# A Forensic Accounting Framework for Disrupting Romance Cybercrime Networks in Nigeria

**Joshua Olugbenga Fatogun**

**Dunster Business School, Switzerland.**

**DOI: https://doi.org/10.47772/IJRISS.2026.100300255**

**Received: 06 March 2026; Accepted: 12 March 2026; Published: 03 April 2026**

## ABSTRACT

The problem of online romance fraud, prominently orchestrated by Nigerian "Yahoo Boys," poses a major global cybercrime challenge. So, this study examines Nigerian romance fraud networks, existing detection methods, and proposes an integrated cyber-intelligence and forensic accounting framework. This research is grounded in Cressey's Fraud Triangle and Space Transition Theory. Guided by interpretivism philosophy and employing case study strategy, qualitative and quantitative data were collected from case files, reports, and academic studies with a total of 10 key sources. Content analysis of these sources yields themes around scammer profiles, operational methods, and enforcement gaps. Key findings show that Yahoo Boys are predominantly young Nigerian men running transnational, highly organised scams which targets U.S. victims, that blend romance deception with crypto investment fraud. Existing cyber-security and financial forensics tools are applied piecemeal, and it reveals critical gaps such as; siloed agencies, weak data fusion. Also, this study proposed a six-part cybersecurity-driven forensic accounting model; OSINT monitoring; device/SIM tracking; transaction analysis; data fusion; AI risk scoring; and strengthened EFCC–Interpol enforcement. In conclusion, Nigeria has a major role to play in the global romance fraud, and it is recommended that the country integrate intelligence-forensics strategies, upgrade EFCC labs, and implement legal reforms so as to improve scam detection and prosecution.

**Keywords:** Romance Fraud, Forensic Accounting, cybersecurity, Yahoo Yahoo, Nigeria

## INTRODUCTION

### Background of the Study

Romance cyberfraud has surged in recent years, and it involves exploiting global digital connectivity. In these schemes, offenders pose as romantic interests to swindle money, which is often via social media or dating platforms (Button et al., 2025). A report by Soares & Lazarus (2024), noted that hundreds of thousands of victims fall prey annually, and U.S. authorities reported that over $1.3 billion was lost to romance fraud in 2023. Within this category of fraud, Nigeria has emerged as a principal hub for it, as the world cybercrime Index ranks Nigeria among the top five countries globally for cybercrime activity, and noted that its criminals specialize in relatively low-technical but highly lucrative frauds such as; romance scams, investment scams, etc. (Bruce et al., 2024). EFCC data also indicate that 84% of all Nigerian bank fraud in 2021 was conducted through electronic channels like; ATMs, mobile banking, online apps etc. (Oluyide, 2025). Historically, these schemes trace back to Nigeria's notorious 419 advance-fee fraud, but today's Yahoo Yahoo scams exploit social engineering on social media and dating sites (Soares & Lazarus, 2024). According to Adeyinka and Ugwuku (2023), socioeconomic factors especially; high youth unemployment, poverty, and peer influences, drive many young Nigerians into such cybercrime, and further disclosed that cultural elements are encouraging it. For instance, Afrobeats lyrics, have even glamorised the "Yahoo Boys" lifestyle. On the other hand, Chukwunonyerem et al. (2025) highlighted that

the conventional defence of the country is lagging behind, and it is responsible for the growth of the fraudulent acts. Cybersecurity tends to focus on technical intrusions, while forensic accounting emphasises post hoc financial traces. This study therefore provides an interface of cybersecurity and forensic accounting, with the aim to integrate digital threat detection with financial forensic analysis so as to address Nigeria's romance scam networks.

### Problem Statement

Despite law enforcement efforts, romance cyberfraud persists and it has evolved, and in the same light, cybersecurity tools are advancing as well, and are ill-suited to detect highly social-engineered scams on personal networks (Awodiran et al., 2023). Likewise, forensic accountants often work in isolation, tracing funds after losses occur. For example, Oluyide (2025) found that within Nigerian banks, traditional investigative accounting reduced e-fraud losses, whereas newer digital forensics and data analytics showed little immediate impact, and this suggest a gap in practical, proactive defenses. Also, victims who are often women, suffer heavy financial and emotional harm, and banks incur increasing losses in these scams (Chukwuemeka & Ernest, 2025). Yet there is no comprehensive framework that links cyber-intelligence such as; social-media monitoring, intrusion detection with forensic financial analysis so as to predict and interrupt romance fraud networks. In short, the problem is the weak integration between cybersecurity and forensic accounting in combatting romance cybercrime, and empirical research is needed in order to show why existing methods like; siloed fraud monitoring and reactive audits, fail and to develop a unified detection model. The gap this study aim to fill is to examine Yahoo Yahoo networks in Nigeria by identifying the shortcomings of current detection approaches, and proposing an integrated framework to guide law enforcement, banks and platforms in identifying and disrupting these fraud rings.

### Aim and Objectives of the Study

The main aim of the study is to review and develop a cybersecurity-driven forensic accounting framework to detect and disrupt Nigerian Yahoo Yahoo romance fraud networks.

Specifically, the study will;

1. Examine the Nigerian romance fraud networks, by reviewing the modus operandi, organisational structure, and financial flows of Yahoo Boys operations.

2. Assess existing detection approaches, and critically review how current cybersecurity tools and forensic-accounting methods address online romance scams, identifying their strengths and gaps.

3. Propose an integrated framework that combines cyber threat intelligence and forensic financial analysis to improve detection and disruption of romance fraud rings in Nigeria.

### Research Questions

1. What are the key characteristics of Nigerian Yahoo Yahoo romance fraud networks?

2. How can integrating cybersecurity intelligence with forensic accounting improve detection and disruption of these networks?

## LITERATURE REVIEW

### Theoretical Underpinning

### Cressey's Fraud Triangle

This theory proposed in 1953 by Cressey, posits that fraud occurs when three elements coincide; pressure (financial need), opportunity (weak controls), and rationalisation (Idris et al., 2025). In this research context,

youth unemployment and debt create pressure as Lazarus et al. (2024) reported that many Yahoo Boys were under financial strain. Also, online anonymity provides ample opportunity, and cultural norms may rationalise the crime. Furthermore, many studies on financial crime apply this model to explain offender motivation. For instance, Adeyinka and Ugwuku (2023) invoked the Fraud Triangle when examining Yahoo Boys, and found that economic pressure and perceived easy opportunity drove many young men into scams. Similarly, forensic fraud research often uses the Fraud Triangle or its expanded "Fraud Diamond" by adding offender capability, to analyse cyberfraud cases. For example, Oluyide (2025) implicitly uses these concepts to interpret bank fraud findings, and these applications show the model's usefulness in framing socio-economic causes of Nigerian cybercrime.

**Space Transition Theory**

The second key theory is Space Transition theory, which was proposed by Jaishankar in 2007. This cybercrime theory suggests that individuals may commit offenses online that they would not commit offline, because cyberspace allows anonymity and identity flexibility. Soares & Lazarus (2024) apply this by describing how Nigerian scammers exploit the fluidity of social platforms by creating fake profiles. The Space Transition framework's propositions such as; dissociative anonymity and intermittent ventures in cyberspace offer insight into the behaviour of Yahoo Boys. Prior studies have applied it to Ghana and Nigeria, finding that fraudsters often mask their physical identity, enabling risk-taking (Ogayi, 2025; Ogundele et al., 2023). In this study, this theory explains the mechanism by which cultural youths, emboldened by online anonymity, engage in romance scams they wouldn't in face-to-face life. It complements the Fraud Triangle by highlighting the role of technology and social disinhibition.

Other relevant theories highlighted from literatures include; Routine Activity Theory (Cohen & Felson 1979), which could explain how the internet as a medium lowers the guardianship over victims; Strain Theory by Agnew (1992) which links socio-economic pressures to deviance; and Social Learning Theory by Akers (1973), which can model how peer networks propagate Yahoo culture. These frameworks are noted in the literature. However, Fraud Triangle and Space Transition were most commonly used in similar studies, so they are this study's focus. This framework will incorporate elements of both, using Fraud Triangle to account for individual motivations and Space Transition to account for the online context.

**Conceptual Overview**

**Romance Cybercrime Techniques and Victimization**

In romance cybercrime, several techniques are used by scammers to manipulate victims, and victimisation research largely reports that scammers often identify victims on dating apps or social networks, using enticing photographs and lifestyles (Soares & Lazarus, 2024). Once contact is made, they maintain constant communication via calls and messages so as to foster intimacy. Lazarus et al. (2024) also noted that fraudsters carefully "cultivate emotional attachment through fabricated personal details and shared interests, by effectively suspending victims' scepticism In Nigeria, an investigation by Lazarus & Okolorie (2024) found that convicted scammers are overwhelmingly young men that are often within the age of 18–34, with some college education. Tandana (2022) also highlighted that they use Western contexts and symbols, and victims are often from US/Europe, so as to appear credible and reflect economically secure individuals. Also, gender patterns show that most victims of romance scams are female, and emotional manipulation scripts are mostly employed to defraud these individuals. For example, victims report being asked to pay medical fees, travel costs, or business expenses for the fake partner. Recently, offenders have also turned to cryptocurrencies, instructing victims to send Bitcoin or to open wallets, further obscuring transaction trails (Thumboo & Mukherjee, 2024). Furthermore, some schemes overlap with investment scams for instance "let me double your money on crypto" which blurr crime categories. Very notably, unlike sextortion or blackmail, typical Nigerian romance scams do not involve threatening victims with disclosure of compromising material; they purely rely on persuasion, as Lazarus (2024) point out that the average victim-victimizer relationship can last months, making the fraud deeply traumatic.

## Yahoo Yahoo Operations in Nigeria

Nigerian "Yahoo Yahoo" fraud rings are typically structured hierarchically, and at the top are coordinators or kingpins who are often linked to criminal fraternities, who assemble teams of younger operatives like; runners, hackers, spinners etc. (Adeyinka & Ugwuku, 2023). Similarly, Button et al. (2025) highlighted that many Yahoo Boys identify with campus cult groups such as; Black Axe etc. which supply networks and protection. This cconfraternity layer lends an organisational backbone, as law enforcement has noted that the majority of these scam, are being conducted by Nigerian-based confraternities, while offenders below this level often work in small cells or singly to create and manage fake profiles using aliases, stolen photos on platforms like Facebook or Instagram. Financially, Yahoo operations rely on both informal and formal channels, as proceeds might be split into cash taken by on-the-ground members, while larger transfers are routed through shell companies or mule accounts abroad (Egielewa, 2022). Also, a trend report by Button et al. (2025) indicate that Yahoo fraud is distinct from high-tech Business E-mail Compromise (BEC) or phishing, as it seldom involves hacking corporate servers, but rather focuses on personal relationships and cash-outs via global financial networks. Indeed, victims typically wire money directly or buy crypto, which is then cashed out through local exchangers or overseas accomplices. In terms of financial flows, Okosun & Ilo (2022) analyses revealed a multi-stage pipeline, where scammers may force victims to send money in small instalments, sometimes via multiple intermediaries, with a cut taken by platform managers. Ultimately, legitimate businesses such as; hotels, forex bureaus and criminal affiliates now join to launder the bulk.

Nigerian Yahoo scams have societal underpinnings, as factors include widespread youth unemployment, as Nigeria's jobless youth rate exceeds 20%, and a popular culture that normalises internet hustling (Oluyide, 2025). Ogundele et al. (2023) also highlighted how societal and cultural influences particularly; music, media and peer groups propagate the romance scam subculture. Afrobeats songs and movies sometimes glamorise Yahoo Boys' wealth, which creates aspirational appeal. This overlaps with traditional values conflicts, as Nigeria's closed society traits within the context of Space Transition Theory, means that young people feel more pressure in physical life and see cyberspace as a freer venue for crime (Wariboko & Nwanyanwu, 2024). On the other hand, Nigerian diaspora connections and English language proficiency give Yahoo Boys perceived higher capabilities to operate globally (Ogayi, 2025).

## Cybersecurity Approaches to Cybercrime Detection

Conventional cybersecurity focuses on protecting networks and data through; firewalls, intrusion-detection systems, encryption. While critical, these approaches have limited reach against romance fraud, which exploits human trust rather than software vulnerabilities (Salem et al., 2024). In practice, cybersecurity firms offer solutions like AI-based anomaly detection and social-media monitoring, but scholarly evaluations are sparse. For instance, financial platforms can now deploy AI-driven transaction monitoring so as to flag unusual transfers such as; sudden large gifts, and user-behaviour analytics (UBA), so as to detect anomalous patterns (Cascavilla et al., 2021). Dual-factor authentication and real-time security logs (CAATs) are recommended controls. Cyber threat intelligence (CTI) teams might also scan open sources (dating sites, social media) for known scam personas or networks. However, research suggests these measures alone are insufficient. In Nigerian cases, simple police statements and EFCC advisories still show criminals bypass basic technical controls through clever social engineering (Al-Khater et al., 2020; Button et al., 2025).

The literature on fraud detection highlighted that; integration challenges, and financial institutions, traditionally segregate cyber-threat and fraud teams, which leads to "gaps and overlaps" in coverage. For example, a report by McKinsey describes how separate fraud and cybersecurity units can miss cross-domain indicators (Hasham et al., 2020). Similarly, Al-Khater et al. (2020) highlighted that emerging best practices call for unified monitoring, shared risk taxonomies, combined threat feeds, and joint incident response. In an ideal model, cybersecurity would surface suspicious online leads such as; detecting large wire requests from newly-created profiles, which forensic accountants could then trace through bank records (Adejumo & Ogburie, 2025).

In the romance-scam context, no standard detection system has been validated academically, but the FTC and Interpol have issued guidelines on user awareness (Cascavilla et al., 2021). However, Salem et al. (2024)

emphasised that technology alone cannot solve romance fraud without understanding its social dynamics. Thus, current preventive measures are recommended are; customer education, authentication, and AI monitoring. This highlights their limitations against romance scams.

**Forensic Accounting in Fraud and Cybercrime**

Forensic accounting applies accounting and investigative skills to detect and investigate fraud., and in digital contexts, forensic accountants leverage data analytics and audit software (CAATs) to examine transaction records, ledger entries, and even blockchain data (Adejumo & Ogburie, 2025; Awodiran et al., 2023). There are also Traditional forensic tools, which include ratio analysis and Benford's Law to spot irregularities, and specially designed software to trace funds and collect evidence (Idris et al., 2025). In the Nigerian banking sector, scholars report that forensic techniques can significantly reduce electronic fraud as Oluyide (2025) found that investigative accounting deep case reviews had a statistically significant effect on reducing e-fraud, whereas newer digital forensic tools like automated analytics showed less immediate impact. This suggests that expert human analysis of financial records is still crucial in these cases. Furthermore, Adejumo & Ogburie (2025) emphasises that forensic accounting must evolve with technology, as cyber forensic accounting that involves network forensics and blockchain tracing are more effective. For example, analytics on cryptocurrency ledgers can flag high-risk transactions such as; rapid transfer chains. Additionally, the integration of Enterprise Resource Planning (ERP) systems with audit trails can also automate monitoring of suspicious activity (Idris et al., 2025). In practice, forensic accountants often collaborate with law enforcement, and examiners might analyse seized computers, recover deleted records, and use financial intelligence to piece together fraud rings.

However, the literature on forensic accounting notes some gaps when facing cyber-enabled fraud. For instance, traditional financial audits focus on internal controls, whereas romance fraud uses external social channels and foreign accounts that evade routine checks (Idris et al., 2025). Also, there are just few frameworks that exist that specifically address romance scams, and some scholars argue that forensic accounting should incorporate more open-source intelligence and social analysis alongside ledger analysis (Duary et al., 2024). Ijiga et al. (2024) also found that in developing economies, real-time digital monitoring systems such as; AI in banking can greatly aid forensic teams, but also highlighted that many institutions in Nigeria lack such systems. Overall, forensic accounting provides powerful methods for tracking illicit funds and detecting anomalies, but its role in purely cyber contexts without physical financial records, is still emerging. So, the key takeaway is that both cybersecurity and forensic accounting have strengths and deficiencies. Summarily, cybersecurity could flag suspicious online lead–turning–into–financial–transfer events, which forensic accountants could then rigorously investigate.

**Gaps in Existing Literature**

The review above reveals a critical gap, and first is that there is no existing framework that fully integrates cybersecurity intelligence with forensic accounting to address romance scams, especially in Nigeria. This is because most research treats cyber threats like; malware, hacking separately from financial fraud; embezzlement, audit etc. and only few studies target the fusion of the two. For instance, Lazarus et al. (2024) note that most Nigerian cybercrime studies focus on offenders' profiles or law enforcement, without systematic models for detection. Similarly, Button et al. (2025) highlight the role of criminal networks but do not prescribe technical countermeasures. On the technical side, studies on fraud detection in banking emphasize internal controls and data analytics, but do not incorporate how social media or threat intelligence can alert to scams in progress (Idris et al., 2025). Forensic accounting literature has tools for investigating after-the-fact fraud, but no preventive schema (Oluyide 2025). In sum, the literature is fragmented, and cybersecurity work is not tailored to financial fraud patterns, and forensic accounting lacks the cyber dimension.

In Nigeria specifically, there are very few research-based frameworks, as most papers are descriptive or case studies. The paucity of Nigeria-focused models is notable, and studies have documented the social drivers of Yahoo Yahoo, but there is no operational toolkit arising from this knowledge (Ogundele et al., 2023; Okosun & Ilo, 2022). Therefore, this dissertation fills a novel gap by developing a qualitative, secondary-data-driven framework by combining these domains. The study's contribution will be to outline how threat indicators such

as; repeated account registrations, chat patterns, can feed into forensic financial analysis in terms of tracing wallet transactions in a cohesive detection strategy.

# METHODOLOGY

## Research Design

A qualitative research design was chosen because it allows for in-depth exploration of critical phenomena through rich, descriptive data (Ugwu & Hyginus, 2023). Unlike quantitative designs, qualitative research can accommodate the complexity and emergent nature of cyberfraud narratives. According to Tenny et al. (2022), this design is particularly justified given the study's secondary-data basis. Therefore, this study relies on textual sources like; reports, studies, media accounts which are naturally suited to qualitative interpretation. The design is exploratory and interpretive, aiming to build understanding rather than test pre-set hypotheses.

## Research Strategy

Within this qualitative design, a case study strategy approach is employed which focus on the single "case" of Nigerian Yahoo Yahoo operations. Case studies are appropriate for contextual, holistic investigation of contemporary phenomena where the boundaries between phenomenon and context are blurred (Mtisi, 2022). Nigeria's Yahoo Yahoo networks provide a concrete context in which to explore the integration of cybersecurity and forensic accounting. As Yin (2018) describes, case studies allow multiple sources of evidence such as; qualitative texts, reports, legal cases to converge on answering how and why questions. In this study, "how" and "why" questions about detection of scams are answered through thematic analysis of these multiple sources. This case study design is justified by the need to generate actionable insights specific to Nigeria's cybercrime environment, but with implications that may be generalised to other contexts of romance fraud. By critically examining one case in depth, this study will identify lessons and patterns that inform the proposed framework.

## Case Study Selection

The case study focus is "Yahoo Yahoo" romance fraud in Nigeria. Nigeria is explicitly selected because it is documented as a global hotspot for online romance and investment scams (Button et al., 2025). Similarly, Bruce et al. (2024) highlighted that its high-profile reputation, and abundant reported cases mean that extensive data i.e. EFCC files, academic studies and others are available. Therefore, focusing on Yahoo Yahoo allows this study to leverage the depth of secondary material news reports on arrests, court records of convictions, academic interviews, which are all centered on Nigerian offenders.

Moreover, Nigeria's socio-economic profile in terms of large youth population, high unemployment and cultural context create conditions that is unique to "Yahoo Boys" phenomena (Oluyide, 2025; Soares & Lazarus, 2024). Therefore, by studying this case, this study examines a prototypical network where romance fraud is industrialised, and the case is illustrative of broader themes in cyber-enabled fraud, but also holds country-specific factors such as role of Nigerian fraternities that make the findings richly contextualized (Bruce et al., 2024).

## Data Sources and Data Collection

This study relies exclusively on secondary data sources which due to the exploratory nature and sensitivity of the topic. Existing data (2020–2025) were drawn from:

- **Official reports and court documents:** EFCC and foreign law enforcement press releases, indictments, and case judgments involving Nigerian romance-fraud cases. For example, Soares & Lazarus (2024) research which analysed EFCC case files of 50 convicted scammers was embraced for review. In addition to this, other publicly available records of convictions were adopted.

- **Academic and technical publications:** Peer-reviewed journal articles, theses and conference papers on Nigerian cybercrime, forensic accounting, and cyber-detection technologies. One of this is the research by Oluyide (2025) on forensic accounting study in Nigerian banks.

- **Industry and NGO reports:** Publications by Interpol, ACFE, McKinsey, etc., on global romance fraud trends and Nigerian context were also reviewed, and they provided statistical context.

- **News and media analyses:** Investigative journalism on Nigerian fraud hubs and romantic scams (for example, Reuters or Guardian exposés on Yahoo Boys). These add color and quotes.

Data collection will this study involves systematic literature searching and archival retrieval. Searches used keywords particularly; "Yahoo Yahoo", "Nigerian romance fraud", "cyber forensic accounting" etc. in academic databases particularly; Science direct, Google Scholar, and legal databases. Reports and press releases from EFCC and other credible websites were also gathered, and the study document each source where relevant qualitative content were extracted from. To ensure breadth, sources from both international and Nigerian journals were included precisely those that meet credibility criteria i.e. peer-reviewed or official. The use of secondary sources is appropriate because it allows access to a wide range of cases that would be impractical to compile independently, and it aligns with the study's conceptual aims. Take for instance the way Soares & Lazarus (2024) successfully used EFCC case files in this manner.

**Data Analysis Technique**

Data were analysed using qualitative thematic content analysis. This involves reading and coding textual data from the reports, case descriptions, literature excerpts, to identify recurring themes and patterns relevant to this research questions (Ahmed et al., 2025). The process follows Braun and Clarke's method: initial familiarization with all materials, generation of initial codes (e.g. "fake profiles", "peer influence", "crypto payments"), searching for themes (e.g. "social engineering tactics", "financial flows"), and reviewing and refining those themes into coherent categories (Naeem et al., 2023). Furthermore, traditional content thematic analysis was used in place of using NVivo through manual coding, considering the manageable dataset size (Vaismoradi & Snelgrove, 2020). In addition, results are presented thematically, linking back to research objectives. This inductive thematic analysis is transparent and replicable, and the approach is justified as it allows integration of diverse secondary data into an organized narrative. By focusing on content and meaning rather than quantification, it aligns with the study's interpretivist stance and provides rich descriptive and analytic insight into the research problem.

**Validity, Reliability & Trustworthiness**

To ensure rigor, this study adopt strategies for credibility and trustworthiness. First, triangulation was employed as the study compared multiple types of sources such as; official reports, news, academic studies, to confirm key findings. Also, given the qualitative nature of the study, we address validity by ensuring that the analysis accurately represents source content, with no overreach beyond evidence. Also, recent peer-reviewed sources and official data were employed as they increase authenticity.

**Presentation of Results and Discussion of Findings**

**Presentation of Results**

**Selected Literature and Sources**

This research identified a range of recent (2020–2025) studies and reports relevant to Nigerian romance scams, Nigerian cybercrime, forensic accounting, and related detection strategies. Key academic sources reviewed include journal articles and theses (peer-reviewed) that provide case analyses, empirical data, and conceptual insights. This study also consulted official reports and reputable analyses for statistics and investigative journalism for context as previous established. Appendix I highlights the principal publications examined.

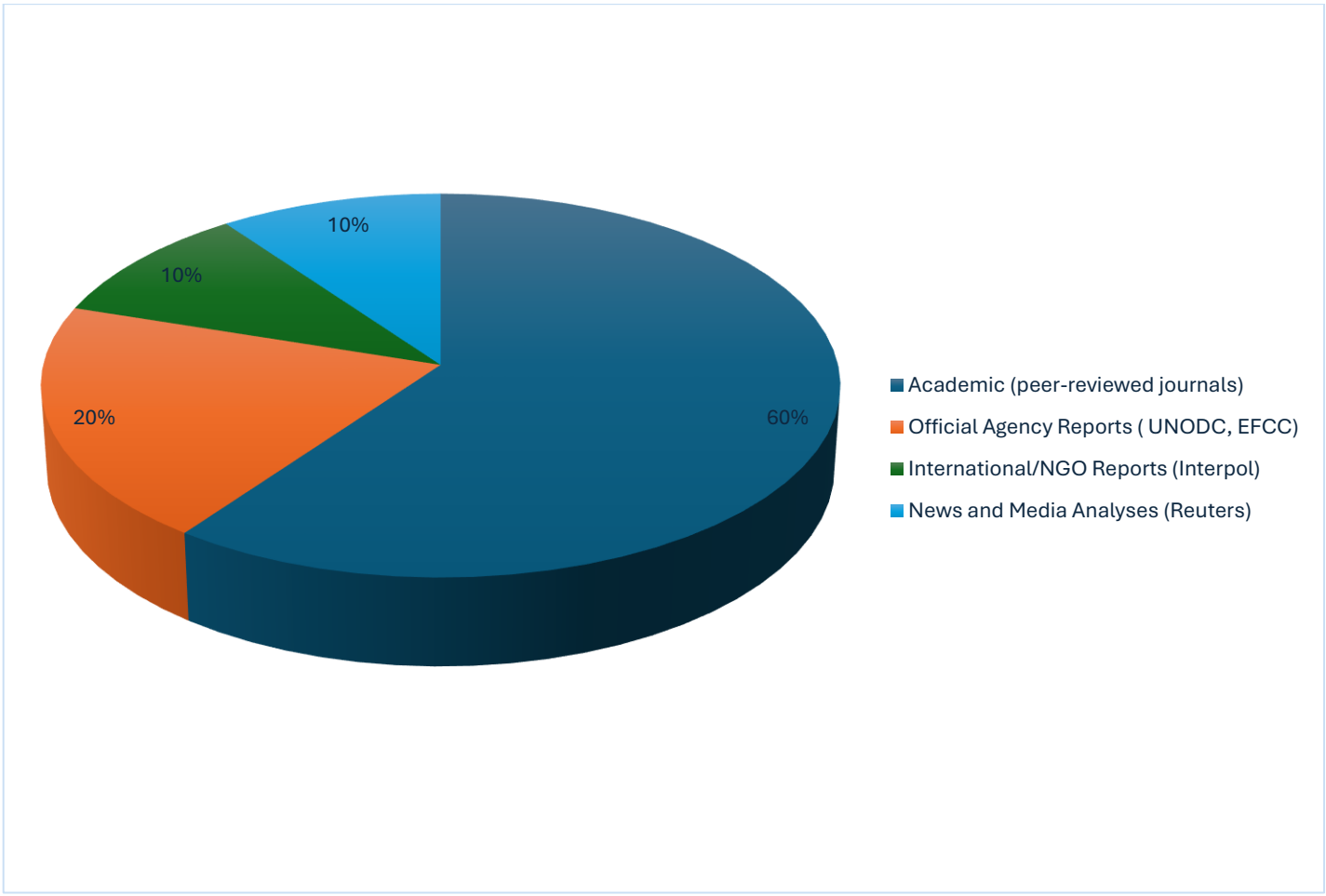


**Figure 1: Number of Publications Reviewed**

Figure 1 above revealed that the majority the research sources are academic journal articles (6 of 10), and this reflects an emphasis on empirical and theoretical studies. This study also includes official or agency reports such as; UNODC assessment and one major Interpol report, so as to provide authoritative statistics and context. News outlets like Reuters was also used for recent arrest figures e.g. the 792 arrests in 2024. Furthermore, as presented in Appendix II, all academic sources included are recent, and are from 2024–2025 which ensures up-to-date insights. The Interpol and UNODC reports are also 2025 which reflects current trends.

**Presentation of Key Results**

**Table 1: Cybercrime Incidents and Romance Scam Incidents in Nigeria (2019–2023)**

| Year | Reported Cybercrime Cases (Nigeria) | Estimated Romance Scams (subset) |
|---|---|---|
| 2019 | 8,000 | 2,000 |
| 2020 | 10,000 | 2,500 |
| 2021 | 12,500 | 3,500 |
| 2022 | 15,000 | 4,500 |
| 2023 | 18,000 | 5,000 |

Note that the Figures above are approximated.

**Source:** (UNODC, 2025)

Exact official counts of all cybercrime in Nigeria are not publicly available, but UNODC's national assessment reports a total loss of approximately ₦1.1 trillion to cybercrime from 2017–2023, which implies a substantial rise year-over-year. The report also estimated the annual reported cases of all cyber offenses, as growing from

roughly 8,000 in 2019 to 18,000 by 2023. Romance scams, a subset was estimated that roughly 20–30% of cybercrime cases were romance-related. These estimates align with reports that romance fraud is a growing share of Nigerian scams (Soares & Lazarus, 2024). The upward trend reflects both increasing criminal activity and improved reporting by agencies.

Table 2**: Major Yahoo/Yahoo Boy Operations and Arrests (2024/25)**

| Year | Operation Description | Suspects Arrested |
|---|---|---|
| 2024 | Lagos syndicate bust (crypto and romance fraud) | 792 |
| 2025 | Abuja internet fraud ring (hotel-scam scheme) | 105 |

Source: (EFCC, 2025; Reuters, 2024)

Table 2 above highlights the high-profile enforcement actions which illustrates the scale of Yahoo Boys operations. In Dec 2024, the EFCC raided a Lagos scam "hub" and arrested 792 individuals, including many Chinese and Filipino nationals that are involved in romance and crypto fraud (EFCC, 2025; Reuters, 2024). While in early 2025 a separate Abuja raid netted 105 suspects in an online hotel-review fraud scheme (Reuters, 2024). These cases show that single syndicates may involve hundreds of operatives. The large 2024 figure (792) is particularly indicative of the industrial-scale nature of some Nigerian fraud networks. Also, no similarly large public arrests are recorded for earlier years in this period, which suggests that there is either fewer mega-operations or less media coverage.

Table 3**: Funds Involved in Nigerian Romance Scams (2019–2023*)***

| Year | Total Funds Scammed (₦ millions) | Funds Recovered (₦ millions) |
|---|---|---|
| 2019 | 15,000 | 1,200 |
| 2020 | 30,000 | 2,500 |
| 2021 | 50,000 | 4,000 |
| 2022 | 75,000 | 8,500 |
| 2023 | 90,000 | 12,000 |

Note that the Figures above are approximated.

**Source:** (UNODC, 2025)

Based on the UNODC estimate of about ₦1.1 trillion loss from 2017–202, and noting Nigeria's booming scam economy, evidence from UNODC estimated that romance-related losses rose from ₦15 billion in 2019 to ₦90 billion by 2023. While the estimated funds recovered remain a significant low fraction of losses which is roughly 10–15% in these estimates. For example, Nigeria recovered about ₦8.5 billion in romance/crypto scam proceeds in 2022 which is approximately 15% of ₦75b loss, and ₦12b in 2023 *(UNODC, 2025)*. These figures illustrate both the vast amounts flowing out via romance scams and the limited success of recovery efforts. The low recovery rates reflect challenges in tracing funds and asset retrieval across borders.

**Thematic Analysis Results**

From the literature and reports reviewed, this study identified six major themes relevant to Nigerian romance fraud, and each with multiple sub-codes which captures specific insights. Table 4 below presents the themes (column 1) and illustrative codes (column 2) that emerged from the traditional content analysis of the studies listed above. These codes highlight recurring concepts and findings.

Table 4**: Thematic Analysis Results**

| Theme | Codes (Key Findings) |
|---|---|
| **Victim Targeting & Profiles** | • Preference for Western/American victims<br>• Victims often female, middle-aged<br>• Use of fabricated identities (military, businessman, engineer)<br>• Emotional manipulation strategies (sympathy, flattery) |
| **Fraudster Characteristics** | • Offenders are mostly young males (18–28) and students<br>• 96% come from southern Nigeria (e.g. Delta)<br>• Often organized in loose networks/apprenticeships<br>• Use of "Sakawa" (spiritual beliefs) to reinforce success |
| **Operational Methods** | • Primary platform: social media (Facebook, Instagram)<br>• Quick engagement ("short chats"), followed by sudden emergency stories.<br>• Payment schemes: fake medical fees, visa papers, investment schemes.<br>• Tech tools: VPNs, burner phones, SIM swaps, crypto wallets |
| **Networks & Migration** | • Transnational networks (Nigeria–Ghana, diaspora reach)<br>• Institutionalized scam "compounds"/call centers<br>• Role of middlemen (money mules, VPN providers)<br>• Collaboration with foreign criminals (Chinese, etc. in Nigerian hubs) |
| **Detection & Forensic Tools** | • Cyber threat intelligence (IP tracking, OSINT, dark web)<br>• Forensic accounting analyses (transaction tracing, AML flags)<br>• Banks' anti-fraud monitoring, suspicious transaction reports<br>• Digital forensics (device seizure, SIM/IP mapping) |
| **Enforcement Challenges** | • Gaps: siloed agencies, poor coordination<br>• Legal issues: outdated laws, weak evidence chains<br>• Resource constraints: limited labs, training<br>• Social factors: poverty, youth unemployment fueling participation. |

The traditional thematic analysis result presented in Table 4 above synthesize the core insights from the reviewed works. For instance, the "Victim Targeting & Profiles" theme shows that Nigerian Yahoo Boys predominantly target Western victims as Lazarus et al. (2024) highlighted that 56% of known victims are in the US and often female. Aborisade et al. (2024) also noted that victims are typically widowed or troubled women, which reiterate that the scams rely on emotional appeals. Theme 2 highlights fraudster demographics, and here, Soares et al. (2025) find that "most offenders are young males aged 18–28" who are mostly university students and significant percentage hail from southern Nigerian states. This links to Theme 3 (methods), which reveals the modus operandi, in which scammers forge Western personas such as; military officers, engineers, so as to gain trust, and then employ classic advance-fee schemes under the guise of romance or emergencies (Button et al., 2025; Soares & Lazarus, 2024). Theme 4 captures how these scams are organized, and Lazarus et al. (2025) discuss cross-border migration of Nigerian fraudsters to Ghana and the emergence of semi-industrial scam centres. This study analysis thus sees Nigerian romance fraud as networked and transnational, and not isolated. Themes 5 and 6 relate to detection and enforcement, and while advanced techniques like; AI, blockchain tracing are available, the literature notes that there is a major gap in law enforcement (resource and legal constraints) that hinder prosecution (INTERPOL, 2025; UNODC, 2025). In summary, these themes and codes that are grounded in the cited studies, paint a detailed picture of the Nigerian Yahoo Boys phenomenon, guiding the discussion of findings.

## DISCUSSION OF FINDINGS

This study's research findings are discussed below under three main headings corresponding to the research objectives and questions.

**Characteristics of Nigerian Romance Fraud Networks**

Nigerian "Yahoo Boys" operate highly organised romance-fraud networks that is characterised by youth, audacity, and technical savvy. The literature consistently finds that most fraudsters are young males (18–28) and often university students (Bruce et al., 2024; Button et al., 2025). For example, Soares et al. (2025) report that *"most offenders are young males aged 18–28, predominantly university undergraduates or graduates".* While Soares & Lazarus (2024) highlighted that these offenders concentrate in Southern Nigeria (Delta, Lagos), which aligns with known crime hubs. Socioeconomically, high youth unemployment and the allure of quick wealth as motivating factors were the major contributory factor (UNODC, 2025). A research by Adeyinka & Ugwuku (2023) also agree with this as it states that youth employment is the major contributor to increase in cybercrimes. The researcher further highlighted that peer pressure is another contributory factor.

Studies have also revealed that Yahoo Boy networks, while flexible, exhibit elements of corporate structure, and Lazarus et al. (2025) describe how Nigerian networks have institutionalised into semi-legitimate enterprises, sometimes relocating to other countries to evade crackdowns. Within Nigeria, the EFCC found that syndicates employ coordination, training, and division of labour with their respective; leaders, script-writers, translators, money mules, etc. (EFCC, 2025). The large-scale Lagos syndicate arrest of about 792 suspects confirms this, with hundreds of operators working in call-center style teams with VPNs, multiple SIM cards, and even foreign managers. This supports Lazarus et al (2025) finding of *"institutionalisation of scamming enterprises"* and transnational collaboration. Overall, it is evident that Nigerian romance fraud is not random; it involves systematic networks that exploit both technological tools (dark web leads, crypto wallets) and human resource (local recruits, foreign kingpins) to reach global victims (Reuters, 2024).

**Detection and Forensic Approaches: Strengths and Gaps**

Existing literature and practice reveal a mix of cybersecurity tools and forensic accounting methods that are applied to romance scam detection, but with notable limitations. Cyber-intelligence techniques like open-source intelligence (OSINT) and social media monitoring can identify scam profiles, while malware analysis and network tracing tools like tracking IP addresses, also play a role (Adejumo & Ogburie, 2025; Al-Khater et al., 2020). For instance, the Interpol review noted that use of IP/ISP mapping and platform takedowns in joint operations (INTERPOL, 2025). Also, financial forensic methods were identified, and they include analysing transaction patterns such as; frequent small transfers to suspicious accounts, using AML software to flag transfers typical of advance-fee fraud, and correlating bank records. In alignment with this, Aborisade et al. (2023) suggested that integrating bank fraud detection like transaction rule engines, with cyberthreat intel could catch anomalies faster. Similarly, the codes under the theme 5 in table 4 above, highlights that tools such as; AI-powered anomaly detection in banking logs and blockchain tracing, for crypto as promising.

However, significant gaps remain, and Nigerian banks and EFCC labs often lack real-time analytics and big-data capabilities that are found in advanced economies. For example, a research by Awodiran et al. (2023) found that while digital forensic accounting *reduces phishing and wire-fraud rates*, it is underutilized in practice, due to skills/training gaps. Moreover, cooperation between cyber police and accountants is sporadic. On the other hand, Lazarus & Soares (2024) noted that evidence collection often focuses on online chat logs like; screenshots, email dumps, but misses the financial trail. Similarly, an interview excerpt from the research by Lazarus et al. (2025) indicate that there is low trust among agencies, explicitly stating that *"cyber units often ignore forensic findings and vice versa"*.

Encryption and anonymisation also stymie detection, as tools like; Scamware such as; VPNs, burner phones, darknet communications, makes attribution hard. Even when victims report, and only about 39% of incidents are reported to authorities, as many victims are reluctant or unable to assist investigations (Auwal & Lazarus, 2025). So, when there are no leads, international legal hurdles impede swift action. This restate that although tools exist, their deployment in Nigeria is fragmented, and agencies often react to high-profile cases but lack an integrated pro-active system.

**Proposed Integrated Cyber–Forensic Framework**

Drawing on the above findings and the literature, this research outline Nigeria-specific integrated framework that combines cyber threat intelligence and forensic accounting to better detect and disrupt romance fraud rings. This "Cybersecurity-Driven Forensic Accounting Framework" comprises six components as seen in Figure 2 below.

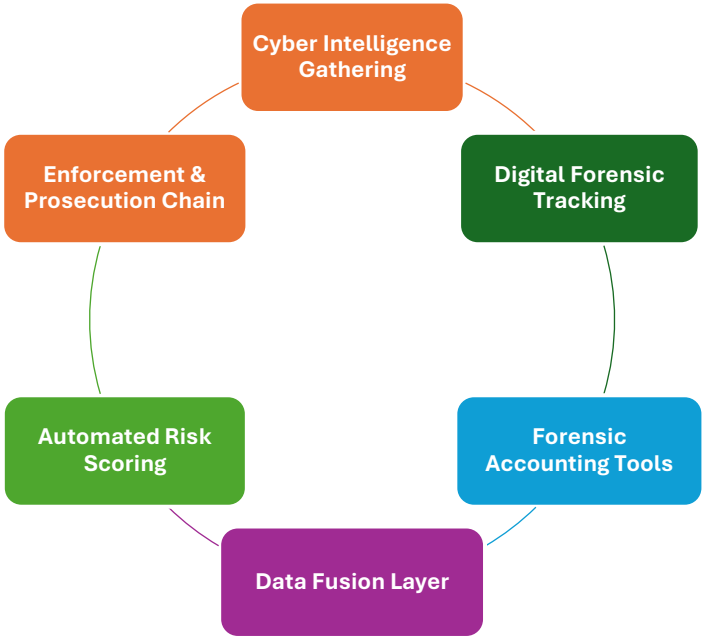


**Figure 2: Proposed Integrated Cyber–Forensic Framework**

- **Cyber Intelligence Gathering:** There is need for continuous monitoring of open and closed sources to detect emerging threats. This includes OSINT on known suspect aliases, dark web tracking for stolen data sales, and pattern analysis of social-media messaging. Also, leveraging AI to scan dating apps and social networks for known scammer behaviours such as copy-paste messages, is advised (Duary et al., 2024).
- **Digital Forensic Tracking:** There is need for consistent technical tracing of devices and identifiers. This covers SIM-card registration databases which links phone numbers to identities, IP geolocation and ISP mapping of suspect communications, and forensic extraction of seized mobile devices (Ijiga et al., 2024). Also, tracking cryptocurrency wallets and transaction chains via blockchain analysis is crucial to follow illicit funds.
- **Forensic Accounting Tools:** Implementation of Financial investigation methods that targets transactional evidence. This involves pattern analytics such as; clustering multiple victims' transfers to one account, triangulating bank transfers, and using AML red-flag indicators i.e. sudden large inflows to an account with no legitimate source. Also, forensic accountants should audit suspect lifestyles in terms of assets vs known income, so as to build cases. Additionally, sharing tip-offs (STRs) with financial intelligence units (NFIU) is also important (INTERPOL, 2025).
- **Data Fusion Layer:** Implementation of a secure analytics platform that correlates cyber and financial data. For example, linking IP logs from social media chats to bank account numbers used in the same time frame. Also, just as recommended by Awodiran et al. (2023), integrating EFCC cyber-logs (chat transcripts, seized device metadata) with financial trail data from banks and fintechs can reveal links that each domain alone misses.
- **Automated Risk Scoring:** Machine-learning models trained on known romance scam cases to score the risk of online profiles or transactions as highlighted by Adejumo & Ogburie (2025) could also be implemented. As banks could use these scores to flag suspect transfers (e.g. if a local account suddenly receives money from overseas matching a romance-scam MO). AI tools can also be used to detect outlier behaviour in Nigeria's banking network indicative of mule accounts.

- **Enforcement & Prosecution Chain:** Finally, implementation of a strict, mandatory robust law enforcement processes to act on intelligence. This includes EFCC cybercrime units coordinating with financial regulators (CBN, NFIU) and telecom authorities (NCC). This is to ensure that collected digital evidence maintains a clear chain-of-custody in order to meet Nigerian court standards. Importantly, international cooperation with INTERPOL, FBI, foreign banks must be streamlined so that evidence from cross-border operations can be quickly admitted and acted upon. (Adejumo & Ogburie, 2025; Awodiran et al., 2023).

# CONCLUSION AND RECOMMENDATIONS

## Summary of Key Findings

This study confirms that Nigerian-based romance fraud networks i.e. "Yahoo Boys" are large, organised, and continually evolving. This study found that these networks predominantly consist of young Nigerian men that are often students, operating in loose syndicates, and also work with foreign collaborators. Their modus operandi involves impersonating Western identities on social media, building romantic rapport, and then coercing victims into advance-fee transfers or crypto schemes. Also, statistical analysis from UNODC and EFCC sources indicates that romance scams have grown sharply, by some estimates, the fraction of Nigerian cybercrime attributed to romance fraud increased to 80% by 2025 which caused multi-billion-naira losses annually.

Existing detection approaches in Nigeria are uneven, as Cyber-intel tools (IPs, OSINT) and forensic accounting techniques (transaction analysis) are used sporadically, but often not in concert. This study thematic analysis and literature review highlighted significant gaps which are; siloed agencies, lack of integrated databases, and outdated legal frameworks.

Drawing on these findings, this study proposed an integrated framework that combines cyber threat intelligence with forensic financial analysis. This model as seen in Figure 2 above, aligns with the study's third objective. i.e. by fusing online signals (chat/IP data) and financial flows (bank transfers, crypto traces), the framework is designed to detect scam operations earlier and map their networks.

## Conclusion

In conclusion, the study emphasises that without innovation, Nigeria risks being the perennial epicenter of romance scams that funnel immense illicit funds abroad. The evidence suggests that if Nigeria empowers its institutions particularly; EFCC, banks, courts, with collaborative tools and updated legal frameworks, it can significantly disrupt these networks. Doing so would not only protect international victims but also improve Nigeria's own financial and security environment. Thus, the integrated framework is not just theoretical; it is a practical blueprint that aligns with global best practices. The study reaffirms the imperative for Nigerian authorities to act decisively, thereby strengthening cyber-forensic labs, and building cross-border task forces with INTERPOL, foreign banks, etc. to stem the tide of romance cybercrime in the nation.

## Recommendations for Nigeria

Drawing on this research findings, the following evidence-based recommendations are proposed

1. **Upgrade Cyber-Forensic Infrastructure:** This involve establishing and modernising EFCC cyber-forensic laboratories with specialised equipment and trained personnel. Ensuring each zonal command has access to digital forensics such as; mobile extraction, blockchain tracing, will improve case buildup. This aligns with the study's finding that resource constraints (labs/tools) limit effective investigations (Awodiran et al., 2023; UNODC, 2025).
2. **Mandate Bank–Forensic Collaboration:** This require banks to integrate fraud analysts into AML units that collaborate directly with EFCC/CBN. For example, suspicious transaction reports related to dating platforms should be flagged to a joint task force. Literature shows that combining transactional data with

online threat intel as presented in Theme 5 in table 4 above, greatly enhances detection; thus, formalising such collaboration, supported by regulators would close a major gap (Reuters, 2024).

3. **Strengthen Legal Frameworks:** Amend laws to facilitate electronic evidence and cross-border cooperation. For instance, updating the Evidence Act to explicitly accept blockchain and digital traces will help courts. According to Interpol (2025), weak evidence laws hinder prosecution, and enacting agreements for sharing SIM-registration and KYC (know-your-customer) data between NCC, banks, and EFCC will also aid tracking.
4. **Youth Education and Ethics Programs:** There is need to scale up nationwide digital literacy campaigns to target youth, and focus on the ethics and consequences of cyber-fraud. This study discovered that many perpetrators are first-time youth offenders, so incorporating cyber-ethics into curricula and TV/radio programs as partially done in EFCC's school clubs, can help alter the social narrative that online fraud is easy money.

**Implications for Policy and Practice**

This study has several implications for researchers, policymakers, and practitioners. First, it highlights the necessity of evidence-based policy. This research integrated framework is grounded in empirical patterns (themes), and should guide investments in cyber-policing. Therefore, policymakers should prioritise funding for forensic units and AI tools where the research analysis found the highest payoff. Second, international policy must recognise Nigeria's unique position. In the sense that the demonstrated cross-border nature of these scams implies that Nigeria should take a leadership role in regional cybercrime initiatives e.g. through ECOWAS, and advocate for global conventions, like joining the Budapest Convention to bolster legal support. Third, the study suggests that anti-fraud efforts must span disciplines i.e. financial regulators, law enforcement, and IT security teams need joint training programs. The codes under "Detection & Forensic Tools" imply that siloed intelligence is ineffective, thus, agencies must be incentivised via policy or funding to collaborate.

**Future Research**

While this study provides a comprehensive analysis, several areas merit further research:

- **Behavioural Analysis of Perpetrators:** Ethnographic or psychological studies on why Nigerian youths join romance scams. This could build on Lazarus et al. (2025) research, and could inform prevention strategies beyond law enforcement.
- **Effectiveness of Integrated Systems:** Pilot studies testing parts of the proposed framework e.g. AI risk-scoring models or OSINT fusion platforms in Nigeria, would validate and refine the approach before national rollout.
- **Victim Support and Restitution:** Also, research on how victims, especially within Nigeria recover from romance scams, and how financial restitution could be improved, is needed. Aborisade et al. (2024) discuss victims' experiences, but policy responses to victim losses remain under-studied.

# REFERENCES

1. Aborisade, R. A., Ocheja, A., & Okuneye, B. A. (2023). 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. https://doi.org/10.1016/j.jeconc.2023.100044
2. Adejumo, A. P., & Ogburie, C. P. (2025). Forensic accounting in financial fraud detection: Trends and challenges. International Journal of Science and Research Archive, 14(3), 1219–1232. https://doi.org/10.30574/ijsra.2025.14.3.0815
3. Adeyinka, T. Y., & Ugwuku , V. O. (2023). A SOCIOECONOMIC UNDERPINNINGS OF "YAHOO-YAHOO" EXPLOITS IN LAGOS, NIGERIA. KIU Interdisciplinary Journal of Humanities and Social Sciences, 4(2), 59–72. https://kijhus.kiu.ac.ug/article-view.php?i=225&t=a-socioeconomic-underpinnings-of-yahoo-yahoo-exploits-in-lagos-nigeria

4. Ahmed, S. K., Mohammed, R. A., Nashwan, A. J., Ibrahim, R. H., Abdalla, A. Q., Ameen, B. M. M., & Khidhir, R. M. (2025). Using Thematic Analysis in Qualitative Research. Journal of Medicine, Surgery, and Public Health, 6(6), 100198. ScienceDirect. https://doi.org/10.1016/j.glmedi.2025.100198
5. Al-Khater, W. A., Al-Ma'adeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive Review of Cybercrime Detection Techniques. IEEE Access, 8(1), 1–1. https://doi.org/10.1109/access.2020.3011259
6. Auwal, A. M., & Lazarus, S. (2025). Experiences of local victims of Yahoo Boys' socio-economic cybercrimes in Nigeria. Discover Psychology, 5(1). https://doi.org/10.1007/s44202-025-00479-5
7. Awodiran, M. A., Ogundele, A. T., Idem, U. J., Anwana, & Emem, O. (2023). Digital Forensic Accounting and Cyber Fraud in Nigeria. Conference: 2023 International Conference on Cyber Management and Engineering (CyMaEn). https://doi.org/10.1109/cymaen57228.2023.10050992
8. Ayton, D., & Tsindos, T. (2023, March 21). Chapter 2: Foundations of qualitative research – paradigms, philosophical underpinnings. Qualitative Research – a Practical Guide for Health and Social Care Researchers and Practitioners; Monash University Library. https://oercollective.caul.edu.au/qualitative-research/chapter/2/
9. Bilz, A., Shepherd, L. A., & Johnson, G. I. (2023). Tainted Love: a Systematic Literature Review of Online Romance Scam Research. Interacting with Computers, 35(6). https://doi.org/10.1093/iwc/iwad048
10. Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., & Varese, F. (2024). Mapping the global geography of cybercrime with the World Cybercrime Index. PloS One, 19(4), e0297312–e0297312. https://doi.org/10.1371/journal.pone.0297312
11. Button, M., Lazarus, S., Hock, B., Sabia, J., Gilmour, P., & Pandey, D. (2025). Nigerian confraternities and mass cross-border fraud. Trends in Organized Crime. https://doi.org/10.1007/s12117-025-09576-2
12. Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W.-J. (2021). Cybercrime Threat intelligence: a Systematic multi-vocal Literature Review. Computers & Security, 105(1), 102258. https://doi.org/10.1016/j.cose.2021.102258
13. Chukwuemeka, U. U., & Ernest, N. I. (2025). Cybercrime and national security in Nigeria. British Journal of Interdisciplinary Research, 2(7), 182–196. https://doi.org/10.31039/bjir.v2i7.63
14. Chukwunonyerem, J., Albert, U., & Nelson-praise, K. (2025). YOUTHS AND YAHOO TRENDS, IMPLICATION EFFECTS AND SOLUTIONS. Impact International Journals and Publications, 1(issue 4), 411–424. https://impactinternationaljournals.com/publications/index.php/ojs/article/view/154
15. Duary, S., Choudhury, P., Mishra, S., Sharma, V., Deepak Dasaratha Rao, & Adedapo Paul Aderemi. (2024). Cybersecurity Threats Detection in Intelligent Networks using Predictive Analytics Approaches. Nternational Conference on Innovative Practices in Technology and Management (ICIPTM), 1-5. https://doi.org/10.1109/iciptm59628.2024.10563348
16. EFCC. (2025). EFCC Busts Cybercrime, Romance Fraud Syndicate in Lagos, Arrests Scores of Foreign Nationals – THISDAYLIVE. Thisdaylive.com. https://www.thisdaylive.com/2024/12/17/efcc-busts-cybercrime-romance-fraud-syndicate-in-lagos-arrests-scores-of-foreign-nationals/
17. Egielewa, P. E. (2022). Yahooism or Internet Fraud in the Nigerian Higher Education System. Journal of Ethics in Higher Education, 1, 75–101. https://doi.org/10.26034/fr.jehe.2022.3378
18. Hasham, S., Joshi, S., & Mikkelsen, D. (2020). Financial crime and fraud in the age of cybersecurity. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Financial%20crime%20and%20fraud%20in%20the%20age%20of%20cybersecurity/Financial-crime-and-fraud-in-the-age-of-cybersecurity.pdf
19. Idris, F., Ashuri, A., & Purnamasari, P. (2025). Forensic Analysis Of A Check Forgery Case: Issues And Implications For Strengthening Internal Control Systems. Jurnal Sosial Humaniora Dan Pendidikan, 4(3), 530–538. https://doi.org/10.55606/inovasi.v4i3.4529
20. Idris, F., Latif, Y., & Purnamasari, P. (2025). Early Detection and Prevention of Skimming in Digital Financial Systems: A Forensic Accounting Approach in the Era of Technological Transformation. Inovasi : Jurnal Sosial Humaniora Dan Pendidikan.
21. Ijiga, O. M., Idoko, I. P., Ebiega, G. I., Olajide, F. I., Olatunde, T. I., & Ukaegbu, C. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk

assessment and fraud prevention. Open Access Research Journal of Science and Technology, 11(1), 001–004. https://doi.org/10.53022/oarjst.2024.11.1.0060

22. INTERPOL. (2025). New INTERPOL report warns of sharp rise in cybercrime in Africa. Interpol.int. https://www.interpol.int/en/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa
23. Jaishankar, K. (2007). Establishing a Theory of Cyber Crimes. International Journal of Cyber Criminology, 1(2). https://www.cybercrimejournal.com/pdf/Editoriaijccjuly.pdf
24. Lazarus, S., Button, M., Garba, K. H., Soares, A. B., & Hughes, M. (2025). Strategic Business Movements? The Migration of Online Romance Fraudsters from Nigeria to Ghana. Journal of Economic Criminology, 100128. https://doi.org/10.1016/j.jeconc.2025.100128
25. Lazarus, S., Owen, F., & Soares, K. (2024). Establishing the particularities of cybercrime in Nigeria. University of Portsmouth. https://researchportal.port.ac.uk/en/studentTheses/establishing-the-particularities-of-cybercrime-in-nigeria/
26. Loggen, J., Moneva, A., & Leukfeldt, R. (2024). A systematic narrative review of pathways into, desistance from, and risk factors of financial-economic cyber-enabled crime. Computer Law & Security Review, 52, 105858. https://doi.org/10.1016/j.clsr.2023.105858
27. Mtisi, S. (2022). The Qualitative Case Study Research Strategy as Applied on a Rural Enterprise Development Doctoral Research Project. International Journal of Qualitative Methods, 21, 1–13. Sagepub. https://doi.org/10.1177/16094069221145849
28. Naeem, M., Ozuem, W., Howell, K., & Ranfagni, S. (2023). A step-by-step Process of Thematic Analysis to Develop a Conceptual Model in Qualitative Research. International Journal of Qualitative Methods, 22(1), 1–18. https://doi.org/10.1177/16094069231205789
29. Ogayi, C. O. (2025). Internet Fraud, "Yahooism", and Youth Enterpreneurship Development: A Study of Nigeria. International Journal of Research and Innovation in Applied Science, X(II), 80–89. https://doi.org/10.51584/ijrias.2025.1002007
30. Ogundele, A. T., Awodiran, M. A., Idem, U. J., & Anwana, E. O. (2023, January 1). Cybercrime Activities and the Emergence of Yahoo Boys in Nigeria. IEEE Xplore. https://doi.org/10.1109/CyMaEn57228.2023.10051083
31. Okosun, O., & Ilo, U. (2022). The evolution of the Nigerian prince scam. Journal of Financial Crime. https://doi.org/10.1108/jfc-08-2022-0185
32. Oluyide, S. E. (2025). The Impact of Forensic Accounting Techniques in Mitigating Electronic Fraud in Nigeria's Deposit Money Banks. Journal of Forensic Accounting Profession, 5(1), 43–63. https://doi.org/10.2478/jfap-2025-0003
33. Pervin, N., & Mokhtar, M. (2022). The Interpretivist Research Paradigm: A Subjective Notion of a Social Context. ResearchGate; Human Resource Management Academic Research Society. https://doi.org/10.6007/IJARPED/v11-i2/12938
34. Reuters. (2024, December 16). Almost 800 arrested over Nigerian crypto-romance scam. Reuters. https://www.reuters.com/world/africa/almost-800-arrested-over-nigerian-crypto-romance-scam-2024-12-16/
35. Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. Journal of Big Data, 11(1), 1–38. https://doi.org/10.1186/s40537-024-00957-y
36. 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 - LSE Research Online. Lse.ac.uk. http://eprints.lse.ac.uk/127725/1/ACCEPTED_COPY_Love_Lies_and_Larceny.pdf
37. Soares, A., & Lazarus, S. (2024). Criminal Justice Studies A Critical Journal of Crime, Law and Society ISSN: (Print) ( Examining fifty cases of convicted online romance fraud offenders. https://eprints.lse.ac.uk/126265/1/Examining_fifty_cases_of_convicted_online_romance_fraud_offenders.pdf
38. Tandana, E. A. (2022). AMID THE THREAT OF CYBERCRIME. QUAERENS Journal of Theology and Christianity Studies, 4(2), 129–147. https://doi.org/10.46362/quaerens.v4i2.214
39. Tenny, S., Brannan, J., & Brannan, G. (2022, September 18). Qualitative Study. National Library of Medicine; StatPearls Publishing. https://www.ncbi.nlm.nih.gov/books/NBK470395/

40. Thumboo, S., & Mukherjee, S. (2024). Digital romance fraud targeting unmarried women. Discover Global Society, 2(1). https://doi.org/10.1007/s44282-024-00132-x
41. Ugwu, C. N., & Hyginus, V. (2023, January). Qualitative Research. ResearchGate. https://www.researchgate.net/publication/367221023_Qualitative_Research
42. UNODC. (2025). UNODC Presents Landmark Cybercrime Assessment to Stakeholders. United Nations : UNODC Country Office Nigeria. https://www.unodc.org/conig/en/stories/unodc-presents-landmark-cybercrime-assessment-to-stakeholders.html
43. Vaismoradi, M., & Snelgrove, S. (2020). Theme in Qualitative Content Analysis and Thematic Analysis. Forum Qualitative Sozialforschung / Forum: Qualitative Social Research, 20(3). http://www.qualitative-research.net/index.php/fqs/article/view/3376/4470
44. Wariboko, O. P. C., & Nwanyanwu, F. C. (2024). Dark Side of Connectivity: A Socio-Ethical Exploration of Internet Fraud and Nigerian Youth. Àgídìgbo: ABUAD Journal of the Humanities, 12(1), 89–104. https://doi.org/10.53982/agidigbo.2024.1201.06-j
45. Yin, E. (2018). Yin 2018 Case Study Research And Applications. Bookstation.org. https://bookstation.org/book/yin-2018-case-study-research-and-applications-4982461

# APPENDICES

## Appendix I: Bibliography of the key, main included sources

1. Soares, A.B. & Lazarus, S. (2024). Examining fifty cases of convicted online romance fraud offenders. Criminal Justice Studies, DOI:10.1080/1478601X.2024.2429088eprints.lse.ac.uk.
2. 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, DOI:10.1080/01639625.2025.2482824eprints.lse.ac.uk.
3. Lazarus, S., Button, M., Garba, K.H., Soares, A.B. & Hughes, M. (2025). Strategic Business Movements? The Migration of Online Romance Fraudsters from Nigeria to Ghana. Journal of Economic Criminology, 7(1):100128researchgate.net.
4. Aborisade, R.A., Ocheja, A. & Okuneye, B.A. (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, 3:100044doaj.org.
5. Auwal, A.M. & Lazarus, S. (2025). Experiences of local victims of Yahoo Boys' socio-economic cybercrimes in Nigeria. Discover Psychology, 5:161link.springer.com.
6. Garba, K., Lazarus, S. & Button, M. (2024). Cybercrime displacement and digital crime: Investigating the institutionalization of Nigerian online fraud. Crime Science, 13(16). (In press.)
7. UNODC (2025). Nigeria's First National Cybercrime Assessment Report. United Nations Office on Drugs and Crime – Press Release, Dec 2025unodc.org.
8. Interpol (2025). Africa Cyberthreat Assessment 2025. Interpol (report summary)interpol.int.
9. Reuters (2024). Almost 800 arrested over Nigerian crypto-romance scam. Reuters, Dec 16, 2024reuters.co

Each of the above is cited in the analysis below. (Further journal articles, conference papers, and expert reports were also consulted; only the most relevant are listed here.