Humanities & Social Sciences Communications

REVIEW ARTICLE

https://doi.org/10.1057/s41599-025-05937-y OPEN

Short-term recovery of expatriates from mobile phone fraud: a systematic literature review

Kyoo-Man Ha[1]✉

Mobile phone fraud has been classified as a technological hazard. However, there is a lack of comparable and thorough research on this topic. This study aimed to describe how expatriates, as a special needs population, manage short-term recovery from mobile phone fraud. A systematic literature review was used as the methodology for this study. The current emphasis on technological support was analyzed via local banks, local police, other local communities, and international institutions to draw an alternative to social support. The key theme was that these four stakeholders could combine technological and social support in the initial phase to help expatriates recover during the initial phase of the mobile phone fraud emergency. They must also address social connotations and empower victims by promoting emergency awareness, time management, education, and training. This study focused on mobile phone fraud from the perspective of human-made emergency management.

Introduction

The wide scope of mobile phone fraud has caused huge economic losses to victims worldwide, amounting to more than $2.64 billion over 13 months (i.e., from January 2022 to February 2023) (Statista, 2024). Every $1 of mobile phone fraud results in an expense of $4.23 through sequential processing, such as criminal investigations, legal services, and recovery activities. Approximately 53% of workplaces have not yet established official fraud teams (Kadar, 2024). Moreover, the characteristics of mobile phone fraud differ across nations.

A total of 302 hazards (i.e., all natural hazards and human-made emergencies) were listed by the United Nations Office for Disaster Risk Reduction (UNDRR) in 2020. These hazards were classified into eight hazard categories (i.e., hydrometeorological hazards, biological hazards, chemical hazards, environmental hazards, geohazards, technological hazards, societal hazards, and extraterrestrial hazards) (United Nations Office for Disaster Risk Reduction (UNDDR, 2020)). Mobile phone fraud has been typically classified as a technological hazard. This is because it exploits weaknesses in communication technology, such as software design and security issues in mobile networks. Typical of technology failures, it also frequently entails complex strategies that control digital systems, resulting in extensive disruptions and monetary losses. In summary, the main cause of technological hazards is the internal or external failure of complicated technological systems.

When expatriates experience mobile phone fraud, they suffer huge economic losses and related psychological impacts (Sarria et al., 2019). For example, in many cases, expatriate victims are unaware of the extent of their losses, are unable to find bank phone numbers, and often fail to report phone fraud to the police. Despite stakeholder efforts, few rigorous studies have been

[1] Faculty of Resilience, Rabdan Academy, Abu Dhabi, UAE. ✉email: ha1999@hotmail.com; kmanha@ra.ac.ae

conducted on this subject. Thus, the research question is "How do major stakeholders deal with (or manage) the initial phase of recovery for expatriates who are victims of mobile phone fraud?"

The goal of this study is to investigate ways to improve the short-term recovery of expatriates from mobile phone fraud. This can ultimately decrease the related economic damages, psychological impacts, as well as human casualties (e.g., suicide, violence, etc.). Technological support is compared to social support received via local banks, local police, other local communities, and international institutions. The rest of the paper is organized as follows: Section 2 presents the literature review; Section 3 presents the methodology; Section 4 presents the results; Section 5 presents the discussion; and Section 6 presents the conclusion.

Literature review

Basic concepts. Mobile phone fraud involves multiple types of banking fraud, such as card fraud (e.g., debit card fraud, credit card fraud, lost card fraud, stolen card fraud, counterfeit card fraud, and other payment card fraud), remote banking fraud, authorized fraud (e.g., authorized push payment fraud), and check fraud (UK Finance (United Kingdom Finance Limited trading, 2022)). In short, mobile phone fraud refers to criminals deliberately deceiving a victim (i.e., an expatriate here) to steal money from their bank accounts via mobile phones, resulting in economic losses and psychological agony as well as human casualties.

When criminals use a mobile device to manipulate and trick a victim into providing financial information by building a degree of trust (by sharing concerns, information security regulations, etc.), mobile phone fraud is categorized as social engineering (Allan, 2023). Criminals using social engineering techniques (e.g., phishing, CEO fraud, and baiting) try to obtain one-time passwords (OTPs), PINs, or other passwords from the targeted victim. On the other hand, a typical victim authorizes bank payments through phone calls, emails, websites, or other means.

The breadth of this study is broader than many anticipated because mobile phone fraud encompasses both the technological risk of UNDRR and the social engineering of other researchers (GSMA Global System for Mobile Communications Association (2024); Zimba et al., 2022). While admitting that mobile phone fraud can take advantage of flaws in both digital systems and human behavior, it is complicated and necessitates a multidisciplinary approach to effectively address the emergencies involved. Conversely, a thorough grasp of fraud dynamics will be possible thanks to this expanded breadth, which will close the gap between technology-driven weaknesses and human-centered exploitations.

Expatriates who temporarily stay in a foreign country as laborers or on any other status are included in the special-needs population in the field of emergency recovery (FEMA (Federal Emergency Management Agency, 2021)). Compared with immigrants, most expatriates tend to return to their home country. Potential obstacles that expatriates may encounter include unfamiliarity with local laws, cultural sensitivities, the economic system, and information availability. In particular, new expatriates may not understand the local languages. Hence, expatriates may be at a higher risk of mobile phone fraud. Furthermore, a lack of access to local resources and support systems may make them even more vulnerable during emergencies.

The emergency management cycle (or emergency management lifetime) comprises four phases: emergency prevention/mitigation, preparedness, response, and recovery. The initial phase of emergency recovery is important in mobile phone fraud (Haddow et al., 2020). To guarantee a thorough return to stability and resilience, emergency recovery entails attending to the physical, mental, and social needs of victims of financial loss in addition to financial support to help them return to a degree of normalcy. Short-term emergency recovery includes freezing bank cards via bank emergency centers (or otherwise), reporting phone fraud to the police, monitoring and checking unauthorized activity, changing passwords, and communicating with close partners (World Bank Group, 2023).

Previous studies. Contrary to the fact that many accredited researchers have studied global cybercrimes (or cybersecurity), such as ransomware attacks, data breaches, COVID-19–related phishing, and targeted attacks, mobile phone fraud has not been examined (WEF (World Economic Forum, 2024)). Similarly, most of these researchers have discussed how to prevent cybercrimes (or emergency prevention), but have not investigated the initial phase of emergency recovery, particularly concerning expatriates (Kemp, 2023). Therefore, this research topic merits independent investigation.

Poppleton et al. (2021) classified all fraud (including mobile phone fraud) in England and Wales into nine categories. The fraud categories are very wide, and the reporting system for fraud is different from that of other crimes. The police, as well as the banks, are also notified. Thus, some stolen money has been refunded to the victims. Nonetheless, the researchers chose three categories (severely harmed victims; older adult vulnerable victims; and young, highly vulnerable victims) as high-vulnerability groups (Poppleton et al., 2021).

Faeth and Kittler, 2017 investigated how expatriates in Africa perceived danger via in-depth interviews and discovered that those exposed to traditional crimes in Johannesburg experienced more dread or fear than those exposed to terror in Nairobi (Faeth and Kittler, 2017). Therefore, while expatriates exposed to terror tried to avoid the possible regions, those exposed to crimes were willing to deal with the connected issues. The findings of this study could indicate that expatriates reacted differently to various hazards in their home environments.

Andersen (2018) examined the prevalence of artificial intelligence and emphasized human rights (Andersen, 2018). Artificial intelligence is widely utilized worldwide and has made human life more convenient, for example, by enhancing work performance and facilitating data analysis. However, artificial intelligence has also caused harm to human society. Given that marginalized people cannot obtain proportionate advantages from its use, the study has emphasized the importance of human rights.

Cross (2021) studied how the COVID-19 pandemic altered the extent of vulnerability among older adults via fraud victimization (Cross, 2021). Mainly because of government strategies to protect against COVID-19, such as home isolation and activity restrictions, several older adults had to stay alone. Under these circumstances, many criminals utilized the impact of COVID-19 as a context for their fraud schemes, increasing related frauds. Researchers have highlighted the importance of connectivity among older adults.

Using an 18-month postal survey, Button et al. (2024) similarly examined how the older adult (i.e., over 75) population in the United Kingdom (UK) responded to phone fraud attempts. Every week, about 20% of senior citizens reported being victims of phone fraud (Button et al., 2024). This indicated that telephones were used to assault elderly people more frequently than other methods. It became evident that older adults were more likely than people of average age to become victims of phone fraud. This could be explained by a rise in phone fraud or recurring victims.

In 2023, the Institute of Internal Auditors released a management report regarding the impact of COVID-19 on fraud risks. It elaborated on the impact of COVID-19 on mobile phone fraud (IIA (Institute of Internal Auditors, 2023)). Although the impact of COVID-19 has decreased in several sectors, it still negatively influences the risk of mobile phone fraud. The report emphasized that the trend of fraud risk reflected a significant change during the COVID-19 pandemic. In other words, criminals believed that individuals and organizations had relaxed their defenses against mobile phone fraud.

Clarke et al. (2001) attempted to draw lessons learned from the situation of mobile phone fraud in the UK, emphasizing the importance of partnerships between governments and industry (Clarke et al., 2001). Many cases in the United States (US) in the 1990s were related to obtaining free services and accessing networks by altering mobile phones. After eliminating these crimes, the US faced new types of phone fraud. To control them, researchers suggested cooperative relationships between governments and businesses.

Study characteristics. Although this study examines the initial phase of emergency recovery immediately after the occurrence of mobile phone fraud, the perspective of human-made emergency management is included more in-depth than in previous studies (Juneau, 2017). Fundamentals of human-made emergency management are referred to during the theoretical processes, such as its interdisciplinary nature (including not only engineering but also social sciences), continuity and reconstitution, comprehensiveness, community engagement, disaster culture, and time.

Two unique emergency recovery strategies—technological support and social support—are proposed in this study. When major stakeholders fully support expatriate victims through the use of cutting-edge technologies, this is referred to as technological support (Sharma, 2022). Additional financial losses are minimized by protecting the victim's mobile device, monitoring account activity, getting in touch with service providers, and other means. Currently, the overemphasis on technology in this strategy has had a negative effect (or is insufficient for emergency recovery).

Social support refers to assistance or encouragement from social circles or other social networks. Social support emphasizes that multiple stakeholders fully defend the victims of mobile phone fraud by offering practical and emotional support (also known as empathy) (Zhang and Ye, 2022). This reduces the immediate social and psychological impact of mobile phone fraud. Specifically, the positive function of social support offsets the negative function of technological support.

Methodology

Review protocol. In this study, the methodology was primarily a systematic literature review, given that a certain number of qualitative texts on short-term recovery from mobile phone fraud were searched, analyzed, and summarized (Jahan et al., 2016; Owens, 2021). Although the importance of empirical methods cannot be denied, appropriate research is needed to address the extent of fraud complexity and interdisciplinary studies, among others, via a systematic literature review. Figure 1 shows the review protocol for this study, including the research question, key variables, research direction, and goal of the study.

With elements like research protocol, pertinent text selection, text analysis, and sequential interpretation (Carrera-Rivera et al., 2022), the presentation above covers a systematic literature review to identify a major theme associated with the research topic, such as the contrast between technological support and social support. With this, the presentation keeps examining how mobile phone fraud affects expatriates, concentrating on the first stage of their emergency recovery. It focuses on how important parties, such as local banks, police, other local communities, and international organizations, deal with this kind of fraud.

Relevant text selection. This study used suitable methods to thoroughly research pertinent texts on the subject (Khan et al., 2003). The study used various sources: databases, such as ScienceDirect, EBSCO, and ProQuest; Google.com for a variety of documents, including research articles, government documents, electronic books, and booklets; and other resources, such as SCOPUS, Taylor & Francis Online, TRAC, SAGE Journals, and Oxford Academic e-journals. Most of the texts were digitized.

To elaborate, the study selection process was to find and incorporate pertinent texts about the short-term recovery of expatriates from mobile phone fraud (Grau-Sarabia and Fuster-Morell, 2021; Khatwani et al. (2024)). A thorough search was first carried out across several databases to guarantee access to a large number of scholarly and professional resources. Digital texts were preferred for ease of access and analysis, and studies were vetted for alignment with the research objective to guarantee relevance. To ensure a strong basis for a systematic literature review, the study selection process focused on peer-reviewed, high-quality research articles.

In this study, text inclusion and exclusion rules were established based on the research question. The first criterion was whether the text addressed emergency recovery or mobile phone fraud. The second criterion was the inclusion of contemporary texts. The third criterion was the rejection of non-English works. The keywords utilized included "cell phone fraud and emergency prevention," "cell phone fraud and emergency recovery," "phone fraud and psychological impacts," "fraud victimization and implications," "technological hazards and mobile phone fraud," "cell phone fraud and local bank," "cell phone fraud and local police," "cell phone fraud and local communities," "cell phone fraud and international organizations," among others.

The included studies were characterized by their emphasis on the relationship between emergency recovery and mobile phone fraud (Luo, 2024). The psychological impacts of phone fraud, its consequences for emergency prevention and recovery, and the roles of key stakeholders in reducing technological hazards were only a few of the many topics covered in the studies. To promote a thorough grasp of social support, targeted keywords were used to source messages that offered insights into the useful features of handling mobile phone fraud in emergencies.

Text analysis and interpretation. Considering that text analysis classifies and evaluates various unstructured texts, four stakeholders—local banks, local police, other local communities, and international institutions—were selected as related analytical units in this study (O'Mara-Eves et al. (2015)). They are all key stakeholders in mobile phone fraud against expatriates, regardless of national boundaries. While victims directly ask both local banks and police for assistance, they also request other local communities, including families and acquaintances, for assistance. International institutions cooperate with national entities regarding phone fraud.

As it is necessary to combine different thoughts on the issue, text synthesis is crucial during text interpretation (Rammal, 2023). Two emergency recovery strategies—technological versus social support—are taken into consideration as two categories of analysis in this study. This study focuses on the direction of these two categories. The same four analytical units are assigned to each category of analysis to address the systematic components. Although each category's content initially appears to be at odds, they complement each other.

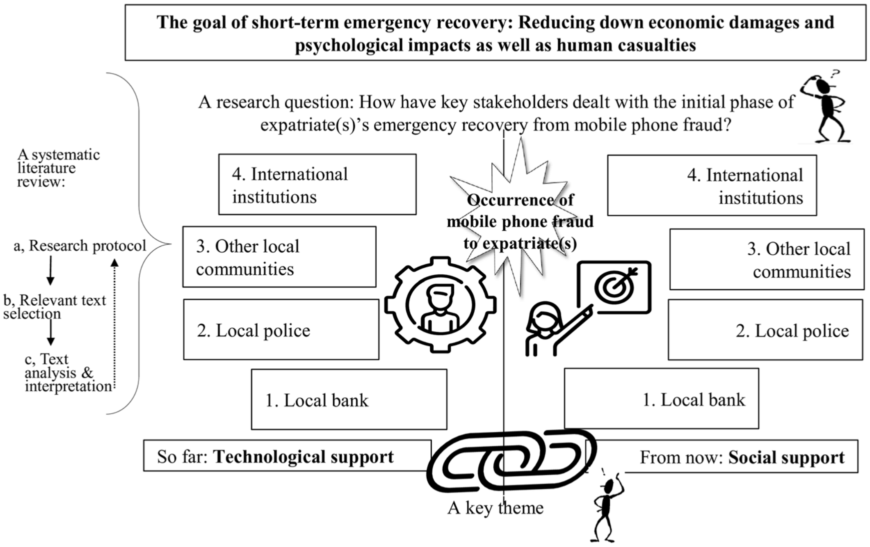
The goal of short-term emergency recovery: Reducing down economic damages and psychological impacts as well as human casualties
A research question: How have key stakeholders dealt with the initial phase of expatriate(s)'s emergency recovery from mobile phone fraud?
A systematic literature review:
a, Research protocol
b, Relevant text selection
c, Text analysis & interpretation
4. International institutions
3. Other local communities
2. Local police
1. Local bank
Occurrence of mobile phone fraud to expatriate(s)
4. International institutions
3. Other local communities
2. Local police
1. Local bank
So far: Technological support
From now: Social support
A key theme

Fig. 1 Research design.

Results: technological support

Local bank. Immediately after receiving phone calls from victims, customer service staff in local banks try to block customers' cash cards, credit cards, and even bank accounts (Tomar et al., 2022). Thus, the local bank involved makes all possible efforts to monitor related bank accounts and freezes monetary transactions. The quicker an emergency operator at the local bank takes action, the more likely it is to minimize financial loss for the victim. Thus, emergency operators and the banking system immediately provide technological assistance to victims.

The fraud department in the local bank continues to consult with the victim to investigate exactly how much money has been stolen and what can be done to prevent future fraud. The local bank provides bank statements to confirm the number of transactions, the number of OTPs used, and the amount of money stolen. Mobile phone fraud victims can file dispute initiation forms for certain categories of stolen money. Owing to uncertainty and complexity, all bank agents do not receive the same knowledge regarding the amount of money that can be refunded to an expatriate, even though the fraud department relies on technical assistance.

Local police. The criminal investigation department assigns a case number shortly after an expatriate visits and reports the mobile phone fraud to the local police station. However, victims may not receive a case number without proper documentation from the local bank, which would make it extremely difficult for the police to continue their investigations. Instead of providing standardized methods to the stakeholders, case numbers must be generated electronically.

The criminal investigation department continues to track the flow of stolen money while working closely with several partners, such as local banks, telecom providers, and international police (Carter, 2023). Local police rely completely on technological support, specifically through various local, regional, and international collaborations. They have also traditionally embraced structured investigation procedures, such as forensic analysis, evidence collection, suspect identification, and suspect arrest.

Other local communities. Given that mobile phone fraud can occur anywhere—at work, at home, or elsewhere—local acquaintances tend to assist expatriates (Hanoch and Wood, 2021). Moreover, close friends and family members try their hardest to provide victims with technological and psychological support. Similarly, victims at work may request assistance from building security guards, who promptly provide the bank's emergency numbers or pertinent local police information.

Other local communities also make an effort to assist mobile phone fraud victims through the use of technology, in part because phone fraud primarily affects individuals. Finance officers ensure that victims of such emergencies take immediate action such as blocking bank cards and reporting cell phone fraud to the local police. Additionally, the mainstream media use technology to report news regarding the prevalence of cell phone fraud in a given region.

International institutions. Given that about two-thirds (2/3) of all mobile phone frauds have a significant connection to foreign transactions, international institutions address the issue for expatriates either directly or indirectly. International revenue share fraud (such as IP box/PBX hacking and roaming fraud) and interconnect bypass (such as SIM box fraud and refilling) are two of the many fraud forms that have affected expatriates the most (BICS, 2024; INTERPOL, 2024b). Scammers in country A may generate fake traffic that originates in country B and finishes in country C because mobile phone fraud can spread like a virus. International institutions play a crucial role in these situations.

The International Criminal Police Organization (INTERPOL) has played a significant role in dealing with recovery from mobile phone fraud worldwide. For example, INTERPOL confiscated almost $150 million in illicit funds from telecom fraud in more than 10,000 sites after a year-long investigation that involved law enforcement agencies from 35 nations globally (INTERPOL The International Criminal Police Organization (2024a)). The cross-jurisdictional nature of criminals presents obstacles to INTERPOL investigations. Thus, the INTERPOL has addressed the significance of close cooperation among member countries via joint international investigations and public-private cooperation, among others. Whatever the situation, technological applications have been put into place to include data analysis and forensics, machine learning, and information exchange.

As the International Telecommunication Union (ITU), a UN agency, works on cybersecurity, UNDRR has underscored the importance of information sharing for mobile phone fraud (as a human-made emergency) recovery (ITU International Telecommunication Union (2021)). Other institutions, such as the

Table 1 Strategies for integrating technological and social support.

Units	Detailed strategies
Local bank	- While using technology to freeze bank cards and accounts, customer service representatives of the local bank must also provide comforting assurance to victims through clear communication and by offering support resources and timely updates. - The fraud department of the local bank must investigate how to provide victims with accurate information regarding the pilfered money swiftly. The department must be transparent with the victims and share information via the initial investigation and verification process.
Local police	- To avoid any potential consequences, especially after immediate requirements are met, the criminal investigation department must contact and interview mobile fraud emergency victims and explain the process and follow-up. - The criminal investigation department should use a victim-based strategy, including experience validation, victim advocacy, and other interactions when collaborating with stakeholders both locally and internationally through technological support.
Other local communities	- Family members, close friends, and building security personnel must speak with victims and help them take proactive steps for initial recovery. This must include emotional support and advocacy for victim rights. - Local communities must systematically assist mobile fraud emergency victims by recognizing the value of social responsibility, through partnerships with law enforcement, corporate responsibility, and risk treatment.
International institutions	- When the INTERPOL addresses technological support as its primary activity, it includes the importance of social support via scientific vision such as comprehensive techno-social awareness and community engagement. - The ITU and UNDRR should promote concrete initiatives for indirect social support for fraud victims (e.g., resilience building, joint research, and analysis) with the support of the FATF, and FS-ISAC, among others.

Financial Action Task Force, the Financial Services Information Sharing and Analysis Center, regional associations, and banks have partially coped with the initial phase of phone fraud recovery. However, these institutions usually rely on technological support for mobile phone fraud recovery. International operators' strategies to reduce fraud exposure have been agile and rapidly evolving with the aid of technology, and mobile phone fraud has been regularly evaluated.

Discussion: technological and social support

Cutting-edge technologies alone cannot prevail during the emergency management cycle without equal dependence on social sciences (including the arts and humanities) (Hess and Sovacool, 2020; Loyola University Chicago, 2024). The application of technologies, such as machine learning, information exchange, and data analysis, is ineffectual when people do not use them appropriately. As technologies are used to construct emergency management programs, the human mind, decision-making, and social networks facilitate their precise application in the field via ethics and social ramifications, among others.

Similarly, while developing, improving, and then distributing technological products for short-term recovery from mobile phone fraud, it is important to study and then apply social connotations to these technologies. Technological evolution consists of path-dependent processes, similar to social evolution (Malloy, 2023). Hence, human behavior, social values, and local culture, as social components, play crucial roles in the acknowledgment, adoption, and diffusion of technological programs for mobile phone fraud recovery. Tangible technologies without an intangible social essence will become short-sighted tools.

The occurrence of mobile phone fraud should not be considered an individual event but a social affair, mainly because it has extensive social implications (Dinisman and Moroz, 2017). Although mobile phone fraud seems to affect only the expatriate victims, causing them to lose money, it results in domino effects that often impact businesses, financial institutions, and network security, damage reputation, and result in legal troubles, among others. Therefore, dealing with the initial phase of mobile phone fraud recovery requires collective action and social responsibility.

Only family members, friends, and building security guards directly embody the extent of social support for victims, which shows the lack of social support from the other stakeholders. The other major stakeholders attempt to provide technological support for short-term recovery. Therefore, we conclude that technological support should not be replaced by social support because techno-social support is required for emergency recovery. Moreover, the four stakeholders complement technological support with social support (Table 1).

By highlighting the crucial interaction between technological and social support during the early stage of emergency recovery following mobile phone fraud, this study presents a fresh viewpoint (Alam et al., 2023). In contrast to earlier research that mostly concentrated on broad theoretical frameworks or technology solutions, this study finds a deficit in the involvement of important stakeholders in offering comprehensive support. This study advances a more thorough and community-centered model of human-made emergency management by suggesting that stakeholders supplement technological interventions with ongoing social support.

On a similar note, the literature focuses on the technological aspects of cyber fraud emergencies; however, human aspects have been ignored (Razaq et al., 2021). This study contributes to the literature by bridging the gap between these two aspects. Although the literature partially discusses mobile phone fraud, research on expatriates, in particular, is not included. This study highlighted the significance of techno-social support for victimized expatriates. Similarly, the theoretical framework expands the scope of mobile fraud emergency recovery in the research domain.

Combining technological and social support empowers the victims (Braverman, 2023). Certainly, mobile phone fraud is not a victimless crime. Considering that quite a few expatriates have lost money, and consequently, some have faced mental health issues or committed suicide, the four major stakeholders must make efforts to empower them by collaboratively utilizing techno-social support. Empowering victims is a fundamental tenet of associated healing.

Although the results around mobile phone fraud may appear apparent, they draw attention to typical answers that are frequently missed in more comprehensive analyzes (Liu et al., 2024). As such, a vital initial step in preventing immediate financial harm is to notify the bank and block cards. A crime number guarantees a formal record for insurance claims and future police investigations. In addition to procedural measures, fraud victims may desire advocacy, proactive fraud prevention, or emotional support (Cross, 2018).

The fact that these reactions are comparable for phone fraud victims who are non-expatriates highlights how the procedural methods are universal in these situations. This resemblance emphasizes how crucial it is to customize support networks to meet the shared emotional and procedural needs of many demographic groups in addition to the particulars of this emergency (Button et al., 2009; Cross et al., 2016). Nonetheless, the extent of expatriates' reactions under unfamiliar environments has been further higher than that of non-expat victims' reactions (Padron–Hernandez, 2024). The difficulties of negotiating linguistic hurdles, cultural differences, and the scarcity of local support systems during emergencies are often blamed for these increased reactions among expats.

There are numerous options for empowering expatriate victims. For example, all four stakeholders must listen without passing judgment on the expatriates' experiences before, during, or after the occurrence of mobile phone fraud. These stakeholders may rapidly conduct needs assessments for victims and use the information to provide techno-social support (NCVC National Center for Victims of Crime and FINRA Financial Industry Regulatory Authority (2021)). Additionally, all stakeholders must work to enhance relevant international rules and regulations, ensuring that expatriates can safely get back their money.

Although many expatriates experience mobile phone fraud, about one-third are unwilling to report it to the authorities such as the police and banks (NTS National Trading Standards (2023)). Almost all victims of mobile phone fraud experience emotions, such as anger, disappointment, frustration, embarrassment, and shame. Because they feel sad and ashamed, they especially tend to keep their suffering a secret, even from friends.

Emergency awareness and information sharing are needed to provide techno-social support to prevent the occurrence of similar crimes (EESC European Economic and Social Committee (2018)). Appropriate public awareness is a key factor for mobile phone fraud prevention, preparedness, and emergency recovery. Additionally, recognizing that the criminals could scam other victims, expatriate victims must share their experiences with others. Local employers should publish related information with the approval of the victim.

Although forgetting (or not remembering) is a positive variable for people's mental health, receiving techno-social support helps alleviate the psychological impact on expatriate victims. Forgetting is similar to clearing unnecessary items from a victim's space to ensure that they can find what is needed (Costanzi et al., 2021). It keeps thoughts from getting in the way of managing the mobile phone fraud situation. Expatriates will not forget the impacts of mobile phone fraud if they do not have enough time to recover.

Furthermore, techno-social support related to time management can help expatriates forget their mobile phone fraud experience. Time management refers to how an individual organizes their time in their own environment (Anderson and Hulbert, 2021). Family members, co-workers, or neighbors can help victims when they face challenges in time management. Moreover, active forgetting will eliminate traces of fraud for expatriate victims.

Considering that current education on mobile phone fraud emphasizes emergency prevention or response (US DOE United States Department of Education (2024)), further concrete actions must be included in the initial phase of emergency recovery when providing techno-social support. Undoubtedly, fraud prevention is the best form of education. However, expatriates are humans and bound to make mistakes. Once criminals have access to an expatriate's bank account, they begin to wreak havoc. Hence, educators must emphasize the importance of taking swift action via techno-social support, following mobile phone fraud.

Primarily because expatriates are part of the special needs population, emergency training to plan and implement tailored programs is not being conducted (Costantini and Raffety, 2021). Moreover, emergency trainers do not discuss practical details regarding short-term recovery from mobile phone fraud. Therefore, trainers must conduct discussion-oriented exercises (e.g., seminars, tabletop exercises, and games) and operation-oriented exercises (e.g., drills, functional exercises, and full-scale exercises) to provide techno-social support.

Conclusion

This study investigated how key stakeholders, such as local banks, local law enforcement, other local communities, and international organizations could enhance the first stage of emergency recovery from mobile phone fraud for expatriates. Important concepts, previous studies, challenges, ramifications, and additional information are included in this study. In particular, this study reached its initial goals when it outlined and described two key approaches: technology support and social support.

This study's most important finding is that all four stakeholders work to provide affected expatriates with both technological and social support. These stakeholders essentially carry out the aforementioned tasks, which include consoling, conducting additional victim interviews, taking proactive measures, and advancing scientific vision. They also cover communal accountability, victim empowerment, information sharing, forgetfulness, time management, emergency education, and training.

The strength of this study is that the theoretical process fully incorporates the human-made emergency management viewpoint. This study expands the bounded discipline of many prior studies by using numerous emergency management principles via interdisciplinary research. However, keeping in mind that many incidents of mobile phone fraud, regardless of geographic boundaries, are voluntarily unreported, one limitation of this study may be a distorted understanding of the topic. In short, underreporting may have led to potential challenges in this study. To overcome this limitation, researchers must concentrate on finding the most effective way to handle unreported incidents of mobile phone fraud.

Other academics could use the analytical framework presented in this study, either directly or indirectly, to further explore mobile phone fraud among expatriates. Further research must be conducted on the same topic for other special-needs populations, including children, older adults, and those with impairments. Numerous research initiatives worldwide can help achieve the final objective of mobile fraud emergency management.

Data availability

Data sharing did not apply to this research because no data sets were generated or analyzed during the study.

Received: 21 June 2024; Accepted: 4 September 2025;
Published online: 03 November 2025

References

Alam SS, Makmor N, Masukujjaman M, Mohamed Makhbul ZK, Ali MH, Al Mamun A (2023) Integrating the social support theory and technology acceptance model of social commerce websites. Rev Galega Econ 32(2):1–24. https://doi.org/10.15304/rge.32.2.8558

Allan K (2023) Understanding and avoiding social engineering attacks. https://cybermagazine.com/articles/understanding-and-avoiding-social-engineering-attacks

Andersen L (2018) Human Rights in the Age of Artificial Intelligence. Access Now, Brooklyn, New York. https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf

Anderson MC, Hulbert JC (2021) Active forgetting: adaptation of memory by prefrontal control. Annu Rev Psychol 72:1–36. https://doi.org/10.1146/annurev-psych-072720-094140

BICS (2024) Understanding international telecoms fraud: protect revenue, mitigate risk. BICS, Brussels, Belgium, https://www.bics.com/wp-content/uploads/2022/02/Telco-Fraud-Whitepaper.pdf

Braverman S (2023) Fraud strategy: stopping scams and protecting the public. HH Global, Leatherhead, UK, https://assets.publishing.service.gov.uk/media/64539087faf4aa0012e132cb/Fraud_Strategy_2023.pdf

Button M, Lewis C, Tapley J (2009) A better deal for fraud victims: research into victims' needs and experiences. National Fraud Authority, London, United Kingdom. https://assets.publishing.service.gov.uk/media/5a7b56b4e5274a319e77e9f0/better-deal-for-fraud-victims.pdf

Button M, Shepherd D, Hawkins C, Tapley J (2024) Fear and phoning: telephones, fraud, and older adults in the UK. Int Rev Victimology 0(0). https://doi.org/10.1177/02697580241254399

Carrera-Rivera A, Ochoa W, Larrinaga F, Lasa G (2022) How-to conduct a systematic literature review: a quick guide for computer science research. MethodsX 9:101895. https://doi.org/10.1016/j.mex.2022.101895

Carter E (2023) Confirm not command: examining fraudsters' use of language to compel victim compliance in their own exploitation. Br J Criminol 63(6):1405–1422. https://doi.org/10.1093/bjc/azac098

Clarke RV, Kemper R, Wyckoff L (2001) Controlling cell phone Fraud in the US: lessons for the UK 'foresight' prevention initiative. Secur J 14:7–22. https://doi.org/10.1057/palgrave.sj.8340070

Costanzi M, Cianfanelli B, Santirocchi A, Lasaponara S, Spataro P, Rossi-Arnaud C, Cestari V (2021) Forgetting unwanted memories: active forgetting and implications for the development of psychological disorders. J Pers Med 11:241. https://doi.org/10.3390/jpm11040241

Cross C(2018) Misunderstanding the impact of online fraud: implications for victim assistance schemes Victims Offenders 13(6):757–776

Cross C (2021) Theorising the impact of COVID-19 on the fraud victimisation of older persons. J Adult Prot 23(2):98–109. https://doi.org/10.1108/JAP-08-2020-0035

Cross C, Richards K, Smith R (2016) The reporting experiences and support needs of victims of online fraud. Trends Issues Crime Crim Justice 518:1–14. https://doi.org/10.52922/ti148355

Dinisman T, Moroz A (2017) Understanding victims of crime: the impact of the crime and support needs. Victim Support, London, UK. https://www.researchgate.net/publication/316787563_Understanding_victims_of_crime_The_impact_of_the_crime_and_support_needs?channel=doi&linkId=59118a70458515bbcb917314&showFulltext=true#fullTextFileContent

EESC (European Economic and Social Committee) (2018) Cybersecurity: ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks. EESC, Brussels, Belgium, https://www.eesc.europa.eu/sites/default/files/files/qe-01-18-515-en-n.pdf

Faeth PC, Kittler MG (2017) How do you fear? Examining expatriates' perception of danger and its consequences. J Glob Mobil 5(4):391–417. https://doi.org/10.1108/JGM-11-2016-0063

FEMA (Federal Emergency Management Agency) (2021) Safeguarding the special needs population. https://www.fema.gov/case-study/safeguarding-special-needs-population

Grau-Sarabia M, Fuster-Morell M (2021) Gender approaches in the study of the digital economy: a systematic literature review. Humanit Soc Sci Commun 8:201. https://doi.org/10.1057/s41599-021-00875-x

GSMA (Global System for Mobile Communications Association) (2024) Mobile money fraud typologies and mitigation strategies. GSMA Head Office, London, United Kingdom, https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2024/05/Mobile-Money-Fraud-Typologies-and-Mitigation-Strategies-20.05.24.pdf

Haddow GD, Bullock JA, Coppola DP (2020) Introduction to emergency management. Elsevier, Boston, Massachusetts. https://doi.org/10.1016/B978-0-12-817139-4.01001-0

Hanoch Y, Wood S (2021) The scams among us: who falls prey and why. Curr Directions Psychol Sci 30(3):260–266. https://doi.org/10.1177/0963721421995489

Hess DJ, Sovacool BK (2020) Sociotechnical matters: reviewing and integrating science and technology studies with energy social science. Energy Res Soc Sci 65:101462, https://ssrn.com/abstract=3540100

IIA (Institute of Internal Auditors) (2023) Lingering fraud risks of the COVID-19 pandemic. Tone at the Top, 115. https://www.theiia.org/globalassets/site/resources/research-and-reports/tone-at-the-top/2022/tatt-final-feb2023.pdf

INTERPOL (The International Criminal Police Organization) (2024a) Cybercrime. https://www.interpol.int/en/Crimes/Cybercrime

INTERPOL (2024b) INTERPOL global financial fraud assessment. INTERPOL General Secretariat, Lyon, France, https://www.interpol.int/Search-Page?search=INTERPOL+Global+Financial+Fraud+Assessment

ITU (International Telecommunication Union) (2021) Operational framework and guidelines for the planning and execution of ITU regional cyberdrills. ITU, Geneva, Switzerland, http://handle.itu.int/11.1002/pub/81b183fd-e

Jahan N, Naveed S, Zeshan M, Tahir MA (2016) How to conduct a systematic review: a narrative literature review. Cureus 8(18):e864. https://doi.org/10.7759/cureus.864

Juneau E (2017) Introduction to disaster management for the family physician. Memorial University of Newfoundland, St. John's, Canada, https://www.cfpc.ca/CFPC/media/Resources/Health-Policy/Principles-Emergency-Disaster-Management.pdf

Kadar T (2024) Global banking fraud index 2023. https://seon.io/resources/global-banking-fraud-index/

Kemp S (2023) Exploring public cybercrime prevention campaigns and victimization of businesses: a Bayesian model averaging approach. Comput Secur 127:103089. https://doi.org/10.1016/j.cose.2022.103089

Khan KS, Kunz R, Kleijnen J, Antes G (2003) Five steps to conducting a systematic review. J R Soc Med 96(3):118–121. https://doi.org/10.1258/jrsm.96.3.118

Khatwani R, Mishra M, Kumar VVR, Mistry J, Mitra PK (2024) Creating quality portfolios using score-based models: a systematic review. Humanit Soc Sci Commun 11:1615. https://doi.org/10.1057/s41599-024-03888-4

Liu M, Liang X, Chen J (2024) Constructing identities in institutional impersonation fraud: self-styling and other-styling practices through stances. Humanit Soc Sci Commun 11:1467. https://doi.org/10.1057/s41599-024-03875-9

Loyola University Chicago (2024) Top reasons why technology needs the humanities. https://www.luc.edu/ctsdh/stories/archive/topreasonswhytechnologyneedsthehumanities.shtml

Luo Q (2024) Cybercrime as an industry: examining the organisational structure of Chinese cybercrime. Humanit Soc Sci Commun 11:1554. https://doi.org/10.1057/s41599-024-04042-w

Malloy DC (2023) Why humanities is still an important study choice in today's technology driven world. https://economictimes.indiatimes.com/nri/study/why-humanities-is-still-an-important-study-choice-in-todays-technology-driven-world/articleshow/99788777.cms

NCVC (National Center for Victims of Crime) and FINRA (Financial Industry Regulatory Authority) (2021) Taking action: an advocate's guide to assisting victims of financial fraud. NCVC, Washington, D.C. https://www.finrafoundation.org/sites/finrafoundation/files/taking-action-an-advocates-guide-to-assisting-victims-of-financial-fraud_1.pdf

NTS (National Trading Standards) (2023) 19 million lose money to scams but fewer than a third report. https://www.nationaltradingstandards.uk/news/19-million-lose-money-to-scams-but-fewer-than-a-third-report/

O'Mara-Eves A, Thomas J, McNaught J, Miwa M, Ananiadou S (2015) Using text mining for study identification in systematic reviews: a systematic review of current approaches. Syst Rev 4:5. https://doi.org/10.1186/2046-4053-4-5

Owens JK (2021) Systematic reviews: brief overview of methods, limitations, and resources. Nurse Author Editor 31(3/4):69–72. https://doi.org/10.1111/nae2.28

Padron-Hernandez I (2024) Attachment and adjustment in expatriate reactions to the 2011 Tohoku disasters. J Asia Bus Stud 18(4):1021–1042. https://doi.org/10.1108/JABS-08-2023-0340

Poppleton S, Lymperopoulou K, Molina J (2021) Who Suffers Fraud? Understanding the Fraud Victim Landscape. Victims' Commissioner for England and Wales, London. https://cloud-platform-e218f50a4812967ba1215eaecede923f.s3.amazonaws.com/uploads/sites/6/2021/12/VC-Who-Suffers-Fraud-Report-1.pdf

Rammal HG (2023) Systematic literature reviews: steps and practical Tips. In: Rana S, Singh J, Kathuria S (eds) Advancing methodologies of conducting literature review in management domain (Review of Management Literature, Vol. 2), pp. 27–35. Emerald Publishing Limited, Leeds, England. https://doi.org/10.1108/S2754-586520230000002002

Razaq L, Ahmad T, Ibtasam S, Ramzan U, Mare S (2021) We even borrowed money from our neighbor": understanding mobile-based frauds through victims' experiences. Proc ACM Hum Comput Interact 5:41. https://doi.org/10.1145/3449115

Sarria E, Recio P, Rico A, Diaz-Olalla M, Sanz-Barbero B, Ayala A, Zunzunegui MV (2019) Financial fraud, mental health, and quality of life: a study on the population of the city of Madrid, Spain. Int J Environ Res Public Health 16(8):3276. https://doi.org/10.3390/ijerph16183276

Sharma D (2022) The use of technology to counter frauds and scams for the benefit of society: a detailed study. Amity Univ Press 4(2):59–66

Statista (2024) Estimated financial value of mobile app fraud worldwide from January 2022 to February 2023, by category. https://www.statista.com/statistics/1380417/app-fraud-value-by-category/#statisticContainer

Tomar I, Dharurkar N, Tiwari M, Mishra R, Gupta S, Sureka N, Syamala M (2022) Combating fraud in the era of digital payments. PwC, Mew Delhi, India, https://www.pwc.in/assets/pdfs/consulting/financial-services/fintech/payments-transformation/combating-fraud-in-the-era-of-digital-payments.pdf

UK Finance (United Kingdom Finance Limited trading) (2022) Annual Fraud Report: the definitive overview of payment industry fraud in 2021. UK Finance, London. https://www.ukfinance.org.uk/system/files/2022-06/Annual%20Fraud%20Report%202022_FINAL_.pdf

UNDRR (United Nations Office for Disaster Risk Reduction) (2020) Hazard definition & classification review: technical report. Geneva, Switzerland. https://www.undrr.org/media/47681/download?startDownload=true

US DOE (United States Department of Education) (2024) A call to action for closing the digital access, design, and use divides: 2024 national educational technology plan. Office of Educational Technology, Washington, D.C, https://tech.ed.gov/files/2024/01/NETP24.pdf

WEF (World Economic Forum) (2024) Global cybersecurity outlook 2024. WEF, Geneva, Switzerland, https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

World Bank Group (2023) Fraud risks in fast payments. The World Bank, Washington, D.C, https://fastpayments.worldbank.org/sites/default/files/2023-10/Fraud%20in%20Fast%20Payments_Final.pdf

Zhang Z, Ye Z (2022) The role of social-psychological factors of victimity on victimization of online fraud in China. Front Psychol 13:1030670. https://doi.org/10.3389/fpsyg.2022.1030670

Zimba A, Mukupa G, Chama V (2022) Emerging mobile phone-based social engineering cyberattacks in the Zambian ICT sector. arXiv 2212:13721. https://doi.org/10.48550/arXiv.2212.13721

Author contributions

Kyoo-Man Ha, as the sole author, was responsible for all aspects of this manuscript, including identifying the research topic, designing the research methods, conducting text analysis, writing a draft file, and finalizing the manuscript.

Competing interests

The author declares no competing interests.

Ethical approval

Ethical approval was not required as the study did not involve human participants.

Informed Consent

This article does not contain any studies with human participants performed by any of the authors.

Additional information

Correspondence and requests for materials should be addressed to Kyoo-Man Ha.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.