Journal of Economic Criminology 11 (2026) 100205

Contents lists available at ScienceDirect

Journal of Economic Criminology

journal homepage: www.journals.elsevier.com/journal-of-economic-criminology

Cybercrime and socioeconomic realities: Perpetrators' perspectives from Ghana

Nii Barnor Jonathan Barnor [a], Eric Ansong [b,*], Sheena Lovia Boateng [c]

[a] Department of Management Sciences, University of Education, Winneba, Ghana
[b] Department of Information Technology and Data Analytics, University of Ghana, Ghana
[c] Department of Marketing and Entrepreneurship, University of Ghana, Ghana

ARTICLE INFO

Keywords:
Romance Fraud
E-commerce fraud
Identity theft
Credit card fraud
Perpetrators

ABSTRACT

This study, grounded in Rational Choice Theory, explores the strategies and decision-making processes of online romance fraud perpetrators in Ghana. Using a qualitative approach, thirteen individuals involved in such fraud were interviewed through purposive and snowball sampling. Data were analysed using Miles and Huberman's transcendental realism. Findings reveal that perpetrators use deceptive online personas, emotional manipulation, and victims as intermediaries in broader cybercrimes like e-commerce fraud, identity theft, and credit card fraud. Their actions reflect rational evaluations of risk and reward, shaped by socio-economic factors such as poverty, unemployment, and lack of education. The study underscores the need for targeted policy interventions and offers rare insights from the perpetrators' perspective in a developing country context.

1. Introduction

The advancements in Information and Communication Technologies (ICTs) have catalysed efficiency across diverse public and private sectors. Simultaneously, the progressive development of ICTs has enhanced aspects of societal and individual lives, including e-commerce, banking, education, and collaborative undertakings (Bibri, 2019). In numerous nations, the provision of universal service and accessibility to ICTs constitutes a paramount policy issue, often encapsulated in the legislative framework governing the sector (Pamungkas and Yusuf, 2019; Manh et al., 2016). Nonetheless, these technological advances bring forth novel and evolving challenges for both individuals and nations to grapple with, prominent among which is cybercrime. This term encompasses the utilisation of computers and associated technologies, inclusive of the internet, to perpetrate crimes such as fraud, child pornography, identity theft, and privacy invasion (Cross, 2020). Despite the borderless nature of these offenses, one crime appears to resonate particularly with West Africa: online romance fraud. For instance, a cross-border investigation by Interpol led to more than 100 arrests and the seizure of over 2 million euros by various West African criminal groups scamming internet users (Reuters, 2023). It is also asserted that online romance scams emanating from West Africa have generated into a global problem, affecting individuals, organisations, and countries, especially in Western societies (Whitty, 2018a).

Romance fraud, also known as dating and relationship fraud or sweetheart swindles, has a devastating impact on the lives of millions of victims worldwide (Lazarus et al., 2023). Under the guise of a legitimate relationship, offenders exploit emotional connections with victims mostly for financial gain (Barnor et al., 2020). For instance, in 2016 alone, 3889 victims in the United Kingdom reported losses of £ 39 million, 15,000 victims in the United States reported losses exceeding USD$230 million, 831 victims in Canada reported losses of almost CAD $21 million, and 1017 victims in Australia reported losses of over AUD $25.5 million (Monroe, 2018). Globally, the Federal Trade Commission (2021) reported a new peak in estimated losses from romance scams, reaching $304 million in 2020, a nearly 50 % increase from the preceding year. These figures underscore the substantial financial losses incurred by victims. Romance fraud consistently ranks among the highest categories of fraud for financial loss, particularly in Australia and Sub-Saharan Africa, where it has been in the top two categories of loss for the past decade (Yar and Steinmetz, 2023; Cross, 2020). Beyond the financial losses, victims of romance fraud must also grapple with social, psychological, and emotional harms (Cross, 2020). These nonfinancial consequences can include shattered trust, feelings of betrayal, humiliation, and a loss of self-esteem (Whitty, 2018b). For instance, the romantic imagery created by scammers can lead to post-traumatic stress

* Corresponding author.
E-mail addresses: jnbbarnor@uew.edu.gh (N.B.J. Barnor), eransong@ug.edu.gh (E. Ansong), slboateng@ug.edu.gh (S.L. Boateng).

https://doi.org/10.1016/j.jeconc.2025.100205
Received 31 October 2025; Received in revised form 10 December 2025; Accepted 11 December 2025
Available online 14 December 2025

disorder-like symptoms, leaving victims emotionally attached even after the deception is revealed (Ianzito, 2022). Additionally, sextortion, where scammers threaten to share explicit photos, has tragically led to suicides among targeted individuals, especially teenagers (Federal Trade Commission, 2021).

Despite the widespread impact on victims worldwide and the seriousness of romance fraud, there is still limited research specifically focused on gaining a better understanding. While some works have emerged in this area (e.g., Cross and Holt, 2021; Hui et al., 2017; Hutchings and Holt, 2018; Tambe Ebot, 2023), significant gaps remain to be explored. For instance, the dynamics of relationships between victims and offenders arguably appear not well understood, and the effects of romance fraud are rarely discussed, especially within the West African context. Paradoxically, the handful of studies on the topic, however, focused on developed countries' contexts, where such economies are arguably more formalised or structured. Cross and Layt (2022), for instance, examined how offenders use non-violent tactics to ensure compliance, focusing on 21 Australian romance fraud victims. Therefore, further research is crucial to comprehensively address this complex and evolving phenomenon, especially from the context of a developing economy within West Africa.

To further elucidate the decision-making processes of perpetrators in online romance fraud, this study draws on Rational Choice Theory (RCT). RCT posits that individuals engage in criminal behaviour after a careful evaluation of the potential risks and rewards (Cocozza, 2023). In the context of online romance fraud, perpetrators are likely to assess the benefits of financial gain against the risks of detection and punishment (Cross, 2020). This theory provides a framework for understanding how these offenders rationalise their actions, choosing strategies that maximise their success while minimising potential repercussions (Cornish and Clarke, 2016). By applying RCT, this study offers insights into the calculated decisions behind the various tactics employed by fraudsters, shedding light on how the socio-economic conditions within a developing country may influence these choices (Kuo and Tsang, 2023). This theoretical lens is essential for comprehending not only the motivations behind romance fraud but also the adaptive strategies that perpetrators use to exploit victims effectively (Cocozza, 2023).

In addition, academic research reveals a gap pertaining to offender-side data (e.g., Hui et al., 2017; Hutchings and Holt, 2018), specifically in relation to the techniques employed by perpetrators to identify and exploit their victims (e.g., Cross and Holt, 2021). This gap is ostensibly attributable to the challenges involved in data collection from offenders, as intimated by Hutchings and Holt (2018). Despite the apparent dearth of primary offender research, extant studies have relied on victim data to delineate the stratagems used by perpetrators to exploit their victims (e.g., Cross and Holt, 2021; Whitty, 2018b; Buchanan and Whitty, 2014). In this context, a study by Cross and Holt (2021) highlighted a research gap warranting future exploration. Their study, centred on the frequency and methods of criminals using military profiles and narratives to deceive victims through romance fraud schemes, found that while the military identity and narrative can be invoked to justify monetary requests, there is insufficient evidence to categorise it as a distinct variant of romance fraud. Similarly, Tambe Ebot (2023) examined generally how advance fee fraud (AFF) scammers build their criminal expertise over time. Despite some anecdotal evidence of the tactics employed by cybercriminals globally, empirical research examining romance fraud strategies, particularly from the perpetrator's perspective, remains scarce. Although the field is expanding, recent studies (e.g., Button et al., 2025; Abubakari, 2024; Button et al., 2024) show that romance fraud continues to evolve in scope and sophistication. Extant studies published in a dedicated special issue on romance fraud by the Journal of Economic Criminology highlight the complex tactics used by offenders, the emotional and financial vulnerabilities of victims, and the links between romance fraud and other forms of online deception (e.g., Abubakari, 2024; Button and Carter, 2024). These studies also emphasise the need for research across different cultural and technological contexts. Hence, Cross and Holt (2021) underscored the need for future research into the strategies adopted by cybercriminals on dating websites and the nefarious methods they employ to exploit vulnerable victims.

This study specifically seeks to answer the question: *What strategies do perpetrators of online romance fraud employ?* This question holds profound significance as it offers an opportunity to delve into the minds of these offenders, gaining invaluable insights directly from their perspective. The elucidation of these strategies stands as a pivotal step forward, offering a firsthand account that will provide researchers, practitioners, and policymakers with invaluable insights. Again, by comprehensively understanding the tactics employed by these perpetrators, stakeholders will better equip themselves to combat the scourge of romance fraud, fortify preventive measures, and formulate more effective policies to safeguard individuals and communities against such deceptive practices. The remaining sections of this paper are organised as follows: The subsequent section undertakes a review of the literature on romance fraud, followed by a detailed account of the study's data collection and analysis methodology. The study's analysis and discussion of findings are presented next. The study ends with the Conclusions and Recommendations section.

2. Literature review

2.1. Online romance frauds

Offenders involved in romance fraud manipulate and exploit their victims by crafting an illusion of a genuine relationship, which ultimately proves to be false (Cross, 2020). Whitty (2019) observed that the end goal portrayed to victims is often not the receipt of large sums of money but the prospect of a committed relationship. Although extant research on romance fraud has shed light on the motivations and techniques of romance scam offenders (Whitty, 2013; Barnor et al., 2020), few have delved into the complexities inherent in the perpetration of these scams. Predominantly, existing studies have focused on the grooming and persuasion techniques employed by fraudsters (Anesa, 2020; Whitty, 2013, 2019; Cross et al., 2018). Despite their value, only a handful have critically examined evidence from the perspective of the offenders, with a significant amount of the literature relying on sources such as victims of romance fraud (Kopp et al., 2015), dating platforms, or law enforcement agents and agencies (Tan and David, 2013).

Kopp et al. (2015), for instance, conducted an exploratory study using qualitative analysis of fraudulent profiles from an international dating website. They posited that the success factors found in legitimate relationships contribute to the success of romance scams. The study indicated that "personal affinities related to personal romantic imaginations, which are described by personal love stories, play an important role in the success of a romance scam." In a similar vein, Cross et al. (2018) sought to understand how romance fraud intersects with other forms of online fraud and non-physical forms of abuse. They used semi-structured face-to-face interviews with 21 Australian victims of romance fraud who had reported online dating scams to the Australian Competition and Consumer Commission (ACCC) Scamwatch website. The findings revealed considerable overlap in the types of psychological maltreatment present in both romance fraud and domestic violence, notwithstanding the absence of a physical relationship.

Whitty (2013) conducted a multi-layered study, analysing posts from a public online support group, carrying out in-depth interviews with victims of romance fraud, and interviewing a Serious Organised Crime Agency officer to delineate the anatomy of online romance fraud. The study identified four primary trajectories of the scam and five distinct stages. In a subsequent study, Whitty (2019) expanded the romance scam trajectories from five to seven stages, examining the persuasive techniques employed by scammers and evaluating whether existing theories on persuasion adequately explain why victims are ensnared by romance fraud.

The first step of Whitty's (2013), (2019) model involves the victim

being motivated to find an ideal lover online. The victim then encounters an enticing profile of the "ideal lover," who tends to be the perpetrator. The grooming process and the sting stage, as described in the earlier model, then ensue. During the grooming stage, offenders assess the viability of stolen credit cards by making small purchases, such as buying roses or other petty gifts for their victims. Whitty (2013) sees "sting" as one of the final phases of a scam. During this phase, the scammer manipulates the victim into sending money or providing financial assistance.

Adding to this body of work, more recent studies have delved deeper into the mechanics and impacts of online romance scams. For instance, a study by Cross and Layt (2022) investigated the strategies employed by scammers to establish trust and emotional connection with their victims. The study found that the scammers often employed "mirroring" techniques, where they would replicate the emotional state, interests, and desires of their victims, thereby creating an illusion of compatibility and shared experiences. Moreover, in a study conducted by Lazarus et al. (2023), the authors argue that traditional cybersecurity measures are inadequate in preventing romance scams.

While the foregoing studies underscore the evolving nature of romance scams and the need for continued research into this form of cybercrime, it is essential to note that the studies did not appear to combine data from primary offenders. The studies primarily depended on victims' accounts and secondary data sources. In West Africa, emerging work has examined broader cyber-fraud activities in the region. Button et al. (2025) identify how economic pressures, peer networks, and digital access influence involvement in cyber-frauds in Ghana and Nigeria. Similarly, Button et al. (2024) describe the fraud infrastructures that facilitate online scams across several countries. While these studies provide valuable regional insights, they rely largely on secondary data and do not offer detailed, first-hand accounts from offenders.

The present study contributes to addressing this gap by drawing directly on the experiences of self-identified perpetrators in Ghana. Given the difficulty of accessing this population, offender-based qualitative research remains rare. By centring offenders' own narratives, this study provides new insight into how romance fraud is organised, rationalised, and executed in the Ghanaian context.

2.2. An emerging cyberculture among Ghanaian youths

The early 2000s witnessed a significant growth in internet penetration in Ghana. This led to the proliferation of internet cafes, providing an affordable alternative to dedicated dial-up internet access for individuals unable to shoulder the associated costs. The increasing popularity of these cafes was paralleled by the emergence of a youth gang culture congregating at these venues to engage in various discussions. These cafes cater to a wide demographic spectrum with diverse interests. For instance, school pupils utilise these facilities for homework-related internet access. Junior and senior high school students frequent these venues for research purposes (Warner, 2011). However, these cafes also attract individuals with more nefarious intentions, making them a bustling hub of patrons with varying objectives.

Furthermore, internet cafes serve as recreational venues for younger children, where they purchase browsing time to play games and watch YouTube videos. Through these activities, they learn to connect with friends on Facebook and other social media platforms and gradually develop a habit of benefiting from these friendships by soliciting petty gifts. Livingstone and Helsper (2007) and Warschauer et al. (2014), for instance, have underscored the importance of internet cafes as access points for young people to go online, socialise, and engage in various online activities.

Contrasting with the use of internet cafes by students and other demographics, these public spaces particularly appeal to young individuals who spend time engaging in discussions and arguments on topics such as football, music, and entertainment. This group gradually forms a unique cyber-culture, often fostered by the round-the-clock operation of some cafes (Romanska, 2012), colloquially known among patrons as "twenty-four." Boyd (2008) and Ellison et al. (2007) allude to the various ways in which young people use social media to include identity expression, social connection, and relationship maintenance. It is within these social interactions that young individuals, driven by needs, request cyber-deviant peers to illegally procure items for them. Upon fulfilment of these requests, the act is repeated, with these individuals progressively receiving instruction on the fundamentals of deviant cyber-activities. It is through such interactions that cyber gangs are formed to compensate for each other's shortcomings.

2.3. Theoretical review

2.3.1. The rational choice theory (RCT)

Rational Choice Theory (RCT) serves as a foundational framework for understanding the decision-making processes of individuals engaged in activities, including online romance fraud. RCT posits that individuals make decisions based on a rational evaluation of the potential risks and rewards associated with their actions (Clarke and Cornish, 2017). This theory assumes that offenders are rational actors who seek to maximise their benefits while minimising potential costs.

In the context of online romance fraud, perpetrators are likely to assess the benefits of financial gain against the risks of detection and punishment (Cross et al., 2021). The anonymity provided by the internet reduces the perceived risk of being caught, making online platforms an attractive medium for fraudsters. By applying RCT, this study aims to elucidate how these offenders rationalise their actions and choose strategies that maximise their success while minimising potential repercussions.

- **The decision-making processes:** RCT provides a framework for understanding the calculated decisions behind the various tactics employed by fraudsters. These decisions are influenced by several factors, including the socio-economic conditions within a developing country, which may drive individuals to engage in fraudulent activities as a means of financial survival (Kuo and Tsang, 2023). The theory suggests that offenders weigh the potential financial rewards against the likelihood of detection and the severity of potential punishments.
- **Adaptive strategies:** Fraudsters continuously adapt their strategies to exploit victims effectively. This adaptability is a key component of RCT, as it highlights the dynamic nature of criminal decision-making. Offenders may employ various tactics, such as creating convincing online personas, manipulating victims' emotions, and using sophisticated communication techniques to build trust and extract money (Cocozza, 2023). Understanding these adaptive strategies through the lens of RCT provides valuable insights into the motivations and behaviours of romance fraud perpetrators.
- **Socio-economic influences:** The socio-economic conditions within a developing country can significantly influence the decision-making processes of fraudsters. High levels of unemployment, poverty, and limited access to legitimate economic opportunities may push individuals towards criminal activities as a means of financial gain (Cornish and Clarke, 2016). RCT helps to contextualise these socio-economic factors, offering a comprehensive understanding of how they shape the rationalisations and actions of online romance fraudsters.

By applying Rational Choice Theory, this study offers a nuanced understanding of the decision-making processes behind online romance fraud. RCT provides a robust framework for analysing how perpetrators rationalise their actions, choose adaptive strategies, and are influenced by socio-economic conditions. This theoretical lens is essential for comprehending not only the motivations behind romance fraud but also the adaptive strategies that perpetrators use to exploit victims

effectively.

3. Research methods

This study employed a qualitative case study research design to fulfil its objective of examining the strategies perpetrators of online romance fraud employ in their operations. The qualitative case study approach was chosen for its ability to provide an in-depth understanding of complex phenomena within their real-life contexts (Yin, 2018). This design is particularly suitable for exploring the nuanced behaviours and decision-making processes of individuals involved in cybercrime, as it allows for a comprehensive examination of the contextual factors influencing their actions. By focusing on a specific case, this study can uncover detailed insights that might be overlooked in broader quantitative studies, thereby offering a richer, more holistic understanding of the subject matter.

3.1. Data collection

Aligned with qualitative research methodologies, this study utilised purposive sampling and semi-structured, open-ended interviews as primary data collection methods (Dudwick et al., 2006). In addition to interviews, participant observation, and document and artifact analysis were employed. The interview guide for the semi-structured interviews was developed based on insights gleaned from existing literature and the Rational Choice Theory (RCT) (See Appendix).

Data were accumulated over five years (2018–2023) from individuals involved in cybercrime. Given the inherent challenges associated with gathering data from cybercrime offenders, the initial respondent (a local internet café operator) was identified through purposive sampling technique. This operator subsequently facilitated the identification of potential participants who expressed willingness to partake in the study. Thereafter, the snowball sampling technique was deployed to identify additional respondents. A total of thirteen respondents (all male) were ultimately interviewed and observed. Prior to data collection, all participants were assured of the confidentiality and anonymity of their identities.

The initial phase of data collection entailed a comprehensive examination of the cybercrime landscape in Ghana to identify prevalent offenses (see Boateng and Barnor, 2020). It emerged at this juncture that amidst the burgeoning cybergang communities, romance scams appeared to be the most predominant form of cybercrime. A noteworthy event during the second phase of data collection was the formation of a syndicate by four of the participants (see Table 1). This syndicate was chosen as the case for this study, considering the complexities of tracking self-identified independent offenders.

During the initial data collection, it became evident that the cybercriminals engage in a wide range of cyber offenses. Notably, romance scams emerged as a top priority for these offenders. Alongside romance scams, other crimes such as credit card fraud, identity theft, deceit, and forgery were also prevalent. Initially, the cybergang operated independently, frequently visiting a community-based internet café. However, as the investigation progressed, four out of the initial eight perpetrators formed a syndicate. This group shifted their operations to one member's apartment. Table 1 outlines the characteristics of both the cybergang, and other self-identified individual perpetrators studied.

3.2. Data analysis techniques

For data analysis, this study adopted Miles and Huberman's (1994) transcendental realism technique as presented in Fig. 1. Again, the analysis was guided by RCT, which provided a theoretical lens to interpret the data. Following data collection, this technique prescribes three additional stages: data reduction, data display and conclusion drawing, and verification.

As per Miles and Huberman's (1994) transcendental realism technique, data reduction involves the selection, focusing, simplification, abstraction, and transformation of raw data from field notes or transcriptions. The collected raw data were organised through a coding process, reducing the data into meaningful segments, and assigning labels for subsequent analysis. Tables and diagrams were utilised to present data, thereby minimising the data's volume without sacrificing their central importance. Potential conclusions were identified early in the data collection and analysis process. However, these preliminary findings were considered provisional due to their lack of detailed substantiation. These findings were revisited and refined during the analysis phase after the completion of data collection and reduction.

4. Data presentation and analysis

As previously indicated, data gathered over the timeframe revealed a plethora of scams that perpetrators engage in. Furthermore, as much as romance scams return some profit to the offenders, it appears that it is

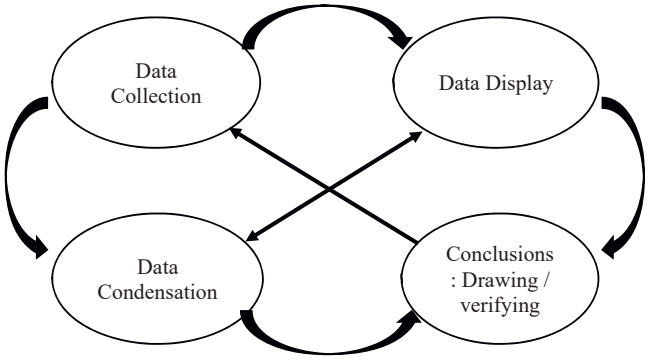

Fig. 1. Miles and Huberman's (1994) Data Analysis Approach.

Table 1
Characteristics of the cybergang and self-identified individual perpetrators.

Pseudonyms	Age	Educational Qualification	Experience	Job Experience	Designation
John	27	Senior High School Leaver with partial IT training	9 years	-	Cybergang
Franklyn	25	Senior High School Leaver	7 years	-	
Chris	25	Senior High School Leaver	7 years	Electrician	
Lucas	26	Dropped out of senior high	6 years	-	
Zack		Senior High School Leaver	5 years	Café attendant	Self-identified independent Perpetrators
Caleb	23	Senior High School Leaver	2 years	-	
Esmond	33	Polytechnic Graduate	9 years	National Service	
Patrick (Ex perpetrator)	36	Postgraduate	12 years	Self-employed	
Noah	26	Senior High School Leaver	-	-	
Benjamin	29	Senior High School Leaver	6 years	Café attendant	
Razak	31	Post-secondary IT training	8years	-	
William	37	Polytechnic Graduate	-	Artist	
Robert	32	Secondary School Leaver	7 years	-	

merely a conduit for the perpetrators to profit from other criminal activities routed through their victims. Motives for individuals who engage in cyber-offenses vary from person to person, but the ultimate motives among the Ghanaian youth are mostly extrinsic. In this regard, any online crime they commit is aimed at generating financial gains.

Financial motivations and economic rationale: The economic drivers behind engagement in romance fraud were explicitly articulated by several participants. Franklyn, a 25-year-old with 7 years of experience, explained: *"When you finish SHS [Senior High School] and there is no job, no money for further studies, what do you do? The internet café becomes your office. You see others making money from these 'things' [fraud], and you learn. Within months, I was making more than my father who worked for 30 years as a teacher."* Similarly, John (27 years) reflected on the economic calculus: *"If I work as a security man, I get maybe 500 cedis [approximately $40] a month. With one successful 'client,' I can make $2000 or more. The risk is there, yes, but the reward… it's not comparable."* These statements underscore how perpetrators engage in rational cost-benefit analyses, weighing limited legitimate opportunities against potentially lucrative illicit gains.

Evidence from the data in relation to romance scams revealed two approaches that offenders adopt: The first is the scammer-led method, in which scammers pose as date seekers and lead and control contact with their victims. This approach seems to be the standard approach by many of the scammers and is also known in literature (e.g., Kydd et al., 2023; Wang, 2024; Cross, 2020; Whitty, 2013). The second method is the victim-led technique, in which scammers pose as young women looking for older men to date. Scammers allow victims to make demands for naked pictures and videos in exchange for money in the second approach. For example, a respondent posits, "*If they ask for pictures, I will tell them if I send ten naked pictures, you will give me $200 and if I send a video, you will give me $500 … they ask for a reduction, and I send the video or pictures, and they also send the money.*"

Strategies for building trust and emotional manipulation: Participants described sophisticated techniques for cultivating emotional connections. Lucas (26 years) detailed his approach: *"You don't just ask for money. You build a story. You become a soldier stationed abroad, lonely, looking for true love. You share 'your' dreams, ask about their day, remember small details. You make them feel special, like they're the only one."* Chris (25 years) emphasized the importance of patience and emotional investment: *"Some people think this is quick money. No. You must invest time. I have spent six months talking to one woman before the first request. You become their emotional support, their confidant. When they trust you completely, that's when you introduce the 'problem' - a medical emergency, a stolen passport, anything that needs money."* These narratives reveal how perpetrators strategically deploy empathy and relational labour to establish credibility and lower victims' defences.

The demands for naked pictures are for most of the time not explicitly done at the beginning of the relationship. Thus, "*he will send a picture like he is half-naked, and I will also send him a half-naked picture. I will not send him anything again till he asks for it, and I also start asking for the money.*" Due to the complications of feeding the victims with nude pictures downloaded from the internet, the timeframe for this method is usually shorter than the scammer-led approach. While the scammer-led approach may last for about eight to twelve months, the victim-led strategy usually starts and ends within three to four months after scammers have blackmailed victims for sexual exploitation.

Rationalizing criminal behaviour: Participants frequently employed neutralization techniques to justify their actions. Esmond (33 years), a polytechnic graduate, stated: *"These people [victims] are not innocent. They are looking for love where they shouldn't - online with strangers. And often they are married! They are cheating on their spouses. So, who is worse?"* Another participant, Benjamin (29 years), echoed this sentiment: *"The White people, they have everything. We are here struggling. If I take some of their money, it's not like I'm hurting them badly. They can recover. For us, that money changes everything."* These justifications reflect how perpetrators frame their actions as morally acceptable within their socioeconomic context, mitigating cognitive dissonance and facilitating continued engagement in fraud.

With the foregoing discussion in perspective, the periods between profile creation, stinging, and revelation (Whitty, 2013) tend to be too long regarding the time used. Therefore, scammers devise other means of profiting from the relationship while they wait to sting their victims, and that is by using the addresses of the victims as transits for e-commerce fraud. A timeline of the activities of the cybercriminals is presented in Fig. 2.

Economic Motivations and Rational Choice Analysis: Participants reported earning between $500 and $8000 monthly from romance fraud operations, with experienced syndicate members reaching the higher end of this range. These earnings significantly exceed legitimate alternatives in Ghana, where the average monthly formal sector wage is approximately $200, and even university graduates typically earn $240 to $360 monthly (Ghana Statistical Service, 2025). As John (27 years) explained: *"My brother with a degree earns 3500 cedis [$280] after five years at a bank. In one good week of 'work,' I can make triple that."* This dramatic income disparity-where fraud earnings can be 4x to 40x legitimate wages-creates powerful economic incentives that align with Rational Choice Theory's emphasis on cost-benefit calculations. Participants consciously weigh these financial rewards against perceived risks of detection, which they consider low due to limited enforcement capacity and cross-jurisdictional complexities. This economic calculus explains why romance fraud represents a rational choice for many young Ghanaians facing limited employment opportunities and economic pressures.

Organizational dynamics and skill development: The formation of the cybergang highlighted evolving professionalization. John described the syndicate's advantages: *"When we worked alone, we had limits. Together, we specialize. Franklyn is good at creating profiles, I handle the emotional conversations, Chris manages the credit card operations, Lucas coordinates shipping. We share risks, knowledge, and profits."* This division of labour demonstrates how offenders optimize efficiency through collaboration. Zack (23 years), who operated independently, acknowledged the learning curve: "*At first, I lost many potential clients because I was impatient. The experienced ones taught me - you must study your target, understand their psychology. Now I have templates for different types: lonely widows, divorced men, young professionals looking for adventure."* These accounts reveal a continuum of expertise development, with knowledge transfer occurring both informally in internet cafes and through structured collaboration in syndicates.

While cybercriminals patiently engage their would-be victims to sting them, they also participate in various forms of cyber offenses to benefit from them. The first step towards benefiting from the victims involves black-market credit card dealings. In these schemes, perpetrators engage unidentified international organised cybergroups whose specialties are in credit card fraud. Such organised groups, according to a respondent, "*hack thecarddetails from stores*" and sell the details of the card to interested cyber-offenders. Even though the cards may not contain funds on them, respondents for the study aver that *"… on average, you may not get less than $200.00 on a card.*"

Risk assessment and mitigation strategies: Participants demonstrated sophisticated risk management approaches. Robert (32 years) explained his precautions: *"I never use my real phone or personal email. Everything is bought with cash - phones, SIM cards, laptops. I change locations frequently. The apartment we use for operations is rented under a fake name."* Chris elaborated on operational security: "*We test every card with small purchases first. If it works for a $20 flower purchase, then we scale up. We never ship directly to Ghana - always through the victim first, then reship. This creates layers of separation."* These practices illustrate how offenders systematically minimize detection risks while maximizing illicit gains.

However, to ensure the true worth of the credit cards, perpetrators claim they have ways of checking – and that is by using the cards to purchase flowers to lavish their victims, also referred to as clients among the perpetrators. According to the perpetrators, the cost of the flowers is

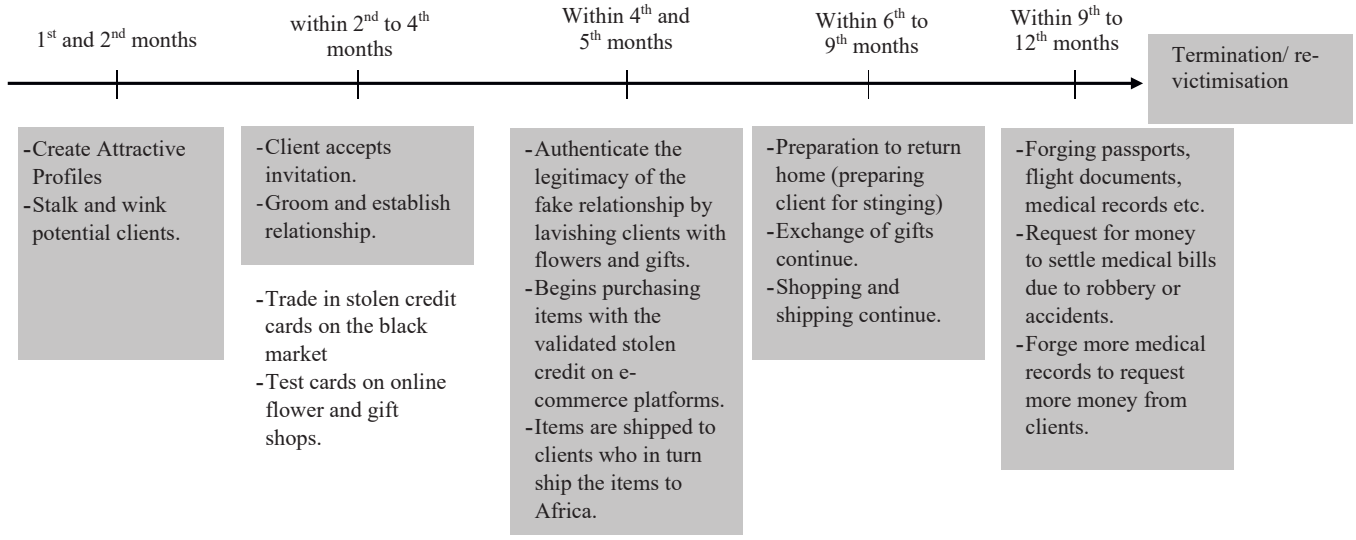

Fig. 2. Romance fraud timeline.

not so expensive, so they are easy to go by, and the stores easily accept the cards. It is worthy of note that the flower gifts sent to the clients are also meant to establish the legitimacy of the relationships.

Economic impact and lifestyle changes: The financial rewards significantly altered participants' socioeconomic standing. Patrick (36 years), a former perpetrator, reflected: *"At my peak, I was making $8000 to $10,000 monthly. I built a house for my mother, bought cars, dressed in designer clothes. Everyone respected me. But the stress… always looking over your shoulder."* Younger participants like Caleb (23 years) described more modest but transformative gains: "*My first big hit was $3000. I paid my sister's university fees, bought a generator for our house, and still had enough to invest in better equipment - new laptop, VPN subscriptions, proxy servers."* These accounts quantify the substantial economic incentives driving participation while highlighting how illicit proceeds are often redistributed within extended family networks, embedding the practice in local socioeconomic structures.

After the authenticity of the credit cards is established, offenders proceed to purchase items with the stolen credit cards on e-commerce platforms. The items are then shipped to the clients in the name of the offenders. More often than not, the victims are unable to identify the scams in the schemes of illegal shopping and shipping because they have established love relationships with perpetrators. It is worth noting that cybercriminals create profiles of military personnel (Cross and Holt, 2021), humanitarian workers (Boateng and Barnor, 2020), and oil rig workers among others and deceive victims with transnational travel lifestyles. As a result, victims are not deeply concerned about shipping items to West Africa.

Psychological adaptation and emotional management: Navigating the emotional dimensions of deception required deliberate strategies. Franklyn described compartmentalization: *"You must separate yourself from the character you play. The person talking to the victim is not you - it's a role. When the day ends, you switch off. Otherwise, the guilt will destroy you."* John acknowledged occasional moral conflict: *"There was one woman, a nurse in Canada. She was so kind, sent money for my 'mother's surgery.' Sometimes I think about her, wonder if she recovered financially. But then I remember my own family's needs."* These reflections reveal the psychological mechanisms perpetrators employ to sustain fraudulent activities despite occasional ethical dissonance, further illustrating the complex interplay between rational choice calculations and emotional experience.

5. Discussion of findings

Romance fraud perpetrators are socioeconomically driven individuals who prey on their victims' feelings of love (Wang, 2024). Owing to the advent of new techniques that criminals use to circumvent platforms ranging from dating to e-commerce, romance fraud scams seem to be flourishing in recent times (Cross, 2020). It is important to note that the commission of online romance fraud is not a linear or uniform process; rather, it encompasses varied timelines and strategies that reflect the adaptive, opportunistic, and context-dependent nature of offender decision-making. Guided by Rational Choice Theory (RCT), the data analysed in the previous section are discussed in relation to extant literature in this section.

First, the study discovers that romance fraud perpetrators engage in a multiplicity of crimes in their quest to acquire wealth. These crimes can be viewed along the lines of credit card fraud, identity theft, e-commerce fraud, forgery, and pure romance scams. Kydd et al. (2023), for instance, assert that methods by which scammers target, select, and exploit their victims vary greatly. RCT posits that offenders make calculated decisions to maximise their benefits while minimising risks, which explains the diverse criminal activities they engage in (Cocozza, 2023). Instead of following a strict structure, romance fraud is continually evolving with multiple variations at each stage of the process, as highlighted in this study. This finding is consistent with Abubakari (2024) who demonstrated that romance fraudsters operated through coordinated structures and shared learning environments that shape their modus operandi.

In cases of credit card fraud, the data analysis showed that romance fraudsters ally with illegal market credit card dealers to obtain credit card information in order to use the victims as shipping transits for illegally purchased goods on e-commerce platforms. Even though the two are unrelated, the association between credit card fraud and romance scams appears to be the starting point for romance scammers. However, the quandary is that while one offender may start with credit card fraud and work his way up to searching for victims, another may start from the opposite end of the spectrum (Sorell and Whitty, 2019). This aligns with RCT, which suggests that offenders evaluate different pathways to achieve their goals based on perceived risks and rewards as intimated by Cornish and Clarke (2016).

Existing studies on romance fraud reveal that fraudsters employ grooming tactics similar to those used by sexual offenders with children (Whitty, 2013; Whitty, 2018b; Boateng and Barnor, 2020). In online romance relationships, offenders maintain victims' commitment through poetic emails and text messages. Additionally, this paper argues

that offenders gauge the viability of stolen credit cards by purchasing small gifts (such as roses) to legitimise their relationships. Once card viability is confirmed, offenders collaborate with carding experts to bypass e-commerce platforms. This stage lies at the core of perpetrators' romance fraud schemes, as it requires time and involves uncertainty. Consequently, criminals often prioritise e-commerce fraud while simultaneously deceiving victims with promises of lasting relationships. Cross et al. (2021) support this finding, emphasising that scammers rely on persuasion techniques to deceive their victims. RCT helps explain these behaviours as rational strategies to maintain control over the victim and ensure the success of their fraudulent activities (Kuo and Tsang, 2023).

Moreover, while romance fraud on its own has drawn research attention, its relationship with e-commerce fraud appears to be an interesting starting point for academic investigations. Existing studies have found that cybercrime perpetrators collaborate with corrupt security agents and bank officials to circumvent national laws (Aransiola and Asindemade, 2011; Button et al., 2025). In order to avoid being flagged for cybercrime, the current study found that perpetrators collaborate with corrupt shipping officials to clear items shipped through their victims. This finding is corroborated by Chomariyah (2021), who carried out an investigation into the cybersecurity issues in the Straits of Malacca and Singapore (SOMS) and shed light on the complexities of cybersecurity in the shipping industry and the collaboration between perpetrators and corrupt officials in clearing items shipped through their victims. RCT provides a framework for understanding these collaborations as rational choices made to reduce the risk of detection and enhance the efficiency of their operations (Clarke and Cornish, 2017).

By applying RCT, this study provides a comprehensive understanding of the rationalisations and adaptive strategies employed by romance fraud perpetrators. It highlights how these offenders make calculated decisions to exploit their victims effectively while navigating the socioeconomic and legal landscapes of their environment.

6. Conclusions and recommendations

This paper has provided insights into the pathways of online romance fraud. It identifies emerging strategies that perpetrators use to outsmart their victims. Additionally, it offers a unique opportunity for researchers to explore both scammer-led and victim-led methods employed by the scheme.

6.1. Implications of the study

The implications of these findings extend to future research, practitioners, and policymakers.

First, the study sheds light on the multifaceted nature of romance fraud, emphasizing that perpetrators engage in a variety of criminal activities beyond pure romance scams. This suggests that efforts to combat romance fraud should not be limited to addressing only the romantic aspect but should also encompass strategies to tackle related crimes such as credit card fraud, identity theft, and e-commerce fraud. Researchers can further investigate the specific mechanisms through which these crimes intersect and how they manifest within the local context.

Second, prevention efforts must be intensified in the Western nations where most victims reside. Dating platforms, financial institutions, and law enforcement in such countries should collaborate to educate users, promote early video verification, and flag transactions linked to romance fraud. Raising victim awareness abroad directly reduces the success rate of these scams, undermining the perpetrator's risk-reward calculus.

Again, the evolving nature of romance fraud highlighted in the study underscores the need for continuous monitoring and adaptation of prevention and detection strategies. In addition to legal enforcement, public education remains a crucial line of defence against romance fraud. One highly effective preventive measure is encouraging potential victims to insist on live video interactions early in online relationships, as scammers often avoid video verification due to the risk of exposure. Practitioners, including law enforcement agencies, banks, and online platforms, must stay abreast of the latest tactics employed by fraudsters and collaborate closely to develop effective countermeasures. In Ghana, for instance, where digital literacy levels are still growing and online platforms are increasingly becoming part of everyday life, there is a pressing need to enhance cybersecurity awareness and provide training to individuals and organisations on how to recognise and respond to potential fraud schemes.

Furthermore, the study underscores the importance of international cooperation in combating romance fraud, particularly in addressing cross-border aspects such as underground credit card dealings and illegal goods trafficking on e-commerce platforms. Policymakers should prioritise strengthening collaboration with international counterparts, including law enforcement agencies and financial institutions, to share intelligence, coordinate investigations, and facilitate the prosecution of perpetrators operating across borders. This may involve enhancing legal frameworks, establishing mutual assistance mechanisms, and promoting information-sharing agreements to combat transnational organised crime networks involved in romance fraud.

Finally, the findings highlight the role of socioeconomic factors in driving individuals to engage in romance fraud. In a developing country like Ghana, where economic disparities exist and opportunities for legitimate employment may be limited, there is a risk that some individuals may turn to illicit activities as a means of survival. Policymakers should therefore address underlying socioeconomic challenges, such as unemployment, poverty, and lack of access to education and skills training, to reduce the vulnerability of individuals to involvement in fraudulent activities. This may involve implementing targeted poverty alleviation programs, promoting entrepreneurship and job creation initiatives, and strengthening social safety nets to provide support to vulnerable populations.

6.2. Suggestions for future research

Building on the findings of this study, several avenues warrant further exploration to deepen our understanding of online romance fraud and its evolving manifestations.

First, future research could extend beyond the Ghanaian context to include comparative case studies across multiple developing and developed regions, examining how cultural, socio-economic, and technological contexts influence offender strategies, victim selection, and scam typologies. Such comparative analyses may illuminate variations in tactics, operational timelines, and motivations, providing a broader theoretical and empirical base. Second, given the growing complexity of online scams, researchers should investigate the emergence of hybrid fraud models, such as pig-butchering scams, in which romance narratives are woven into longer-term financial frauds. These schemes, often run by organised transnational syndicates, present a different kind of psychological manipulation, and may share commonalities or distinctions with the strategies documented in this study. Third, future inquiries could examine the role of gender in shaping the dynamics of online romance fraud. Investigating how scam approaches differ depending on the victim's gender, and potentially the perpetrator's, could yield valuable insights into personalisation, emotional manipulation, and susceptibility. This line of inquiry may also contribute to more gender-sensitive awareness campaigns and prevention strategies.

Future studies may explore a longitudinal approach to track how scammers' strategies evolve over time in response to platform regulations, law enforcement tactics, and victim awareness. Such studies would offer a temporal dimension to existing models and could uncover cycles of adaptation and innovation in cybercrime behaviour.

CRediT authorship contribution statement

Sheena Lovia Boateng: Writing – review & editing, Validation, Formal analysis. **Eric Ansong:** Writing – review & editing, Writing – original draft, Methodology, Formal analysis. **Nii Barnor Jonathan Barnor:** Writing – original draft, Methodology, Conceptualization.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix. : Interview guide

Thank you for agreeing to participate in this interview. The purpose of this study is to understand the strategies and motivations behind online romance fraud from the perspective of those who have engaged in it.

Your responses will be kept confidential and used solely for academic purposes. You are free to decline to answer any question or to stop the interview at any time.

Section A: background information

1. Can you tell me a little about yourself?

– Age
– Education level
– Occupation

Section B: initial involvement

2. How did you first become involved in online romance fraud?

– What motivated you to start?
– How were you introduced to this activity?

Section C: planning and execution

3. Can you describe the process you use to select and approach potential victims?

– What platforms do you use?
– What criteria do you use to select victims?

4. What strategies do you use to build trust and develop relationships with your victims?

– Can you provide examples of communication techniques or scripts you use?

Section D: operational details

5. How do you manage and maintain multiple relationships with victims simultaneously?
   - How do you keep track of different conversations and personas?
6. What types of requests do you make to your victims?

– Financial requests
– Personal information requests
– Other types of requests

Section E: challenges and risks

7. What challenges do you face in conducting online romance fraud?

– Legal risks
– Ethical considerations
– Technical challenges

8. How do you mitigate the risks associated with this activity?

– Techniques to avoid detection.
– Strategies to handle potential exposure.

Section F: Psychological and Emotional Aspects

9. How do you perceive your relationship with the victims?

– Do you experience any emotional attachment or detachment?
– How do you justify your actions to yourself?

10. What impact, if any, has this activity had on your personal life and well-being?

Conclusion

Is there anything else you would like to share about your experiences or insights that we have not covered?

Thank you for your time and insights. Your participation is greatly appreciated and will contribute significantly to our understanding of online romance fraud.

References

Abubakari, Y., 2024. Modelling the modus operandi of online romance fraud: Perspectives of online romance fraudsters. J. Econ. Criminol. 6, 100112.

Anesa, P., 2020. Lovextortion: persuasion strategies in romance cybercrime. Discourse Context Media 35, 100398.

Aransiola, J.O., Asindemade, S.O., 2011. Understanding cybercrime perpetrators and the strategies they employ in Nigeria. Cyber Behav. Soc. Netw. 14 (12), 759–763.

Barnor, J.N.B., Boateng, R., Kolog, E.A., Afful-Dadzie, A., 2020. Rationalising online romance fraud: in the eyes of the offender. AMCIS 2020 Proc. 1–11.

Bibri, S.E., 2019. On the sustainability of smart and smarter cities in the era of big data: an interdisciplinary and transdisciplinary literature review. J. Big Data 6 (1), 1–64.

Boateng, R., Barnor, J.N.B., 2020. Unveiling cybercrime in a developing country. Proceeding of Encyclopedia of Criminal Activities and the Deep Web. IGI Global, Hershey, PA, pp. 66–92.

Boyd, D., 2008. Why youth (heart) social network sites: The role of networked publics in teenage social life. In: Buckingham, D. (Ed.), Youth, identity, and digital media. MIT Press, Cambridge, MA, pp. 119–142.

Buchanan, T., Whitty, M.T., 2014. The online dating romance scam: causes and consequences of victimhood. Psychol. Crime. Law 20 (3), 261–283.

Button, M., Carter, E., 2024. Relationship fraud: romance, friendship and family frauds. J. Econ. Criminol. 4, 100069.

Button, M., Gilmour, P., Hock, B., Jain, T., Jesperson, S., Lazarus, S., Pandey, D., Sabia, J., 2024. Scoping study on fraud centres: Ghana, India and Nigeria. Itad. ⟨https://www.itad.com/wp-content/uploads/2024/11/Fraud-Scoping-Study-for-publication-2024.pdf⟩.

Button, M., Lazarus, S., Hock, B., Bugbilla Sabia, J., Pandey, D., Gilmour, P., 2025. Factors influencing involvement in cyber-frauds in West Africa and the implications for policy. Eur. J. Crim. Policy Res. 1–23.

Chomariyah, 2021. Cyber security issues in implementing shipping traffic separation scheme (TSS) in Straits of Malacca and Singapore. Int. J. Cyber Criminol. 15 (1), 17–30.

Clarke, R.V., Cornish, D.B., 2017. Modeling offenders' decisions: A framework for research and policy. Proceeding of Crime opportunity theories. Routledge, London, pp. 157–195.

Cocozza, A., 2023. The theory of rational choice: potential and criticality. The Unexpected in Action: Ethics, Rationality, and Skills. Springer Nature Switzerland, Cham, pp. 75–90.

Cornish, D.B., Clarke, R.V., 2016. The rational choice perspective. Proceeding of Environmental criminology and crime analysis. Routledge, London, pp. 48–80.

Cross, C., 2020. Romance fraud. Proceeding of The Palgrave handbook of international cybercrime and cyberdeviance. Palgrave Macmillan, Cham.

Cross, C., Dragiewicz, M., Richards, K., 2018. Understanding romance fraud: Insights from domestic violence research. Br. J. Criminol. 58 (6), 1303–1322.

Cross, C., Holt, T.J., 2021. The use of military profiles in romance fraud schemes. Vict. Offenders 16 (3), 385–406.

Cross, C., Layt, R., 2022. I suspect that the pictures are stolen: romance fraud, identity crime, and responding to suspicions of inauthentic identities. Soc. Sci. Comput. Rev. 40 (4), 955–973.

Dudwick, N., Kuehnast, K., Nyhan Jones, V., Woolcock, M., 2006. Analysing social capital in context: A guide to using qualitative methods and data. World Bank Institute, Washington, D.C.
Ellison, N.B., Steinfield, C., Lampe, C., 2007. The benefits of Facebook "friends": social capital and college students' use of online social network sites. J. Comput. Mediat. Commun. 12 (4), 1143–1168.
Federal Trade Commission. (2021). Romance scams take record dollars in 2020. ⟨https://www.ftc.gov/news-events/blogs/data-spotlight/2021/02/romance-scams-take-record-dollars-2020⟩. Accessed February 28, 2024.
Ghana Statistical Service. (2025). Ghana Annual Household Income and Expenditure survey: *Quarterly Labour statistics (July edition)*. Accra, Ghana: GSS. ⟨https://statsghana.gov.gh/gssmain/fileUpload/pressrelease/Labour%20Statistics%20Bulletin%20(2025%20July%20Edition).pdf⟩.
Hui, K.-L., Kim, S.H., Wang, Q.-H., 2017. Cybercrime deterrence and international legislation: evidence from distributed denial of service attacks. MIS Q. 41 (2), 497–523.
Hutchings, A., Holt, T.J., 2018. Interviewing cybercrime offenders. J. Qual. Crim. Justice Criminol. 7 (1), 75–94.
Ianzito, C., 2022. Many victims struggle with mental health in scams' aftermath. AARP. ⟨https://www.aarp.org/money/scams-fraud/info-2022/mental-health-impact.html⟩. Accessed July 6, 2024.
Kopp, C., Layton, R., Sillitoe, J., Gondal, I., 2015. The role of love stories in romance scams: a qualitative analysis of fraudulent profiles. Int. J. Cyber Criminol. 9 (2).
Kuo, C., Tsang, S.S., 2023. Detection of price manipulation fraud through rational choice theory: evidence for the retail industry in Taiwan. Secur. J. 36, 712–731.
Kydd, M., Shepherd, L.A., Szymkowiak, A., Johnson, G.I., 2023. Love at first sleight: a review of scammer techniques in online romance fraud. Proceeding of The international conference on cybersecurity, situational awareness and social media. Springer Nature, Singapore, pp. 327–341.
Lazarus, S., Whittaker, J.M., McGuire, M.R., Platt, L., 2023. What do we know about online romance fraud studies? A systematic review of the empirical literature (2000–2021). J. Econ. Criminol. 2, 100013.
Livingstone, S., Helsper, E., 2007. Gradations in digital inclusion: children, young people, and the digital divide. New Media Soc. 9 (4), 671–696.
Manh, T., Falch, M., von Simeon, S., 2016. Universal service policy in Vietnam: a supply–demand perspective. J. NBICT 1, 123–140.
Miles, M.B., Huberman, A.M., 1994. Qualitative Data analysis: An Expanded Sourcebook. Sage, Thousand Oaks, CA.
Monroe, R., 2018. Explore the perfect man who wasn't. Atlantic. ⟨https://www.theatlantic.com/magazine/archive/2018/04/our-time-com-con-man/554057/⟩.
Pamungkas, B., Yusuf, M., 2019. Exploring digital legislation concepts and practices: Inspiration for Indonesia city government. Proceeding of International Conference on Democratisation in Southeast Asia (ICDeSA 2019). Atlantis Press, pp. 322–328.
Reuters. (2023). More than 100 arrests in West African internet scam investigation, says Interpol. *France24*. ⟨https://www.france24.com/en/africa/20230808-more-than-100-arrests-in-west-african-internet-scam-investigation-says-interpol⟩. Accessed July 5, 2024.
Romanska, M. (2012). Café culture history, part 5: The history of the cybercafé. ⟨https://artsemerson.org/2012/03/23/cafe-culture-history-part-5-the-history-of-the/⟩. Accessed July 6, 2024.
Sorell, T., Whitty, M., 2019. Online romance scams and victimhood. Secur. J. 32, 342–361.
Tambe Ebot, A., 2023. Advance fee fraud scammers' criminal expertise and deceptive strategies: a qualitative case study. Inf. Comput. Secur. 31 (4), 478–503.
Tan, H.K., David, Y., 2013. Preying on lonely hearts: a systematic deconstruction of an Internet romance scammer's online lover persona. J. Mod. Lang. 23 (1), 28–40.
Wang, F., 2024. Victim-offender overlap: the identity transformations experienced by trafficked Chinese workers escaping from pig-butchering scam syndicate. Trends Organ. Crime. 1–32.
Warner, J., 2011. Understanding cyber-crime in Ghana: a view from below. Int. J. Cyber Criminol. 5 (1), 736.
Warschauer, M., Matuchniak, T., Cotten, S.R., 2014. From digital divide to digital inequality: Studying Internet use as penetration increases. In: Dutton, W.H. (Ed.), The Oxford handbook of Internet studies. Oxford University Press, Oxford, pp. 129–150.
Whitty, M.T., 2013. The scammers persuasive techniques model: development of a stage model to explain the online dating romance scam. Br. J. Criminol. 53 (4), 665–684.
Whitty, M.T., 2018a. 419—It's just a game: pathways to cyber-fraud criminality emanating from West Africa. Int. J. Cyber Criminol. 12 (1), 97–114.
Whitty, M.T., 2018b. Do you love me? Psychological characteristics of romance scam victims. Cyber Behav. Soc. Netw. 21 (2), 105–109.
Whitty, M.T., 2019. Who can spot an online romance scam? J. Financ. Crime. 26 (2), 623–633.
Yar, M., Steinmetz, K.F., 2023. Cybercrime and Society, Therd ed. SAGE Publications, London.
Yin, R.K., 2018. Case study Research and Applications: Design and Methods, Sixth ed. Sage, Los Angeles, CA.

Nii Barnor Jonathan Barnor is a lecturer at the Department of Management Sciences, University of Education, Winneba. He has a PhD in Information Systems and a Master of Philosophy Degree in Management Information Systems, both from the University of Ghana Business School. Cybercrime, information systems security, information systems adoption, ICT for growth, digital mobile maps, and digital technologies are among Jonathan's research interests.

Eric Ansong holds a PhD degree in Information Systems from the University of Ghana. He is a lecturer at the Department of IT and Data Analytics, University of Ghana. His research interests include Information Systems adoption, innovations in education, Digital business strategies and ICT4D. He has published a number of research articles in peer-reviewed academic journals and has presented papers at international conferences.

Sheena Lovia Boateng is an Associate Professor at the University of Ghana Business School. She is the Communications Coordinator for the College of Humanities, University of Ghana. She is an Associate Editor for the Springer journal, Humanities & Social Sciences Communications. Her research interests span artificial intelligence and marketing, gender and technology, fashion and beauty marketing, and influencer marketing. Sheena's research has been published in the Information Development, and International Journal of Bank Marketing.