as music, can both reflect and reinforce the moral disengagement strategies used by online fraudsters. These representations shape public perceptions of victims and contribute to the legitimization of exploitative behavior.

Bilz, Shepherd, and Johnson (2023) and Lazarus et al. (2023b) further observed that rapport-building plays a pivotal role in romance fraud, as scammers adopt familiar relationship behaviors to establish trust, gather personal information, and enhance the plausibility of their personas. Once trust is secured, they script expectations of loyalty and support, framing exploitative requests as natural relationship dynamics (Carter 2024; Herrera and Hastings 2024; Lazarus et al., 2023b). This process transforms manipulation into what appears to be a genuine emotional connection, relying on crafted storytelling and feigned vulnerability to create reciprocal trust.

Other researchers have examined West African internet fraudsters operating under various identities across the region, manipulating victims through different forms of advance fee fraud (Alhassan and Ridwan 2023; Lazarus 2018; Lazarus and Okolorie 2019; Lazarus et al. 2025; Yushawu and Jaishankar 2025). These groups include "Brouteurs" in Côte d'Ivoire (Cretu-Adatte et al. 2024), "Yahoo Boys" in Nigeria (Lazarus, Button, and Adogame 2022), "Sakawa Boys" in Ghana (Abubakari 2024; Alhassan and Ridwan 2023; Lazarus et al. 2025), and "Feh men" or "Feh guys" in Cameroon. Similarly, Han and Button's (2025) interviews with Chinese victims and police officers reveal that scammers strategically persuade victims to invest a small sum, fostering a sense of commitment that escalates into significant financial loss. This tactic mirrors the Nigerian 419 fraud model, also known as advance fee fraud, which was pioneered and refined in the 1980s and 1990s by prominent, highly "educated fraudsters, including *Fred Chijindu Ajudua*, a Nigerian lawyer" (Lazarus et al. 2023a, p.10). Despite regional variations, these groups employ overlapping tactics, allowing them to adapt and enhance their effectiveness in exploiting victims, particularly in romance scams and other online fraud schemes.

Researchers have consistently highlighted the psychological and emotional toll of romance scams, arguing that the harm often extends beyond financial loss (Bilz, Shepherd, and Johnson 2023; Lazarus et al., 2023b). This is supported by a Lloyds Banking Group-commissioned survey (Lazarus and Ziegler 2024) and systematic reviews covering over two decades (Bilz, Shepherd, and Johnson 2023; Lazarus et al., 2023b). Button et al. (2021) and Cross and Holt (2023) emphasize that fraud victims experience trauma comparable to sustained psychological abuse. Cole (2024), through qualitative interviews with 19 participants, as well as Modic and Anderson (2015), through a large-scale survey of 6,609 respondents, illustrate how emotional manipulation, when combined with monetary exploitation, compounds victim harm. Drew and Webster (2024), Cole (2024), and Thumboo and Mukherjee (2024) identify clear parallels between romance scams and emotional abuse, noting that offenders strategically target victims at vulnerable life stages. Drew and Webster (2024) further analyze how scammers adapt their methods to foster trust and dependence, making victims more emotionally invested and vulnerable. This calculated approach intensifies psychological distress and financial consequences. While Lazarus and Ziegler (2024) highlight the urgent need for tailored support systems addressing both financial and psychological recovery, the findings above collectively highlight the importance of post-scam services that prioritize victims' emotional well-being and financial stability. Research highlights significant disparities between scammers' fabricated identities and their real profiles (Herrera and Hastings 2024, Huang, Stringhini and Yong, 2015; Lazarus et al., 2023b; Soares and Lazarus 2024). To exploit perceived credibility, West African scammers consistently align their demographic claims with high-trust locations, such as North American nations and Europe (Abubakari 2024; Button et al. 2024). Similarly, Soares and Lazarus's (2024) examination of convicted romance scammers in Nigeria and

Abubakari's (2024) interviews with active scammers in Ghana collectively reveal that these offenders frequently pose as nationals from Western countries, such as the United States, which have high online dating activity. Abubakari (2024) further demonstrated that offenders in Ghana believe adopting non-Western identities reduces their chances of eliciting responses on dating apps or social media. This reluctance stems from the tendency of Western users to hesitate in engaging with individuals from Africa south of the Sahara due to racial, economic, and historical prejudices (e.g., Lazarus, Whittaker, McGuire, and Platt, 2023b). Additionally, Lazarus et al. (2025) found that online romance offenders justify their actions through higher loyalties, portraying fraud as reparative justice for colonial exploitation. While these offenders frame their crimes as a means of reclaiming wealth taken during colonial rule, the findings indicate that online romance fraudsters view colonial legacies as a key driver of cybercrime.

Furthermore, disclosing personal information significantly increases the risks faced by victims of romance scams. Studies by Cross and Holt (2023), Soares and Lazarus (2024), and Cross and Holt (2021) consistently demonstrate that such disclosures heighten victims' vulnerability to both financial exploitation and physical threats. For instance, Cross and Holt (2023) observed that victims who shared personal information were exposed to greater risks, while Cross and Lee (2022) documented cases where victims feared not only financial loss but also physical harm, including threats of kidnapping. Additionally, Cross and Holt (2021) highlighted that many were defrauded by scammers' frequent use of fictitious military identities. Abubakari's (2024) and Soares and Lazarus's (2024) findings corroborate these observations, noting that West African scammers often employ military identities to increase their credibility and gain victims' trust. In particular, Soares and Lazarus (2024) demonstrated that the majority of offenders posed as Caucasian American males (46%), while 56% of victims were from the United States. These findings illustrate that scammers' strategies go beyond financial deception, leveraging emotional manipulation and physical intimidation to exert control on their romance fraud victims.

Certain dimensions of differentiation are pivotal in shaping how scammers construct fraudulent profiles. For example, research by Soares and Lazarus (2024) highlights a significant gender disparity among victims: 70% of offenders primarily targeted women, 14% targeted men, 10% targeted both genders and 6% did not specify the victims' gender. Scammers often misrepresent traits such as masculinity, financial stability, and cultural identity to align with victims' expectations, thereby enhancing their perceived trustworthiness (Bilz, Shepherd, and Johnson 2023; Soares and Lazarus 2024). Kopp et al. (2015) observed that male scammer profiles emphasize masculinity, wealth, humor, and religious devotion, while female profiles often highlight financial independence and sometimes include suggestive characteristics. Edwards et al. (2018) examined 5402 online profiles and further noted frequent misrepresentations of gender, race, and profession tailored to match the scammers' claimed geographic origins. For example, male personas are commonly linked to regions such as Malaysia, South Africa, and Nigeria, while female identities are frequently associated with Senegal, Ukraine, and the Philippines. However, scammers' use of VPNs to obscure their actual locations complicates efforts to analyze geographic patterns reliably. These findings collectively suggest that gendered portrayals are not merely deceptive tactics but exploit culturally ingrained trust signals, enabling scammers to manipulate victims more effectively.

Victim vulnerability is a key theme in the literature on romance scams, with studies examining the interplay between psychological and socioeconomic factors that increase susceptibility to fraud (Carter 2024; Lazarus et al. 2025). Researchers consistently highlight that vulnerability arises from a combination of factors rather than a single cause. Studies on catfishing, a subset of romance scams, identify specific risk factors linked to victim susceptibility (e.g., Snyder and Golladay, 2024). Snyder and Golladay's (2024) study of over 1,500 catfishing victims found that nearly half had been deceived multiple times. Common tactics include initiating contact, misrepresentation, avoiding video communication, and soliciting financial support, with victims providing money in about half of the cases (Snyder and Golladay, 2024). As part of this deception, scammers frequently transition from e-mails to platforms like WhatsApp or Google Hangouts to gain identifying information and strengthen their relationship with the victim (Dickinson, Wang, and Maimon 2023). These patterns suggest that while psychological traits contribute to vulnerability, scammers' strategies reinforce and perpetuate these susceptibilities, creating a recurring cycle of victimization.

The literature reveals significant gaps in current strategies for preventing and detecting romance scams. While Cross and Holt (2021) highlight the potential effectiveness of proactive measures, such as security warnings, Suarez-Tangil et al. (2020) demonstrate that scammers' sophisticated mimicry complicates detection, particularly on platforms that lack advanced textual analysis capabilities. Cross

and Holt (2021) found that early security warnings reduced victims' susceptibility. Soares and Lazarus (2024) reported that 74% of romance fraudsters were university students, with Facebook being the most frequently used platform for fraudulent activities (46%). Additionally, Lazarus and Soares (2025) observed that some romance scammers acquire their skills in Hustle Kingdoms, which function as cybercrime apprenticeship schools. "These institutions [sometimes called Hustle Kingdoms, cyber- crime academies or scamming schools] systematically train individuals in Internet fraud through structured learning, peer support, and mentorship" (Lazarus and Soares 2025:1–2). The emergence of Hustle Kingdoms, scamming schools, and underground cybercrime training centers in West Africa reflects the persistence of socioeconomic inequalities and systemic barriers that drive individuals toward cybercriminal enterprises (Lazarus and Soares 2025). Despite these insights, the effectiveness of prevention measures remains uncertain due to the diversity of the platforms and the adaptability of scammers.

Nonetheless, these findings collectively indicate that a multifaceted approach is essential. Numerous research papers have explored cybercrime in Nigeria (Ajayi, Adesope, and Oso 2024; Akanle, Adesina, and Akarah 2016; Aransiola and Asindemade 2011; Lazarus and Okolorie 2019; Lazarus and Soares 2025; Ogunleye, Ojedokun, and Aderinto 2019; Ojedokun and Eraye 2012; Orhero and Nwoke 2025). Only a few studies, such as Soares and Lazarus (2024), Aborisade et al. (2024), and Lazarus et al. (2025), focus specifically on romance fraud. Similarly, despite extensive research on romance scams (Abubakari 2024, Cole, 2024; Cross and Holt 2021; Lazarus et al. 2025), no studies, except for Soares and Lazarus (2024), have utilized convicted case files of romance scammers. However, Soares and Lazarus (2024) focused on a different timeline and region, analyzing cases that exclusively involved romance scams in Nigeria. Direct examination of convicted romance scam offenders is needed. This study seeks to contribute to the ongoing discussion on romance fraud offenders by analyzing case files of convicted online romance scammers prosecuted by Nigeria's Economic and Financial Crimes Commission (EFCC).

Established in the early 2000s, Nigeria's Economic and Financial Crimes Commission (EFCC) was tasked with combating economic crimes, particularly online fraud, to restore the country's tarnished international reputation (Lazarus and Okolorie 2019; Lazarus and Soares 2025). While the EFCC's formation represented a critical step in addressing cybercrime, the literature underscores that Nigeria's reputational challenges extend beyond cybercrime. Corruption among public officials, as extensively analyzed by Ibrahim (2016), Hall and Yarwood (2024), Lazarus and Soares (2025), and Smith (2017) remains a significant barrier. It indicates that anti-cybercrime measures alone are insufficient for holistic reputational repair.

Nevertheless, the EFCC is widely regarded as one of West Africa's most impactful agencies in prosecuting cybercrime (Lazarus and Okolorie 2019; Orji, 2019). However, the systemic challenges it faces are deeply intertwined with broader societal factors influencing cybercrime offenders in Nigeria (Orji, 2019; Soares and Lazarus 2024). Profiling these offenders requires an understanding of their multifaceted activities, as their online behaviors often reflect their offline realities. This study aims to explore the dynamics of romance scammers and evaluate the relevance of Space Transition Theory in understanding their behavior.

Table 1: Summary of Space Transition Theory Propositions

Proposition Theme	Key Elements	Description
Repressed Criminal Behavior	Physical vs. Cyberspace	Offenders may commit crimes in cyberspace that they would not undertake in the physical world.
Identity Flexibility and Anonymity	Cyberspace Characteristics	The anonymity and flexible identities in cyberspace lower deterrents, encouraging cybercriminal activity.
Import-Export of Criminal Behavior	Cyberspace to Physical Space	Criminal behaviors can transfer between digital and physical spaces, showcasing their interconnectedness.
Intermittent Ventures	Dynamic Nature of	The transient nature of cyberspace allows offenders to

Proposition Theme	Key Elements	Description
	Cyberspace	evade consequences and engage in sporadic criminal acts.
Unification of Strangers and Associates	Collaboration in Cyberspace	Cyberspace facilitates criminal collaboration between strangers and associates across different environments.
Influence of Closed Societies	Societal Characteristics	Individuals from closed societies are more inclined to engage in cybercrime than those from open societies.
Conflict of Norms and Values	Norms Clash	Conflicting norms between physical and cyberspace environments may push individuals toward cybercrime.

Source: Adapted from Garba et al. (2024: 6)

3. *Theoretical background*

This study applies the Space Transition Theory to analyze online romance scams, as summarized in Table 1. Developed by Jaishankar (2007) and (2008), the theory provides a framework for under- standing behavioral shifts between physical and virtual spaces. It posits that individuals may conform to norms in one setting while engaging in deviant actions in another, influenced by the unique characteristics of each space (Jaishankar 2008, 2018). Jaishankar underscores the theory's relevance in cybercrime research, particularly its ability to explain online deviance (Ngo and Jaishankar 2017). Crucially, the Space Transition Theory does not suggest that individuals without criminal tendencies in the physical world will engage in fraud online simply due to anonymity. Rather, it argues that those with repressed criminal tendencies, individuals constrained by sociocultural, legal, or personal deterrents in physical space, may exploit cyberspace, where these constraints are weakened. The flexibility and anonymity of the internet lower traditional barriers to crime, enabling individuals to act on previously suppressed behaviors. This dynamic is particularly relevant in West Africa, where strict sociocultural and legal constraints shape patterns of criminal behavior.

Empirical studies provide support for these theoretical claims. Garba, Lazarus, and Button (2024) and Soares and Lazarus (2024) examine cybercrime in Nigeria, focusing on cryptocurrency offenders and online romance fraudsters, respectively. Their findings align with the Space Transition Theory, particularly in illustrating how dissociative anonymity and identity flexibility in cyberspace allow offenders to manipulate victims and enhance their credibility. Similarly, Abubakari (2023) highlights how women, whose involvement in offline fraud is heavily constrained by societal norms, engage in online romance scams under the cover of anonymity. Meanwhile, Assarut, Bunaramrueang, and Kowpatanakit (2019) observe a broader tendency for individuals in Thailand to commit cybercrime, reinforcing the Space Transition Theory's applicability across different cultural contexts.

Although Abubakari (2023) does not explicitly apply Space Transition Theory as Garba, Lazarus, and Button (2024) and Soares and Lazarus (2024) do, the study demonstrates how offline deterrents influence cybercriminal behavior, further validating the theory's relevance in cybercrime research in Africa south of the Sahara. These studies collectively illustrate how transitions between physical and virtual spaces shape online criminal behavior. The space Transition Theory, therefore, offers a valuable lens for understanding how transitions between physical and virtual spaces shape online criminal behavior, providing insights into the mechanisms of romance scams and other forms of digital crime.

4. Method and materials

Like Garba, Lazarus, and Button (2024) and Soares and Lazarus (2024) studies in Nigeria, this study utilized documentary analysis, focusing on case files from the Economic and Financial Crimes Commission (EFCC). One hundred cases, primarily involving convictions for romance scams, were selected from one of the EFCC's Zonal Commands. The sample covered convictions

secured between January 2021 to April 2023, with selection criteria including the offender's mode of arrest, financial amounts, role in the scheme, victim's country, and penalties imposed. This structured approach ensured a focus on significant, recent cases within a defined timeframe.

Justification for using case files

The decision to use case files in this study is justified on several grounds. Ethically, relying on case files mitigates the challenges associated with interviewing active offenders, reducing potential risks for both researchers and participants. From a cost-effectiveness standpoint, accessing existing legal records is more practical and resource-efficient than conducting extensive fieldwork, which may require pro- longed engagement and logistical expenses. Judicially, case files offer direct insight into how the legal system processes cybercriminals, providing a structured and verifiable source of offender profiles, sentencing patterns, and judicial responses. This approach ensures a robust investigation into cyber-crime in Nigeria.

Documentary analysis framework

Scott's (2014) framework for document analysis guided the evaluation of case files, applying four criteria: authenticity, credibility, representativeness, and meaning (Platt 1981). This systematic approach ensured the validity and relevance of the data to the research objectives. Recognizing the limitations of documentary sources, often created for purposes such as prosecution rather than research (Denscombe 2017), the study acknowledged potential contextual constraints (Appleton and Cowley 1997; Denscombe 2017).

Recent case files were prioritized to enhance reliability, following Blackstone's (2019) recommendation to minimize historical bias. Cross-referencing offenders' handwritten statements with investigation reports reduced biases and verified data accuracy. Consistent with methodologies in related studies (Garba, Lazarus, and Button 2024; Scott et al. 2023; Soares and Lazarus 2024), variables such as age, gender, and the punishment imposed were documented. Data were systematically organized into an Excel spreadsheet for detailed content analysis and comparative review.

Ethical considerations

Access to sensitive case files required ethical clearance from both law enforcement and academic institutions. The research team included representatives from both sectors. Formal agency approval, with the official number *CB:4000/EFCC/UYO/LEGAL/VOL.1/103*, permitted data access, ensuring compliance with legal protocols. Additionally, ethical clearance was obtained from one of the authors' universities. The study adhered to the Helsinki Declaration, ensuring participant confidentiality, data integrity, and ethical standards.

Data and scope of analysis

This study provides an overview of judicial outcomes (n = 100) on a case-by-case basis. Notably, no appeals were filed post-conviction, ensuring the data represented final legal outcomes. The cases analyzed were independent, with no evidence of offender collaboration, reflecting individual criminal activities.

Comparative methodology

The approach aligns with prior research that leveraged law enforcement data to study cybercrime networks (Garba, Lazarus, and Button 2024; Lusthaus et al., 2023; Leukfeldt and Holt 2019; Soares and Lazarus 2024). For instance, Soares and Lazarus (2024) examined 50 cases in Nigeria, while Leukfeldt et al. (2017) investigated 18 Dutch cybercrime cases, both focusing on offender characteristics and operations. Similarly, Lusthaus et al. (2023) analyzed 10 UK-based cases involving financially moti- vated cybercrime. Many of these studies, including Hock et al. (2025), Lusthaus et al. (2023), Garba, Lazarus, and Button (2024), Leukfeldt and Holt (2019), and Soares and Lazarus (2024), underline the reliability of case file data in criminological research. Case files provide structured, verifiable, and judicially vetted insights into offender profiles, criminal methodologies, and legal responses, making them a valuable resource for empirical analysis. By drawing on this established methodological approach, the present study reinforces the

credibility of case file analysis as a valuable tool for examining cybercrime in Nigeria. This study narrows its scope to 100 convicted individuals engaged in romance scams within a specific timeframe and jurisdiction, offering a robust dataset for analysis.

Limitations

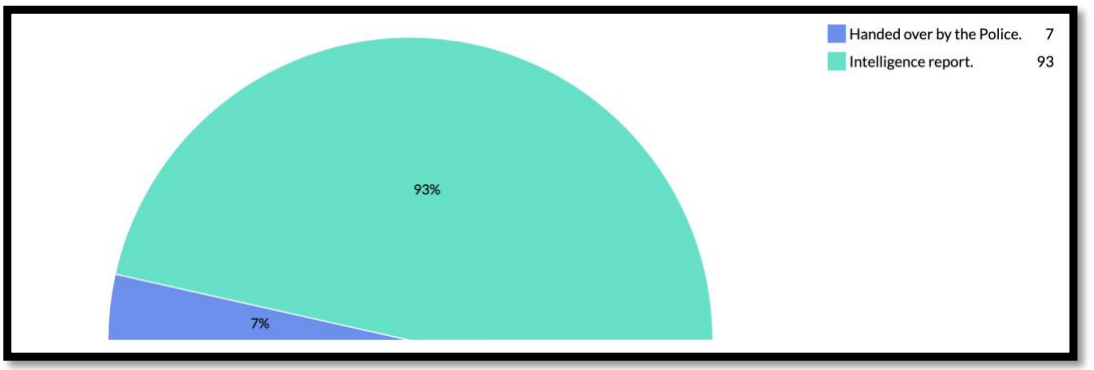
While this methodology provides valuable insights into romance scam offenders, it is constrained by its focus on convicted individuals, who may not fully represent the broader cybercriminal population. Consequently, these findings should be interpreted as a snapshot of romance scams in Nigeria, contributing empirical data to an understudied domain of cybercrime. Key findings are presented below.

5. Results

The data analysed in this study were derived from examining official case files pertaining to one hundred convicted cyber fraudsters prosecuted by the Economic and Financial Crimes Commission (EFCC) in Nigeria between 2021 and 2023.

Figure 1 illustrates that the EFCC apprehended 93% of these convicted cyber fraudsters through intelligence-driven operations, while the remaining 7% were transferred to the EFCC for prosecution by the Nigerian police. Within these case files, 93 intelligence reports and 7 Nigerian police handover notes were documented, providing crucial insights into the investigative and prosecutorial processes surrounding cyber fraud cases handled by the EFCC during the specified timeframe.

Figure 1: - ***Mode of apprehension.***



The perpetrators engaged in a variety of cybercrimes, as depicted in Table 2, which include cyber-impersonation, romance scams, cryptocurrency scams, investment fraud, and credit card fraud. Significantly, romance scams and cyber impersonation constituted the largest share at 75%, with cryptocurrency investment scams and impersonation trailing behind at 15%. A more crucial issue is that 80% of the offences were linked to romance scams. Additionally, investment scams, hacking, advance fee fraud, and credit card fraud with impersonation collectively comprised 10% of the offences. Notably, the offenders employed social media platforms such as Facebook and Instagram to impersonate individuals before perpetrating romance scams or other fraudulent activities.

Table 2: - Types of Scams

TYPE OF SCAMS	COUNT
Crypto Investment Scams	2
Advance Fee Fraud, and Cyber Impersonation	1
Investment Scam, Romance Scams and Cyber Impersonation	2
Cyber impersonation	1
Hacking and Cyber Impersonation	1
Romance scams, Crypto Investment Scam and Cyber Impersonation	1
Crypto Investment Scam, & Cyber Impersonation	15
Romance scams, Crypto Scam, and Cyber Impersonation	1
Romance Scams, Credit Card Fraud and Cyber Impersonation	1
Romance Scam, & Cyber Impersonation	75
Grand Total	100

Table 3 presents the motivations behind offenders' engagement in cybercrime. Analysis of investigation reports and offender statement sheets revealed that 56% of offenders were primarily motivated by greed, which manifested in extravagant spending on luxury items and social activities such as iPhones and parties.

Table 3:- Cybercrime Motivations

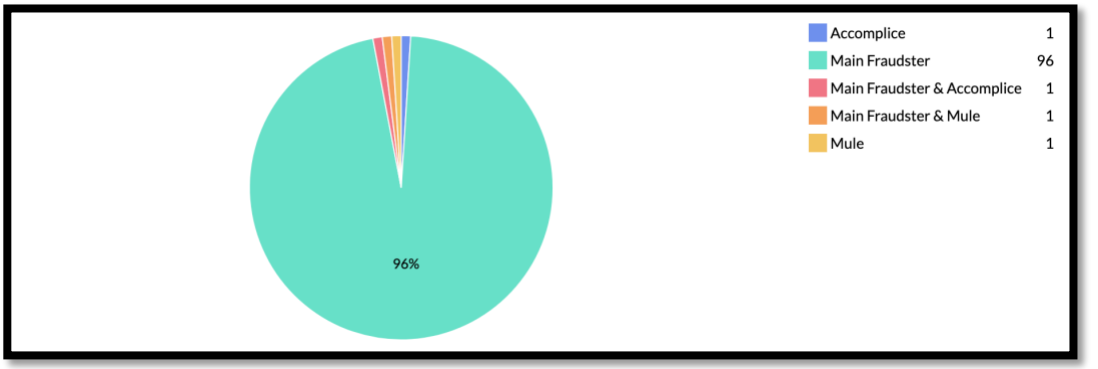
MOTIVATION OF OFFENDER	COUNT
Economic Hardship	1
Family Pressure	1
Financial Strain & Greed	30
Financial Strain & Peer Pressure	3
Financial Strain, Peer Pressure & Greed	3
Frustration, Financial Strain & Greed	1
Greed	56
Peer Pressure	1
Peer Pressure & Greed	3
Poverty/Economic hardship	1
Grand Total	**100**

A further 30% of offenders were also driven by greed but directed their illicit gains towards maintaining a lavish lifestyle and providing financial support to their families. In contrast, 4% cited financial strain and pressure as their primary motivator, while a combination of peer pressure and greed influenced 3%. Similarly, another 3% reported being motivated by financial strain, greed, and external pressures. Additionally, 4% of offenders attributed their involvement in cybercrime to a mix of poverty, economic hardship, peer pressure, and familial obligations.

Those influenced by family and peer pressure often cited association with criminal-minded acquaintances and an inability to meet basic needs, such as rent payments, as reasons for their criminal behaviour. Conversely, economically disadvantaged offenders frequently cited unemployment as the driving force behind their involvement in cybercrime, highlighting the complex interplay of individual, social, and economic factors influencing offenders' decisions to engage in illicit behaviour.

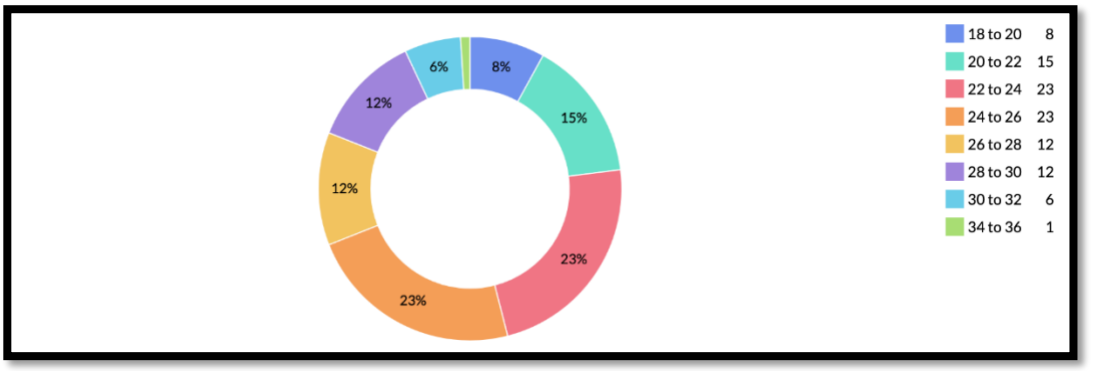
In Figure 2, 96% of offenders assumed the role of the primary fraudster in their schemes, while 2% acted as mules or accomplices, and an additional 2% played both roles concurrently. Analysis of fraudulent communications with victims, investigation reports, and offender statements indicated that 98% of offenders were directly implicated in cybercrime, engaging directly with their victims. These findings underline the significant involvement of offenders in perpetrating cybercrimes and highlight their active participation in fraudulent activities, as evidenced by their direct interactions with victims.

Figure 2: - ***Role of the offenders in the schemes***



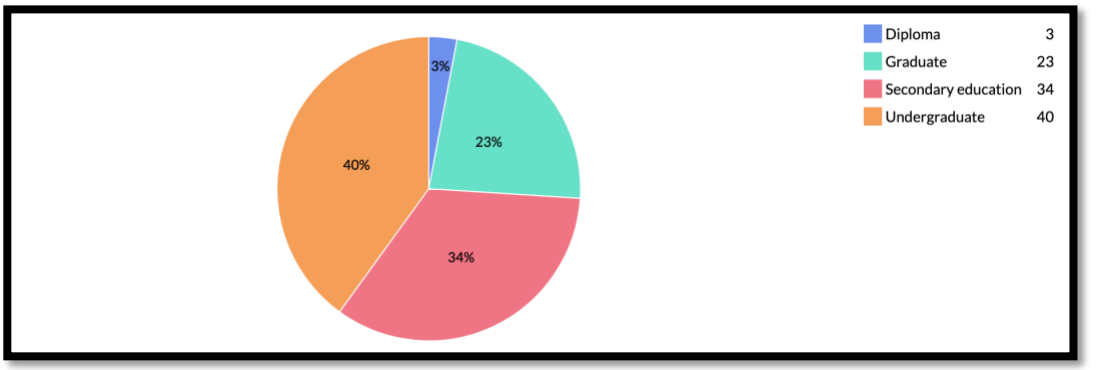
In Figure 3, the average age of offenders is depicted. Analysis of investigation reports, offenders' statements, and bank account opening documents revealed that 46% of offenders fall within the age range of 18 to 23, while 39% are aged between 23 and 28. Only 1% of offenders were aged 34, with 14% falling within the age bracket of 28 to 33. Based on these data, the median age of offenders is determined to be 24 years. The results of this study offer essential information about the age range of online offenders, showing that most offenders are in their early to mid-twenties. The age distribution of cyber criminals is vital in tailoring preventive measures to specific age groups.

Figure 3: - ***Age of the offenders***



The results, as encapsulated in Figure 4, show the educational attainment patterns of online scammers, and 100% of them are men. Among these individuals, 63% were either undergraduates or graduates, 3% held a diploma, and 34% had completed only secondary education.

Figure 4: - ***Offenders' level of education***

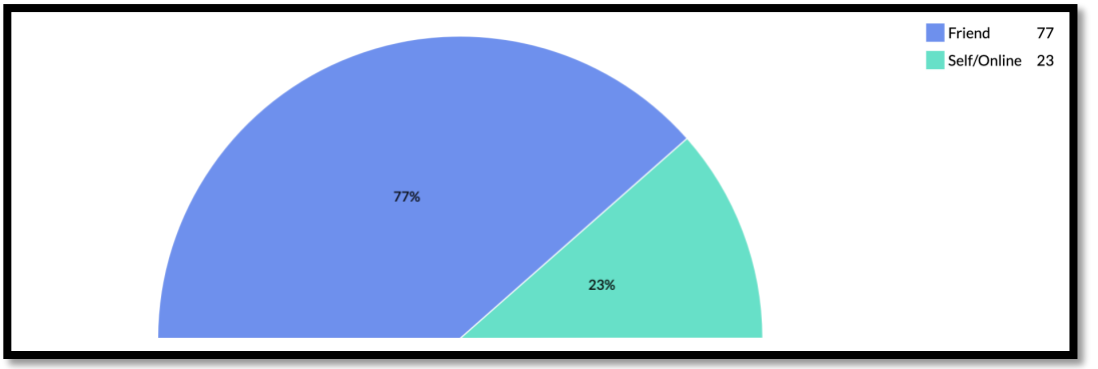


The data indicates that 96% of offenders originated from the southern region of Nigeria, with the South-South contributing 50% and the South-East accounting for 43%. Within the South-South, Akwa Ibom represented the highest proportion at 22%, followed by Cross River (13%), Delta (9%), Bayelsa (3%), Rivers (1%), and Edo (1%). In the South-East, Imo led with 16%, followed by Abia (14%), Anambra (8%), Ebonyi (3%), and Enugu (2%). The South-West contributed 3% of offenders, including Lagos (2%), Oyo (1%), and Ondo (1%). The remaining 4% came from the North-Central region, specifically Benue. This data underscores a significant concentration of offenders in southern Nigeria, particularly in the South-South and South-East regions. These findings highlight the predominance of southern male youths among cyber fraudsters and draw

attention to the relatively high levels of educational attainment within this demographic group.

Furthermore, Figure 5 illustrates the modes through which cybercriminals acquire their skills. Analysis revealed that 77% of offenders learned cybercrime methods through interpersonal interactions, predominantly from friends and other close contacts, while 23% acquired knowledge from online sources. The narratives provided by the offenders in their statement sheets elucidated their initiation into cybercriminal activities.

Figure 5:- Mode of Learning Cybercrime as Offenders



Moreover, Figure 6 delineates the channels cybercriminals utilise to receive illicit proceeds. Findings indicate a predominant reliance on anonymised payment channels, notably Bitcoin wallets and gift cards. Analysis of the offenders' financial transactions, including Bitcoin, cash app, gift cards, and bank records, revealed that 27% employed Bitcoin and an equivalent percentage utilised gift cards. A mere 1% of offenders resorted to Cashapp, while 14% opted for local bank transactions. Interestingly, 31% of cybercriminals did not disclose their chosen method of receiving proceeds.

Figure 6: - Mode of Receiving Cybercrime Proceeds

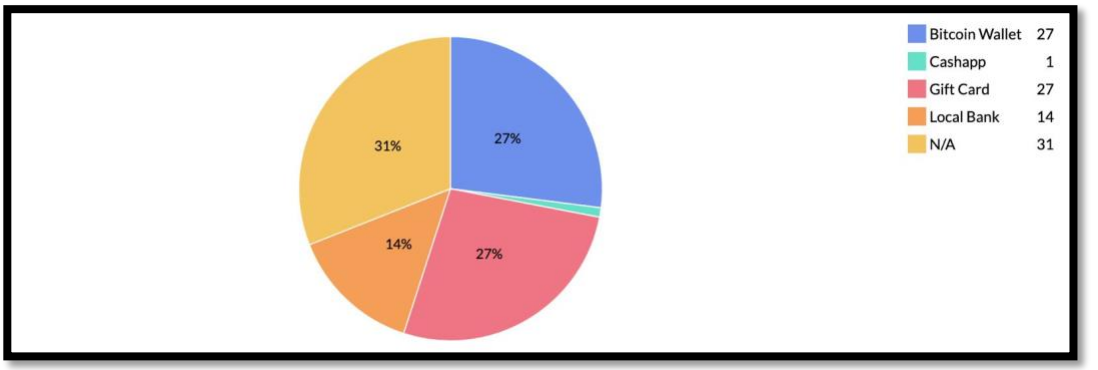


Table 4 also provides an overview of offenders' post-conviction punishments. Analysis of conviction warrants and court orders revealed that 64% of offenders received prison sentences ranging from three to eighteen months, with the option of fines ranging from =N=10,000 to

=N=2,000,000. The remaining 36% of offenders received varying prison terms without fines.

Specifically, the data on punishments with the option of fines highlights the following distribution among 64 offenders:

- The majority of sentences included six months' imprisonment with varying fine options. Among these, fines of **₦500,000** were the most common, applied in **11 cases,** followed by fines of **₦100,000** in **9 cases, ₦200,000** in **8 cases, ₦300,000** in **7 cases,** and **₦10,000** in **6 cases.**
- A smaller number of offenders received three months' imprisonment, with fines ranging from **₦50,000** to **₦300,000,** including **₦100,000** in **3 cases,** and **₦150,000, ₦300,000,** and **₦50,000,** each in **1 case.**
- One-year imprisonment sentences were associated with higher fines, including **₦800,000** (2 cases), **₦500,000** (2 cases), **₦700,000** (1 case), and **₦300,000** (1 case).
- Additional sentences included **nine months' imprisonment with a fine of ₦2,000,000, eighteen months' imprisonment with a fine of ₦250,000,** and **five months' imprisonment with a fine of ₦500,000**, each applied in **1 case.**
- Notably, there were multiple instances where six months' imprisonment included fine options below **₦100,000,** with fines as low as **₦50,000** recorded in **1 case** each.

This data reflects significant variability in the fines attached to imprisonment sentences, with six months' imprisonment being the most frequently imposed duration. Fine amounts show a wide range, suggesting flexibility in the punishment structure depending on the severity of the offense or judicial discretion.

Whether accompanied by a fine or not, the median sentence was determined to be six months, as depicted in Table 4. These findings shed light on the judicial outcomes faced by convicted cyber fraudsters and highlight the range of penalties imposed by the legal system.

Table 4: - ***Punishment without the option of fine***

PUNISHMENT OF OFFENDER (WITHOUT OPTION OF FINE)	**COUNT**
Six Months Imprisonment	12
One Year Imprisonment	8
One Month Imprisonment	7
Three Months Imprisonment	4
Two Months Imprisonment	2

Four Months Imprisonment	2
Two Years Imprisonment	1
GRAND TOTAL	**36**

Also, interestingly, results show that all offenders (n=100) had parents and guardians who were unaware of the existence of cybercrime perpetration. Examination of bail documents and casefile diaries revealed that none of the offenders' parents or guardians knew of their involvement in cybercrime activities before their arrests and subsequent prosecution. Throughout the month-long investigation and prosecution, the offenders deliberately chose not to disclose their cybercrime arrest to their parents or guardians. Instead, they sought assistance from friends, classmates, and girlfriends to secure bail and obtain legal representation. These findings underline the lack of parental involvement and awareness regarding their children's engagement in cybercriminal activities.

6. Discussion

Core findings and comparison with prior studies

Cybercrime sentencing and realities

This section focuses on the key findings outlined in Table 5. Criminal justice systems are responsible for administering punishment to offenders, enacting criminal laws, investigating, prosecuting, and punishing (e.g., Olonisakin, Ogunleye, and Adebayo 2017). Our statistical findings reveal that 64% of offenders received sentences ranging from 3 to 18 months between 2021 and early 2023, with the option of paying fines instead of imprisonment. Despite significant convictions for cybercrime-related offenses by the EFCC, lenient sentencing persists, exemplified by the case file E.A.E. in this study, who received a minimal four-month sentence in both 2021 and 2022. Although there has been an increase in cybercrime arrests and incidents (e.g. Economic and Financial Crimes Commission 2023a, 2023b, 2023c), Nigerian courts persist in imposing lenient sentences on offenders. This leniency appears ineffective given the escalating cybercrime rates in Nigeria, thus indirectly exacerbating the issue. The concept of recidivism, emphasized in this study, underlines the necessity of appropriate punishment to deter both present and future offenders (cf. Andrews 1989; Latessa and Lowenkamp 2006). Although punishment does not invariably deter crime (Lazarus, Button, and Adogame 2022), adequate imprisonment for cybercriminals is often proposed as a means to mitigate cybercrime in Nigeria.

However, this view is overly simplistic. The boundaries between offenders, so-called Yahoo Boys, and some representatives of authority are increasingly blurred (Lazarus, Button, and Adogame 2022; Lazarus 2023). "In West Africa, the collaboration between cyber fraudsters and certain government representatives in financial crimes blurs traditional boundaries, fostering an environment conducive to the unrestricted practice of money laundering and fraud" (Lazarus 2024: 472). Both Yahoo Boys and politicians ("Yahoo Men") demonstrate overlapping expertise in bribery, corruption, and fraud, according to research (Lazarus 2024; Lazarus, Button and Adogame 2022). While Yahoo Boys primarily target victims outside Nigeria through internet scams, politicians routinely embezzle public funds domestically. As Lazarus (2023) and Lazarus, Button and Adogame (2022) note, the convergence of deviant tactics among these actors complicates the assumption that imprisonment alone will meaningfully reduce cybercrime.

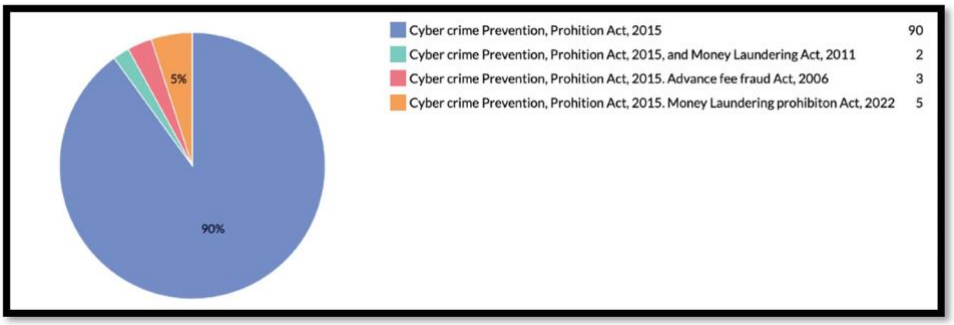


Figure 7. **Penal laws used to prosecute the offenders.**

Moreover, the physical versus cyberspace theme concerning repressed criminal behavior, as out- lined in Table 1, is particularly relevant to the Space Transition Theory, developed by Jaishankar (2007) and (2008). Space Transition Theory suggests that online crimes may be perceived as less tangible or harmful, leading to more lenient sentencing. The authors should emphasize this in the discussion, as it reinforces the theory's relevance in explaining both criminal behavior and judicial responses to offenses committed in different spaces.

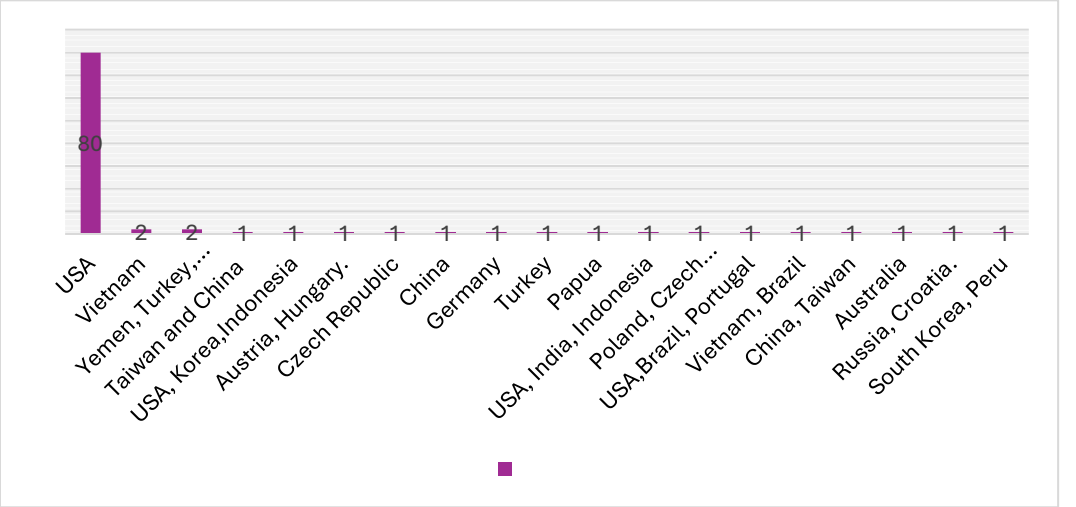
For instance, the disparity between lenient sentencing for cybercrimes and harsher penalties for physical offenses illustrates how spatial context influences legal decisions. This perspective could serve as a basis for future research on the relationship between cyberspace, crime perception, and judicial outcomes. The notion that offenders may commit crimes in cyberspace that they would not undertake in the physical world aligns with the idea that cybercrimes are often viewed as less concrete, affecting judicial leniency in sentencing. Additionally, the conflict of norms and values theme is pertinent, as it addresses how differences between physical and virtual spaces shape legal and moral perceptions. The contrast between harsher penalties for physical offenses and more lenient sentencing for cybercrimes underscores how these norm clashes shape judicial responses. These aspects provide a robust foundation for future research on how cyberspace influences crime perception, sentencing practices, and legal frameworks.

Furthermore, the ineffectiveness of current sentencing strategies is evident, raising concerns about their impact on future cybercrime rates (Eboibi 2017, 2022; Eboibi and Ogorugba 2023). The Cybercrime (Prohibition, Prevention, etc.) Act of 2015 was enacted in Nigeria to address the increasing incidence of cybercrime by establishing legal frameworks for prevention and prosecution (Eboibi 2017; Eboibi and Ogorugba 2023; Izevbuwa and Ngwoke 2022). However, prosecution rates under this Act remain low, highlighting the need for more effective legal measures. Notably, the Act was applied in 90% of the cases examined in this study (see Figure 7), yet its sentencing approach appears inadequate, raising questions about its deterrent effect and the broader efficacy of Nigeria's cybercrime legislation.

The limited media coverage of cybercrime in Nigeria Television stations may contribute to weak sentencing and enforcement, as public discourse and awareness often shape legal responses. Grant and Buil-Gil (2025) demonstrate that romance fraud documentaries shape public perceptions by increasing awareness and influencing attitudes. Greater awareness encourages victims to seek help and report offenses to the police. A rise in reporting can, in turn, impact legal responses and contribute to variations in sentencing severity.

Despite stipulating a five-year prison term for identity theft, none of the offenders in this study received the maximum penalty, undermining the Act's deterrent effect. Regarding lenient sentencing in Nigeria, other West African nations, such as Ghana, have even more permissive legal frameworks. Lazarus et al. (2025) indicate that Nigerian cybercriminals frequently operate in Ghana, taking advantage of lighter sentencing, weaker enforcement mechanisms, and legal loopholes. Unlike Nigeria, where the Economic and Financial Crimes Commission (EFCC) leads cybercrime enforcement (Lazarus and Okolorie 2019; Orji, 2019), Ghana's cybercrime task force remains in a developmental phase, making enforcement less stringent (Abubakari and Blaszczyk 2023; Torsu, 2024).

Figure 8. **Countries of cybercrime victims**



This discrepancy has contributed to the migration of Nigerian fraudsters to Ghana, reinforcing the jurisdictional adaptability of cybercriminals. For instance, one law enforcement officer interviewed by Lazarus et al. (2025: 4) stated:

> Several factors contribute to the migration of Internet fraudsters from Nigeria to Ghana. One is the fear of prosecution and forfeiture of criminal proceeds to the Nigerian government. Two, the fear of local anti-corruption agencies publishing their pictures on social media. Three, using Bank Verification Numbers in Nigeria, which links accounts to cybercriminals, makes local banks unattractive. They prefer to conduct transactions elsewhere. I believe too that the lack of a government database in Ghana is a factor, giving them almost a ghost-like status.

Although empirical data directly comparing Ghanaian and Nigerian sentencing patterns remains limited, Lazarus et al. (2025) suggest that sentencing in Ghana is generally less severe. Cybercrime laws in Ghana are still evolving, and enforcement remains inconsistent. EFCC officers in Nigeria have also highlighted the difficulties in extraditing offenders from Ghana, further complicating cross-border cybercrime prosecution.

In contrast, the American criminal justice system demonstrates a firmer stance, imposing harsher penalties and disallowing fines instead of jail time (e.g., Busari 2023; Essien 2022; Johnson 2023; Oluwafemi 2023). As shown in Figure 8, our study demonstrated that 80% of online offenders in Nigeria targeted United States residents, potentially subjecting them to extradition and prosecution by the United States. The predominance of United States citizens as victims of online scams originating from Nigeria, accounting for 80% of cases, as shown in the figure "*Countries of Cybercrime Victims*," is consistent with findings from prior studies on romance fraud. For example, Edwards et al. (2018) quantitative analysis of dating profiles, Soares and Lazarus's (2024) qualitative examination of convicted romance scammers, and Abubakari's (2024) interviews with active scammers collectively reveal that offenders frequently pose as nationals from Western countries, such as the United States, where online dating activity is high.

Lazarus et al. (2023b) and Abubakari (2024) further demonstrated that romance fraudsters believe that adopting non-Western identities reduces their chances of eliciting responses. From the perspectives of online romance fraudsters, any potential "clients" (victims), typically Western users, may be reluctant to engage with individuals from Africa south of the Sahara due to longstanding racial prejudices, particularly against accepting West Africans as romantic partners within their social or cultural communities.

By extension, the predominance of United States citizens as victims of online scams originating from Nigeria, accounting for 80% of cases, aligns with findings from prior media reports (Essien 2022; Johnson 2023; Oluwafemi 2023) and scholarly research. For instance, Soares and Lazarus (2024) found that 56% of dating fraud targeting United States citizens was perpetrated by offenders operating from Nigeria. This pattern is also evident in other forms of online fraud. For example, Garba, Lazarus, and Button (2024) found that 55% of cryptocurrency fraud targeting United States citizens was perpetrated by fraudsters operating from Nigeria.

Furthermore, this study's finding refutes claims from some researchers (Akanle, Adesina, and Akarah 2016; Bello and Griffiths 2021; Tade 2021) attributing the surge in cybercrime in Nigeria to law enforcement agencies, suggesting a robust intelligence system that supports proactive policing and contributes to crime reduction policies. Predominantly, arrests, investigations, and convictions were intelligence-led, showcasing the effectiveness of Nigerian law enforcement agencies like the EFCC in combating cybercrime, according to 100 cases we studied. Having discussed offenders' sentencing and their preference for Western victims, we now focus on gender and the predominance of romance fraud.

Romance fraud: offenders and gender

In examining the demographic characteristics of individuals involved in cybercrime, it is noteworthy that 80% are implicated in romance scams, as outlined in Table 5. This is consistent with previous research on digital crimes in Nigeria, which highlights online romance scams as one of the main forms of cybercrime perpetrated by Nigerian internet scammers, both within and outside of Nigeria (Aborisade, Ocheja, and Okuneye 2024; Soares and Lazarus 2024). These scammers (Yahoo Boys) defraud victims globally.

Our findings also corroborate previous empirical studies that have observed a connection between romance fraud and other economic cybercrime topics, such as the migration of fraudsters from Nigeria to Ghana (Lazarus et al. 2025) and deviant website developers who create fraudulent platforms for pet scammers in Cameroon (Whittaker, McGuire, and Lazarus 2025). Furthermore, our research reveals that all convicted fraudsters in these cases are male, comprising 100% of the convicted population. This observed gender trend aligns with earlier findings on cybercriminals in Nigeria, as evidenced by multiple data sources, such as interviews with offenders (Aransiola and Asindemade 2011), narratives from Economic and Financial Commissions operatives (Lazarus and Okolorie 2019), examinations of convicted cryptocurrency offenders (Garba, Lazarus, and Button 2024), assessment of song lyrics (Lazarus 2018; Lazarus et al. 2023a), and interviews with offenders' parents (Aborisade 2022, 2023; Ibrahim 2017).

These studies frequently emphasize the involvement of university students, graduates, and dropouts, particularly those aged 18 to 34 years, in cybercriminal activities (Aransiola and Asindemade 2011; Garba, Lazarus, and Button 2024; Lazarus and Okolorie 2019; Soares and Lazarus 2024). The predominance of male perpetrators reflects familial and cultural influences that shape gender roles in Nigerian society. Men are traditionally socialized to be the primary providers and heads of households in West Africa (Ibrahim 2015; Rush and Lazarus 2018; Skinner et al. 2024; Tuki 2024), with some involved in polygamous marriages. These cultural norms place heightened pressure on men to achieve financial success, often more so than on women (Ibrahim 2016; Skinner et al. 2024; Tuki 2024), potentially pushing them toward cybercrime as a means of fulfilling societal expectations. Having discussed the gendered aspect of offending, we now analyze regional differences in the production of cybercrime across various parts of Nigeria.

North-south divide among offenders

In addition to the gender dimension, our study uncovered a significant pattern: 96% of cybercrime offenders originate from southern Nigeria. In contrast, we only traced a few offenders back to the north-central region (n = 4) and none from the northern region, as shown in Table 5. This geographical distribution of offenders prompts the need for deeper investigation. The observed "North- South" contrast echoes findings from prior research, such as the analysis of Lazarus and Button (2022: 504-508) on over 100,000 tweets and the study by Lazarus et al. (2023a: 13-14) examining 33 songs. However, it is crucial to exercise caution in interpreting this aspect of our findings. While online offenders can operate from any location, the lead researcher obtained the case files directly from a zonal office situated in southern Nigeria. This suggests a potential influence of the research study's location on the distribution of offenders captured in our analysis. Additionally, some may argue that analyzing a sample of only 100 case files may not yield definitive conclusions. Nevertheless, the north- south trend in cybercrime production and prosecution we found in this study warrants further exploration to gain deeper insights into "the geographies of cybercrime" (cf. Hall and Yarwood 2024; Hall et al. 2021; Lazarus and Button 2022). Furthermore, we invite a more profound exploration through the lens of Space Transition Theory.

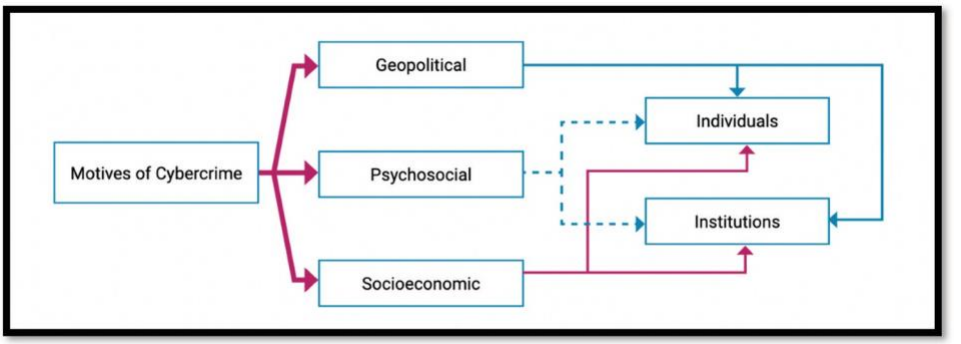


Figure 9. The socioeconomic classification. Source: Adapted from Auwal and Lazarus (2024: 919).

Core findings and theoretical implications

Space Transition Theory posits that individuals may exhibit different behaviors in cyberspace com- pared to physical space. However, the Nigerian cybercrime landscape shows a significant gender imbalance, with men aged between 18–28 being more involved than other demographics, implicating this subgroup more significantly. This gender-specific trend contradicts a facet of Jaishankar's (2008) theory, which suggests that those who do not exhibit criminal tendencies in physical space might engage in fraudulent activities in the relatively anonymous cyberspace. In the Nigerian context, men, rather than women, show a higher propensity for offending, challenging this theoretical postulation. Additionally, this observation aligns with another aspect of the Space Transition Theory, asserting that criminal behavior in cyberspace may influence physical space and vice versa. This highlights the interconnectedness of these spaces, introducing a nuanced dimension to the discourse on the theory's applicability. While the demographic findings deviate from some aspects of Jaishankar's (2008) theory, they highlight the complex "marriage" between cyberspace and physical space, suggesting that

a nuanced dataset and evaluation are required to (dis)agree with the theory.

Transitioning to examining methods and platforms employed for cryptocurrency fraud, the Space Transition Theory's emphasis on identity flexibility and dissociative anonymity in cyberspace finds resonance in the study's findings. This theoretical perspective posits that these characteristics are pivotal in influencing criminal behavior within the digital realm. The current study aligns with this viewpoint, revealing the prominence of various online platforms, particularly social media giants like Facebook, Instagram, Telegram, and Hangout, in facilitating cryptocurrency fraud. The utilization of platforms such as Facebook, Instagram, Telegram, and Hangout reflects the theoretical propositions of the Space Transition Theory (Jaishankar 2007; 2008), wherein the flexibility and anonymity inherent in these online spaces are seen as conducive to criminal activities. Offenders may leverage the dynamic nature of cyberspace and intermittent ventures to evade the consequences of their actions. In this context, the study's findings affirm the theory's relevance, showcasing how fraudsters exploit the identity flexibility and dissociative anonymity provided by platforms like Facebook, Instagram, Telegram, and Hangout to engage in cryptocurrency fraud while navigating the intricacies of the digital landscape.

Exploring the financial dimensions of fraud, the Space Transition Theory, while not explicitly addressing financial motivations, highlights the dynamic nature of cyberspace as a facilitator of criminal activities. However, while the theory remains silent on direct financial incentives, this study's findings reveal that individuals exploit cyberspace's fluid environment to achieve substantial financial gains, an aspect not fully captured by the explanatory lens of Space Transition Theory, developed in 2007 and 2008. This limitation exposes the evolving nature of internet-facilitated crimes over close to two decades, emphasizing the need for theoretical updates that better reflect these shifting dynamics.

To address these gaps, our findings highlight the significance of the Tripartite Cybercrime Framework (TCF) (Ibrahim 2016). The TCF (a) provides a valuable view by categorizing cybercrime motivations into three distinct dimensions and (b) posits that socioeconomic cybercrime, including romance scams, advance fee fraud, and similar offenses, constitutes the most prevalent and relevant category in the Nigerian context (as far as "Yahoo Boys" are concerned), unlike cyber espionage (geopolitical cybercrime) and cyberbullying (psychosocial). Aligning with prior empirical research (e.g., Garba, Lazarus, and Button 2024; Hall and Ziemer 2024) and non-empirical papers (e.g., Lazarus, Tickner, and McGuire, 2024 Hall and Ziemer 2023), this study builds on the Tripartite Cybercrime Framework (TCF). We demonstrate that the cybercrime types examined here primarily fall within the framework's socioeconomic classification, as illustrated in Figure 9.

This framework emphasizes the prevalence and perpetration of cybercrime within the socioeconomic category, particularly among Nigerians both domestically and internationally (Ibrahim 2016). It stresses the critical importance of understanding diverse cybercrime motivations and their broader societal implications. Focusing specifically on fraud-related motivations, this study offers a more detailed exploration of the socioeconomic drivers of cybercrime. Simultaneously, it acknowledges the role of individual agencies in the decision to engage in these activities, providing a nuanced perspective on the interplay between structural factors and personal choices in cybercrime participation.

7. Conclusion

The research has explored the interconnectedness of physical and digital spaces, emphasizing the transferability of criminal behaviors, and has various implications and values. This study examined key demographic, operational, and geographical observations regarding Nigerian cybercriminals engaged in romance scams, offering broader implications for both policy and practice. While most offenders are young males aged 18–28 who target Western victims, particularly in the United States, their choice of geographical base in southern Nigeria highlights the interplay of socio-cultural and structural factors in shaping cybercriminal operations. Although these observations support prior research, they also challenge certain elements of the Space Transition Theory by emphasizing Nigeria's distinctive socioeconomic and cultural setting.

The overwhelming proportion of U.S. victims (80% of cases) resonates with earlier studies, including Soares and Lazarus (2024) and Abubakari (2024). The tendency of offenders to adopt Western identities in response to perceived biases against West Africans exemplifies how cultural preconceptions profoundly influence fraudulent tactics. These dynamics hint at a broader pattern, wherein cybercriminals tailor their methods to circumvent prejudicial barriers and thereby maximize victim compliance.

The research evaluates the Nigerian Cybercrime Act of 2015 and highlights persistent gaps in sentencing practices. Although the Economic and Financial Crimes Commission (EFCC) strives to curb cyber offenses, lenient penalties embolden repeat offenders. Comparing these outcomes with the comparatively strict U.S. criminal justice model accentuates the urgent need to recalibrate Nigeria's legal and punitive frameworks to strengthen deterrence. The findings also reinforce the Tripartite Cybercrime Framework (TCF), emphasizing that socioeconomic stressors are primary motivators for cyber-offenses in Nigeria.

By integrating the Tripartite Cybercrime Framework (TCF), this study underscores how deep-rooted economic disparities and limited job opportunities compound the lure of cyber-fraud. Insights generated here can guide policymakers in developing culturally informed interventions, ranging from community-level economic empowerment to stringent enforcement protocols. Effective strategies to address cybercrime in Nigeria require a holistic approach. Revised sentencing guidelines, backed by consistent enforcement, could bolster deterrence. Building capacity among law enforcement through training in digital forensics, intelligence gathering, and cross- border cooperation would further address operational gaps. Future research might investigate regional distinctions in cybercrime across Nigeria and Africa south of the Sahara to assess how factors such as local governance, internet penetration, and cultural norms affect both offender behavior and victim profiles.

Additionally, ongoing technological advancements call for studying how shifting online environments could alter the methods and motivations of cybercriminals. Certainly, this study provides a meaningful foundation for evidence-based strategies in Nigeria and beyond by exploring socio economic drivers, legal responses, and cross-cultural dimensions. Bridging identified policy gaps and strengthening institutional capacities contribute to the global fight against cybercrime and pave the way for more equitable and sustainable socioeconomic development.

Future research directions

To further enhance these efforts, future research should explore the socioeconomic and psychological factors driving cybercriminal activity in greater depth. Expanding the scope to examine regional and international cybercriminal migration patterns is also crucial. A key area of focus should be offender movements between Nigeria and neighboring countries, which could provide valuable insights into how cybercriminals adapt to jurisdictional differences to sustain their operations. Lazarus et al. (2025) examined this phenomenon, highlighting how legal and enforcement discrepancies influence cyber- criminal behavior.

While this study represents a collaboration between law enforcement officers and academics, such partnerships remain rare in Africa south of the Sahara. Expanding and institutionalizing these efforts is essential for strengthening cybercrime prevention, investigation, and policy development. Research collaborations, such as those by Lazarus and Okolorie (2019) and Garba, Lazarus, and Button (2024), provide valuable models. However, sustained efforts are needed to bridge the gap between academic insights and practical enforcement strategies. This will foster deeper collaboration, greater impact, and more effective interventions that genuinely acknowledge the vulnerabilities of cybercrime victims and the challenges of cybercrime enforcement in practice.

Additionally, comparative studies on sentencing patterns and law enforcement strategies between Nigeria and other key cybercrime-affected countries, such as Ghana, Cameroon, and Côte d'Ivoire, would help assess the effectiveness of existing legal responses. Further research could also examine the long-term outcomes of convicted cybercriminals, including recidivism rates and post-conviction reintegration challenges. Integrating qualitative interviews with offenders, law enforcement officers, and other stakeholders would complement case file analysis, offering richer insights into offender motivations, decision-making processes, and adaptation strategies in response to evolving law enforcement efforts.

Author contributions

CRediT: **Adebayo Benedict Soares:** Conceptualization, Data curation, Formal analysis, Investigation, Writing – original draft; **Suleman Lazarus:** Conceptualization, Formal analysis, Investigation, Methodology, Supervision, Validation, Writing – original draft, Writing – review & editing; **Mark Button:** Conceptualization, Investigation, Supervision, Writing – original draft.

Mr Adebayo Benedict Soares – ***Economic and Financial Crimes Commission (EFCC)***

Dr Suleman Lazarus – ***London School of Economics and Political Science (LSE)***

Professor Mark Button – ***University of Portsmouth***

References

Aborisade, R. A. 2022. "Internet Scamming and the Techniques of Neutralization: Parents' Excuses and Justifications for children's Involvement in Online Dating Fraud in Nigeria." *International Annals of Criminology* 60(2):199–219. doi:10.1017/cri.2022.13.

Aborisade, R. A. 2023. "Yahoo Boys, Yahoo Parents? An Explorative and Qualitative Study of parents' Disposition Towards children's Involvement in Cybercrimes." *Deviant Behavior* 44(7):1102–20. doi:10.1080/01639625.2022. 2144779.

Aborisade, R. A., A. Ocheja, and B. A. Okuneye. 2024. "Emotional and Financial Costs of Online Dating Scam: A Phenomenological Narrative of the Experiences of Victims of Nigerian Romance Fraudsters." *Journal of Economic Criminology* 3:100044. doi:10.1016/j.jeconc.2023.100044.

Abubakari, Y. 2024. "Modelling the Modus Operandi of Online Romance Fraud: Perspectives of Online Romance Fraudsters." *Journal of Economic Criminology* 100112:1–13. doi:10.1016/j.jeconc.2024.100112.

Abubakari, Y. and M. Blaszczyk. 2023. "Politicization of Economic Cybercrime: Perceptions Among Ghanaian Facebook Users." *Deviant Behavior* 45(4):483–502. doi:10.1080/01639625.2023.2253487.

Abubakari, Yushawu. 2023. "The Espouse of Women in the Online Romance Fraud World: Role of Sociocultural Experiences and Digital Technologies." *Deviant Behavior* 45(5):708–35. doi:10.1080/01639625.2023.2263137.

Abubakari, Yushawu and Awurafua Amponsaa Amponsah. 2024. "Economic Cybercrime in the Diaspora: Case of Ghanaian Nationals in the USA." *Journal of Money Laundering Control* 28(1):15–29. doi:10.1108/JMLC-03-2024-0047.

Ajayi, T. M., O. A. Adesope, and I. O. Oso. 2024. "Yahooism to Ritualism: Ideological Motivations for Cyber Fraud in Selected Yoruba Films." *Southern African Linguistics and Applied Language Studies* 43(1):102–16. doi:10.2989/16073614.2024.2341708.

Akanle, O., J. O. Adesina, and E. P. Akarah. 2016. "Towards Human Dignity and the Internet: The Cybercrime (Yahoo Yahoo) Phenomenon in Nigeria." *African Journal of Science, Technology, Innovation & Development* 8(2):213–20. doi:10.1080/20421338.2016.1147209.

Alhassan, A. R. K. and A. Ridwan. 2023. "Identity Expression—The Case of 'Sakawa'boys in Ghana." *Human Arenas* 6 (2):242–63. doi:10.1007/s42087-021-00227-w.

Andrews, D. A. 1989. "Recidivism is Predictable and Can Be Influenced: Using Risk Assessments to Reduce Recidivism."

Forum on Corrections Research 1(2):11–18.

Anesa, P. 2020. "Lovextortion: Persuasion strategies in romance cybercrime." *Discourse, Context & Media* 35(100398):1–8. doi:10.1016/j.dcm.2020.100398

Appleton, J. V. and S. Cowley. 1997. "Analysing Clinical Practice Guidelines. A Method of Documentary Analysis." *Journal of Advanced Nursing* 25(5):1008–17. doi:10.1046/j.1365-2648.1997.19970251008.x.

Aransiola, J. O. and S. O. Asindemade. 2011. "Understanding Cybercrime Perpetrators and the Strategies They Employ in Nigeria." *Cyberpsychology, Behavior and Social Networking* 14(12):759–63. doi:10.1089/cyber.2010.0307.

Assarut, N., P. Bunaramrueang, and P. Kowpatanakit. 2019. "Clustering Cyberspace Population and the Tendency to Commit Cyber Crime: A Quantitative Application of Space Transition Theory." *International Journal of Cyber Criminology* 13(1):84–100.

Auwal, A.M., and S. Lazarus. 2024. "Sociological and Criminological Research of Victimization Issues: Preliminary Stage and New Sphere of Cybercrime Categorization." *Journal of Digital Technologies and Law* 2(4):915–942. doi:10.21202/ jdtl.2024.44.

Bello, M. and M. Griffiths. 2021. "Routine Activity Theory and Cybercrime Investigation in Nigeria: How Capable are Law Enforcement Agencies?" *Rethinking Cybercrime*, edited by T. Owen and J. Marshall. Cham: Palgrave Macmillan. doi:10.1007/978-3-030-55841-3_11.

Bilz, A., L. A. Shepherd, and G. I. Johnson. 2023. "Tainted Love: A Systematic Literature Review of Online Romance Scam Research." *Interacting with Computers* 35(6):773–88. doi:10.1093/iwc/iwad048.

Blackstone, A. 2019. *Social Research: Qualitative and Quantitative Methods*. Boston, MA: FlatWorld.

Bruce, M. J. Lusthaus, R. Kashyap, N. Phair, F. Varese. 2024. "Mapping the global geography of cybercrime with the World Cybercrime Index." *PLOS ONE* 19(4):e0297312. doi:10.1371/journal.pone.0297312

Busari, B. 2023. "Nigerian Bags Seven Yrs Imprisonment Over Multi-Million-Dollar Cybercrime in US." *The Vanguard* March 17. https://www.vanguardngr.com/2023/03/nigerian-bags-seven-yrs-imprisonment-over-multi-million- dollar-cybercrime-in-us/.

Button, M., D. Blackbourn, L. Sugiura, D. Shepherd, R. Kapend, and V. Wang. 2021. "From Feeling Like Rape to a Minor Inconvenience: Victims' Accounts of the Impact of Computer Misuse Crime in the United Kingdom." *Telematics and Informatics* 64:101675. doi:10.1016/j.tele.2021.101675.

Button, M., P. Gilmour, B. Hock, T. Jain, S. Jesperson, S. Lazarus, D. Pandey, and J. Sabia. 2024. *Scoping Study on Fraud Centres: Ghana, India and Nigeria*. ITAD. https://www.itad.com/knowledge-product/scoping-study-on-fraud- centres-ghana-india-and-nigeria/.

Carter, E. 2024. *The Language of Romance Crimes: Interactions of Love, Money, and Threat*. Cambridge: Cambridge University Press.

Cole, R. 2024. "A Qualitative Investigation of the Emotional, Physiological, Financial, and Legal Consequences of Online Romance Scams in the United States." *Journal of Economic Criminology* 100108:1–14. doi:10.1016/j.jeconc.2024. 100108.

Cretu-Adatte, C., J. W. Azi, O. Beaudet-Labrecque, H. Bunning, L. Brunoni, and R. Zbinden. 2024. "Unravelling the Organisation of Ivorian Cyberfraudsters: Criminal Networks or Organised Crime?" *Journal of Economic Criminology* 3:100056. doi:10.1016/j.jeconc.2024.100056.

Cross, C. and T. J. Holt. 2021. "The Use of Military Profiles in Romance Fraud Schemes." *Victims & Offenders* 16 (3):385–406. doi:10.1080/15564886.2020.1850582.
Cross, C. and T. J. Holt. 2023. "More Than Money: Examining the Potential Exposure of Romance Fraud Victims to Identity Crime." *Global Crime* 24(2):107–21. doi:10.1080/17440572.2023.2185607.
Cross, C. and M. Lee. 2022. "Exploring Fear of Crime for Those Targeted by Romance Fraud." *Victims & Offenders* 17 (5):735–55. doi:10.1080/15564886.2021.2018080.
Denscombe, M. 2017. *The Good Research Guide: For Small-Scale Social Research Projects [Ebook]*. London: McGraw-Hill Education.
Dickinson, T., F. Wang, and D. Maimon. 2023. "What Money Can Do: Examining the Effects of Rewards on Online Romance Fraudsters' Deceptive Strategies." *Deviant Behavior* 44(9):1386–400. doi:10.1080/01639625.2023.2197547. Drew, J. M., and J. Webster 2024. "The victimology of online fraud: A focus on romance fraud victimisation." *Journal of Economic Criminology*, 3:100053. doi:10.1016/j.jeconc.2024.100053
Eboibi, F. E. 2017. "Curtailing Cybercrime in Nigeria: Applicable Laws and Derivable Sources." *African Journal of Criminal Law and Jurisprudence* 2:14–31.
Eboibi, F. E. 2022. "Trivialising Penalty for Internet Fraud: Review of the Federal Republic of Nigeria Vs Aifuwa Courage Osasumwen." *International Review of Law and Jurisprudence* 4(3):69–73.
Eboibi, F. E. and O. M. Ogorugba. 2023. "Cybercrime Regulation and Nigerian Youths Increasing Involvement in Internet Fraud: Attacking the Roots Rather Than the Symptoms." *Journal of Legal, Ethical & Regulatory Issues* 26 (S2):1–17.
Economic and Financial Crimes Commission. 2023a. "Ex-Convict, 17 Others Convicted for Internet Fraud." Retrieved from https://www.efcc.gov.ng/efcc/news-and-information/news-release/9034-ex-convict-17-others-convicted-for- internet-fraud.
Economic and Financial Crimes Commission. 2023b. "EFCC Arrests 'Crossdresser', 32 Others for Alleged Internet Fraud in Lagos." Retrieved from https://www.efcc.gov.ng/efcc/news-and-information/news-release/9134-efcc-arrests -crossdresser-32-others-for-alleged-internet-fraud-in-lagos.
Economic and Financial Crimes Commission. 2023c. "EFCC Arrests 14 Internet Fraud Suspects in Port-Harcourt." Retrieved from https://www.efcc.gov.ng/efcc/news-and-information/news-release/9127-efcc-arrests-14-internet- fraud-suspects-in-port-harcourt.
Edwards, M., G. Suarez-Tangil, C. Peersman, G. Stringhini, A. Rashid, and M. Whitty. 2018. "The Geography of Online Dating Fraud." *Workshop on Technology and Consumer Protection: Co-Located with the 39th IEEE Symposium on Security and Privacy, (ConPro)*, May, San Francisco, CA, 1–7.
Essien, H. 2022. "Over Half of Nigerians in Our Prisons Jailed for Fraud: THE UNITED STATES Govt." *Peoples Gazette*. https://gazettengr.com/over-half-of-nigerians-in-our-prisons-jailed-for-fraud-u-s-govt/.
Garba, K. H., S. Lazarus, and M. Button. 2024. "An Assessment of Convicted Cryptocurrency Fraudsters." *Current Issues in Criminal Justice* 1–17. doi:10.1080/10345329.2024.2403294.
Grant, S. and D. Buil-Gil. 2025. "The Effect of True Crime Docuseries on Romance Fraud Reporting to the Police." *Crime Science* 14(1):1. doi:10.1186/s40163-025-00244-y.
Hall, T., B. Sanders, M. Bah, O. King, and E. Wigley. 2021. "Economic Geographies of the Illegal: The Multiscalar Production of Cybercrime." *Trends in Organized Crime* 24(2):282–307. doi:10.1007/s12117-020-09392-w
Hall, T., and R. Yarwood. 2024. "New Geographies of Crime? Cybercrime, Southern Criminology and Diversifying Research Agendas." *Progress in Human Geography* 48(4):437–57. doi:10.1177/03091325241246015.
Hall, T., and U. Ziemer. 2023. "Cybercrime in Commonwealth West Africa and the regional cyber-criminogenic framework." *The Commonwealth Cybercrime Journal* 1(1):5–27.
Hall, T. and U. Ziemer. 2024. "Online Deviance in Post-Soviet Space: Victimisation, Perceptions and Social Attitudes Amongst Young People, an Armenian Case Study." *Digital Geography and Society* 7:100096. doi:10.1016/j.diggeo. 2024.100096.
Han, B. and M. Button. 2025. "An Anatomy of 'Pig Butchering Scams': Chinese Victims' and Police Officers' Perspectives." *Deviant Behavior* :1–19. doi:10.1080/01639625.2025.2453821.
Herrera, L. and J. Hastings. 2024. "The Trajectory of Romance Scams in the U.S." *2024 12th International Symposium on Digital Forensics and Security (ISDFS)*, San Antonio, TX, USA, 1–6. doi:10.1109/ISDFS60797.2024.10527224.
Hock, B., H. Park, J. Oh, and M. Button. 2025. "The Profile and Detection of Bribery in South Korea." *Crime, Law, & Social Change* 83:1. doi:10.1007/s10611-025-10201-0.
Huang, J., G. Stringhini, and P. Yong. 2015. "Quit Playing Games with My Heart: Understanding Online Dating Scams." *Detection of Intrusions and Malware, and Vulnerability Assessment: 12th International Conference, DIMVA 2015, Milan, Italy, July 9–10, 2015, Proceedings 12* (Pp. 216-236), Springer International Publishing.
Ibrahim, S. 2015. "A Binary Model of Broken Home: Parental Death-Divorce Hypothesis of Male Juvenile Delinquency in Nigeria and Ghana." In *Contemporary Perspectives in Family Research*. Edited by Sheila Royo Maxwell and Sampson Lee Blair. New York: Emerald Group Publishing Limited, vol. 9, 311–40.
Ibrahim, S. 2016. "Social and Contextual Taxonomy of Cybercrime: Socioeconomic Theory of Nigerian Cybercriminals." *International Journal of Law, Crime and Justice* 47:44–57. doi:10.1016/j.ijlcj.2016.07.002.
Ibrahim, S. 2017. "Causes of socioeconomic cybercrime in Nigeria." Paper presented at IEEE International Conference on Cybercrime and Computer Forensic (ICCCF), Vancouver, BC, Canada; pp. 1–9.
Izevbuwa, O. G. and R. B. Ngwoke. 2022. "Combating the Menace of Cybercrime in Nigeria: A Review of the Cybercrime (Prohibition, Prevention Etc) Act 2015 and Other Legislations." *Journal of Law, Policy and Globalization* 119:1–17.
Jaishankar, K. 2007. Establishing a theory of cyber crimes. International journal of cyber criminology, 1(2):7–9.
Jaishankar, K. 2008. "Space Transition Theory of Cyber Crimes." Pp. 283–301 in *Crimes of the Internet*, edited by F. Schmallager& M. Pittaro. Upper Saddle River, NJ: Prentice Hall.
Jaishankar, K. 2018. "Cyber Criminology as an Academic Discipline: History, Contribution and Impact." *International Journal of Cyber Criminology* 12(1):1–8.

Johnson, H. 2023. "Nigerian Jailed for Four Years Over $1m Cyber-Fraud in US." *Punch*. https://punchng.com/nigerian-jailed-for-four-years-over-1mcyberfraudinus/#:~:text=A%20Nigerian%2C%20Solomon%20Ekunke%20Okpe,million%20in%20losses%20to%20victims.

Kopp, C., R. Layton, J. Sillitoe, and I. Gondal. 2015. "The Role of Love Stories in Romance Scams: A Qualitative Analysis of Fraudulent Profiles." *International Journal of Cyber Criminology* 9(2):205.

Latessa, E. J. and C. Lowenkamp. 2006. "What Works in Reducing Recidivism?" *University of St Thomas Law Journal* 3 (3):521–35.

Lazarus, S. 2018. "Birds of a Feather Flock Together: The Nigerian Cyber Fraudsters (Yahoo Boys) and Hip-Hop Artists." Criminology, Criminal Justice, Law & Society 19(2):63–80.

Lazarus, S. 2023. "Social media users compare internet fraudsters to Nigerian politicians." Africa at LSE. https://blogs.lse.ac.uk/africaatlse/2023/02/02/social-media-users-compare-internet-fraudsters-to-nigerian-politicians/

Lazarus, S. 2024. "Cybercriminal Networks and Operational Dynamics of Business Email Compromise (BEC) Scammers: Insights from the 'Black Axe Confraternity." *Deviant Behavior* 46(4):456–480. doi:10.1080/01639625. 2024.2352049

Lazarus, S. 2025. "Online romance scams: who Nigeria and Ghana's fraudsters are, how they operate, and why they do it." The Conversation https://theconversation.com/online-romance-scams-who-nigeria-and-ghanas-fraudsters-are- how-they-operate-and-why-they-do-it-247916

Lazarus, S. and M. Button. 2022. "Tweets and Reactions: Revealing the Geographies of Cybercrime Perpetrators and the North-South Divide." *Cyberpsychology, Behavior and Social Networking* 25(8):504–11. doi:10.1089/cyber.2021.0332. Lazarus, S., M. Button, and A. Adogame. 2022. "Advantageous Comparison: Using Twitter Responses to Understand Similarities Between Cybercriminals ("Yahoo Boys") and Politicians ("Yahoo Men")." *Heliyon* 8(11). doi:10.1016/j.heliyon.2022.e11142.

Lazarus, S., M. Button, K. H. Garba, A. B. Soares, and M. Hughes. 2025. "Strategic Business Movements? The Migration of Online Romance Fraudsters from Nigeria to Ghana." *Journal of Economic Criminology* 7:100128. doi:10.1016/j. jeconc.2025.100128.

Lazarus, S., M. Hughes, M. Button, and K. H. Garba. 2025. "Fraud as Legitimate Retribution for Colonial Injustice: Neutralization Techniques in Interviews with Police and Online Romance Fraud Offenders." *Deviant Behavior* :1–22. doi:10.1080/01639625.2024.2446328.

Lazarus, S. and G. U. Okolorie. 2019. "The Bifurcation of the Nigerian Cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) Agents." *Telematics and Informatics* 40:14–26. doi:10.1016/j.tele.2019.04.009. Lazarus, S., O. Olaigbe, A. Adeduntan, E. T. Dibiana, and G. U. Okolorie. 2023a. "Cheques or Dating Scams? Online Fraud Themes in Hip-Hop Songs Across Popular Music Apps." *Journal of Economic Criminology* 2:100033. doi:10.1016/j.jeconc.2023.100033.

Lazarus, S. and A. B. Soares. 2025. "From Business Centres to Hustle Kingdoms: Historical Perspectives on Innovative Models of Deviant Education." *International Annals of Criminology*, 1–20. doi:10.1017/cri.2025.1.

Lazarus, S., P. Tickner, and M. R. McGuire 2024. "Cybercrime against senior citizens: exploring ageism, ideal victim-hood, and the pivotal role of socioeconomics." *Security Journal*, 1–20. https://eprints.lse.ac.uk/123873/

Lazarus, S., J. M. Whittaker, M. R. McGuire, and L. Platt. 2023b. "What Do We Know About Online Romance Fraud Studies? A Systematic Review of the Empirical Literature (2000 to 2021)." *Journal of Economic Criminology* 100013. doi:10.1016/j.jeconc.2023.100013.

Lazarus, S. and L. Ziegler. 2024. *What is the Emotional Impact of Fraud?*. Lloyds Banking Group. https://www.lloydsbankinggroup.com/insights/what-is-the-emotional-impact-of-fraud.html.

Leukfeldt, E. R., and T. J. Holt. 2019. "Examining the Social Organization Practices of Cybercriminals in the Netherlands Online and Offline." *International Journal of Offender Therapy and Comparative Criminology* 64(5):522–538. https:// doi.org/10.1177/0306624X19895886 (Original work published 2020)

Leukfeldt, E. R., E. R. Kleemans, and W. P. Stol. 2017. "A typology of cybercriminal networks: from low-tech all-rounders to high-tech specialists." *Crime, Law and Social Change* 67:21–37.

Lusthaus, J., E. Kleemans, R. Leukfeldt, M. Levi, and T. Holt. 2023. "Cybercriminal networks in the UK and Beyond: Network structure, criminal cooperation and external interactions." *Trends in Organized Crime* 27:1–24. doi:10.1007/ s12117-022-09476-9

Modic, D., and R. Anderson. 2015. "It's all over but the crying: The emotional and financial impact of internet fraud."

IEEE Security & Privacy 13(5):99–103. doi:10.1109/MSP.2015.107

Ngo, F. and K. Jaishankar. 2017. "Special Article: Commemorating a Decade in Existence of the International Journal of Cyber Criminology: A Research Agenda to Advance the Scholarship on Cyber Crime." *International Journal of Cyber Criminology* 11(1):1–9.

Ogunleye, Y. O., U. A. Ojedokun, and A. A. Aderinto. 2019. "Pathways and Motivations for Cyber Fraud Involvement Among Female Undergraduates of Selected Universities in South-West Nigeria." *International Journal of Cyber Criminology* 13(2):309–325.

Ojedokun, U. A. and M. C. Eraye. 2012. "Socioeconomic Lifestyles of the Yahoo-Boys: A Study of Perceptions of University Students in Nigeria." *International Journal of Cyber Criminology* 6(2):1001.

Olonisakin, T. T., A. J. Ogunleye, and S. O. Adebayo. 2017. "The Nigeria Criminal Justice System and Its Effectiveness in Criminal Behaviour Control: A Social-Psychological Analysis." *Journal of Humanities & Social Science* 22(2):33–48. doi:10.9790/0837-2202043348.
Oluwafemi, A. 2023. "US Court Jails Nigerian for 60 Months Over $200k Romance Scam." *The Cable*. https://www.thecable.ng/us-court-jails-nigerian-for-60-months-over-200k-romance-scam.
Orhero, M. I., and C. Nwoke. 2025. "Theorizing the hypeman in Nigerian popular culture: poetics, performance, and the e-fraud economy." *Canadian Journal of African Studies* 1–20. doi:10.1080/00083968.2025.2462217
Orji, U. J. 2019. "An inquiry into the legal status of the ECOWAS cybercrime directive and the implications of its obligations for member states." *Computer Law & Security Review* 35(6):105330. doi:10.1016/j.clsr.2019.06.001
Platt, J. 1981. "Evidence and Proof in Documentary Research: Some Specific Problems of Documentary Research."
Sociological Review 29(1):31–52. doi:10.1111/j.1467-954X.1981.tb03021.x.
Rush, M. and S. Lazarus. 2018. "'Troubling' Chastisement: A Comparative Historical Analysis of Child Punishment in Ghana and Ireland." *Sociological Research Online* 23(1):177–96. doi:10.1177/1360780417749250.
Scott, J. 2014. A matter of record: Documentary sources in social research. London: John Wiley & Sons.
Scott, S., R. Geffner, R. Stolberg, and S. Sirikantraporn. 2023. "Common Characteristics of Women Who Kill in the Context of Abuse: A Content Analysis of Case Files." *Journal of Aggression, Maltreatment, & Trauma* 32(1–2):15–33. doi:10.1080/10926771.2022.2029657.
Skinner, O. D., J. Duckett, N. A. Smith, V. V. Volpe, and S. M. McHale. 2024. ""Actually, I Don't Do Different": Black parents' Perceptions of Gender Socialization of Sons versus Daughters." *Journal of Family Psychology* 38(7):1040–50. doi:10.1037/fam0001240.
Smith, D. J. 2017. *To Be a Man is Not a One-Day Job: Masculinity, Money, and Intimacy in Nigeria*. Chicago: University of Chicago Press.
Snyder, J. A., and K. Golladay. 2024. "More Than Just a 'Bad' Online Experience: Risk Factors and Characteristics of Catfishing Fraud Victimization." *Deviant Behavior* 1–21. doi:10.1080/01639625.2024.2416071
Soares, A. B. and S. Lazarus. 2024. "Examining Fifty Cases of Convicted Online Romance Fraud Offenders." *Criminal Justice Studies* 37(4):328–51. doi:10.1080/1478601X.2024.2429088.
Suarez-Tangil, G., M. Edwards, C. Peersman, G. Stringhini, A. Rashid, and M. Whitty. 2020. "Automatically Dismantling Online Dating Fraud." *IEEE Transactions on Information Forensics and Security* 15:1128–1137. doi:10.1109/TIFS. 2019.2930479.
Tade, O. 2021. "COVID- '419': Social Context of Cybercrime in the Age of COVID-19 in Nigeria." *African Security* 14 (4):460–83. doi:10.1080/19392206.2021.2004642.
Thumboo, S. and S. Mukherjee. 2024. "Digital Romance Fraud Targeting Unmarried Women." *Discover Global Society 2* (105). doi:10.1007/s44282-024-00132-x.
Torsu, L. A. 2024. "Crime prevention in the digital age: Challenges and technologies for policing in Aflao border township in Ghana." *The Police Journal*. doi:10.1177/0032258X241309190
Tuki, D. 2024. "Examining the Effect of Gender, Education and Religion on Attitudes Toward Gender Equality in Nigeria." *Politics, Groups & Identities* 13(1):1–27. doi:10.1080/21565503.2024.2304311.
Whittaker, J. M., M. R. McGuire, and S. Lazarus. 2025. "Conversations with Deviant Website Developers: A Case Study of Online Shopping Fraud Enablers." *Journal of Criminology*. doi:10.1177/26338076251321844.
Yushawu, A. and K. Jaishankar. 2025. "Sakawa in Ghana: The Influence of Weak Ties on Economic Cybercrime Offender Networks." *Deviant Behavior* :1–21. doi:10.1080/01639625.2025.2459681.