ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

The Role of Cybersecurity in Addressing Express Kidnappings: Challenges and Innovative Solutions

Khutso Lebea | Academy of Computer Science and Software Engineering, University of Johannesburg, South Africa | ORCID: 0000-0002-1183-0718

Sherali Zeadally | College of Communication and Information, University of Kentucky, Lexington, KY, USA | Academy of Computer Science and Software Engineering, University of Johannesburg, South Africa | ORCID: 0000-0002-5982-8190

Aditya Sood | Security Engineering and AI Strategy, Aryaka, Santa Clara, CA, USA | ORCID: 0000-0002-7738-2890

Abstract

Countries worldwide are confronting severe threats from organised criminals, with express kidnapping emerging as a particularly concerning form of abduction. Unlike traditional kidnappings, express kidnappings are brief, often lasting only a few hours, during which victims are coerced into withdrawing money from automated teller machines (ATMs) or transferring funds through online or mobile banking applications. The rapid nature of these crimes poses significant challenges to law enforcement and financial institutions, necessitating a proactive, technology-driven cybersecurity approach to mitigation. We examine security-centric mechanisms essential for combating express kidnapping, emphasising the critical role of financial institutions in implementing enhanced cybersecurity measures, such as advanced authentication protocols and real-time fraud detection systems. Our results underscore the necessity of multi-layered advanced security solutions that include artificial intelligence-driven transaction monitoring, biometric authentication, and geofencing to minimise financial

Received: 26.03.2025

Accepted: 03.09.2025

Published: 13.10.2025

Cite this article as:
K. Lebea, S. Zeadally, A. Sood, "The role of cybersecurity in addressing express kidnappings: Challenges and innovative solutions," ACIG, vol. 5, no. 1, 2026, doi: 10.60097/ACIG/210222

Corresponding author:
Khutso Lebea, Academy of Computer Science and Software Engineering, University of Johannesburg, Auckland Park, Johannesburg, South Africa; E-mail: klebea@uj.ac.za
0000-0002-1183-0718

losses and enhance victim protection. Furthermore, public awareness campaigns are vital in educating individuals about precautionary measures, such as transaction limits and emergency banking protocols, to deter potential threats. By adopting a comprehensive approach that integrates technological innovations with policy interventions and law enforcement strategies, governments and financial institutions can strengthen their defences against express kidnappings. This study highlights the urgency of collaborative efforts among cybersecurity professionals, policymakers, and financial service providers to establish a more robust and resilient security framework in response to evolving criminal tactics.

Keywords

cybersecurity, express kidnapping, mobile banking security, online fraud prevention

1. Introduction

Express kidnappings are increasing significantly, posing a growing challenge for law enforcement and increasing insecurity among the public. The rise in express kidnapping is a troubling trend, particularly in regions where economic instability, social inequality, and weak law enforcement converge. South Africa, in 2024, was ranked sixth globally in kidnappings for ransom, after Turkey, Lebanon, Kuwait, Canada, and Belgium [1, 2]. The South African Police Service (SAPS) reported over 4500 cases of kidnappings in the third quarter of 2023, with an average of 50 kidnappings a day [1, 3]. These types of kidnappings have increased exponentially, partly due to the restrictions and technological protection mechanisms put on accounts by financial service providers (FSPs) [3]. It has proven more difficult for criminals to transact on a victim's account without the victim being present because of multi-factor authentication, such as biometric verification, one-time pins, and general security on third-party digital wallets, such as ApplePay, GooglePay, and SamsungPay, security features that are mandated and promoted by FSPs [4, 5]. When certain activities on a victim's account trigger a fraud alert, the FSP will typically put a soft block on the account, contact the account holder via text or phone, and ask for verification and confirmation that they or someone authorised to transacton their account actioned the activity. At this point, the victim is still with the kidnappers and often verifies and confirms the transaction under the threat of life and limb [4]. Funds are transferred from the victim's account into the kidnapper's accounts, usually opened using fake credentials and immediately withdrawn before the FSP's fraud

department is notified. With access to the victim's online banking platforms, the kidnappers can also increase daily ATM and transfer limits [3]. With enhanced cybersecurity measures, FSPs could mitigate this issue by tracking unusual activity on users' accounts and implementing measures that will reduce the financial loss and avoid loss of life and serious injuries.

People who are victims of express kidnappings, or any crime that results in financial loss, typically contact their FSP after being released or after realising that their money has been taken to reverse the transactions. However, most FSPs in South Africa have terms and conditions on their online platforms that state that the institution is not liable for transactions made on a client's account before the institution is notified of unauthorised or fraudulent transactions [1]. These terms and conditions restrict the National Financial Ombud (NFO), an organisation that investigates and resolves complaints against FSPs, from acting against them [1, 3]. Typically, FSPs can refund a portion of the loss, usually to a maximum of 50%, as a gesture of goodwill, which is at the service provider's discretion, meaning that there is no guarantee that this partial refund will be made to most clients [1].

Advancements in information technology are partly to blame for the increase in express kidnappings because clients no longer need to go to their FSP branch to change ATM and transfer limits [2]. These technological advancements are often introduced without security considerations, and the typical metric for assessing success is often convenience and not security, which in most cases is an afterthought add-on. Banking is no longer somewhere one goes; it is something one does on one's smartphone and personal computer, further showing the inverse relationship between security and convenience. The solution to express kidnapping should be technological advancements.

1.1. Research Question

The main research question this work addresses is: 'How can advanced cybersecurity measures in financial institutions mitigate the risks associated with express kidnappings?'

1.2. Research Contributions

The main contributions of this paper are as follows:

1. Exploring technological solutions for kidnapping prevention and mitigation, as the South African NFO sets out.

2. Exploring technological measures that smartphone users can use right now to reduce the financial loss due to express kidnappings.
3. Lastly, there will be a discussion of solutions that FSPs can adopt on their online platforms to reduce the financial impact for victims in the future.

This paper explores how advancements in cybersecurity can be used to reduce the financial losses experienced by victims of express kidnappings and potentially other forms of financial application frauds. We aim to bring awareness to this research field and propose several solutions with theoretical benefits to implement and evaluate their efficacy in the future. Section 2 describes what express kidnappings are. Section 3 highlights the express kidnapping attack cycle and draws distinctions between traditional kidnapping and express kidnapping, while Section 4 explores the recommendations of the South African NFO and other industry experts for victims and potential victims. Section 5 highlights the technological advancements in cybersecurity that can help victims and potential victims; these technologies are currently being used in other industries. This section focuses on how FSPs can implement technology to reduce financial damage. Section 6 explores mechanisms that currently exist and are employed by various FSPs, which users may not be aware of, while Section 7 recommends cybersecurity measures and features that FSPs should consider implementing. Finally, we make some concluding remarks in Section 8.

2. Background

Express kidnapping is a type of abduction where, unlike traditional kidnapping, the victim is held for a short period; the intention of the kidnapping is typically to extort money from the victim quickly and the victim's family or employer [1]. This type of kidnapping often targets citizens in the middle class, tourists, and people who are perceived to have quick access to money. The victim is forced to withdraw money from ATM or give the kidnappers their credentials for access to their online banking platforms [2]. Express kidnapping is prevalent all over the world. However, its impact is felt more in certain parts of the world, particularly in regions where economic hardship, weak law enforcement, and organised crime intersect. The swift nature of these kidnappings, combined with the relatively low ransom demands, makes them attractive to criminals seeking immediate financial gain with minimal risk.

Table 1. Countries with the highest rates of kidnappings [6].

Country	Kidnappings per 100,000 people
Turkey	42.669
Lebanon	15.384
Kuwait	12.69
Canada	10.285
Belgium	10.245
South Africa	9.569
New Zealand	9.508
Pakistan	9.452
Eswatini	9.354
United Kingdom	8.835

Table 1 illustrates the top 10 countries with the highest rate of kidnappings per 100,000 people. This list illustrates that kidnappings are not exclusive to developing countries, with countries like Canada, Belgium, New Zealand, and the United Kingdom in the top 10 [6]. It is important to note that Table 1 illustrates all types of kidnappings and is not limited to express kidnappings.

Developed countries generally have a better way of dealing with kidnapping through advanced law enforcement capabilities. These include well-trained and well-equipped specialised task forces with quick response time and surveillance combined with sophisticated technology, such as closed-circuit television (CCTV) networks across major cities. Developed countries typically also have strong legal frameworks intended to discourage criminals [7].

Several factors contribute to the rise of express kidnappings—first, economic hardships with high levels of poverty and unemployment. Second, weak law enforcement reflects the low likelihood of apprehension and prosecution, where police and legal systems are under-resourced or corrupt. Third, organised crime involves express kidnappings as a part of broader criminal activities, which are lucrative and low-risk enterprises. Fourth, the ease of ransom payment has increased due to the proliferation of ATMs, mobile banking, and digital payment systems. Obtaining ransom money has become a matter of hours, not days. Fifth, there is difficulty in identifying criminals because express kidnappings often occur in crowded urban areas, which makes it harder for the victims to provide accurate descriptions to authorities to track the criminals [8].

These challenges illustrate the complexity of addressing express kidnapping and highlight the need for a comprehensive approach and advanced technology solutions.

3. The Attack Cycle

Unlike high-value kidnappings for ransom, which involve meticulous planning and an extended attack cycle, express kidnappings are often crimes of opportunity with a much shorter attack cycle. Express kidnappers typically operate as ambush criminals, lying in wait near potential attack sites for a suitable victim to cross their path [5, 9].

The reality is that kidnappings do not simply occur by chance; they typically follow a version of a discernible process that can be detected and interrupted. Figure 1 depicts the attack cycle of this process [5].

3.1. Target Identification and Selection

High-value kidnappings typically start with identifying a potential target. In contrast to kidnappings, the planning and preparation phase of the cycle typically occurs first, and the amount of surveillance on potential targets is normally very limited [3].

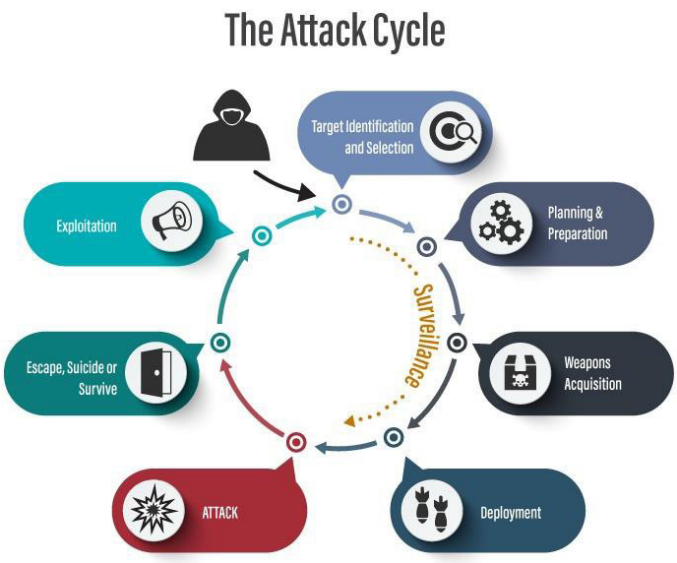

Figure 1. The attack cycle of kidnappings [9].

Selecting the target occurs quickly, often based on superficial assessments. The kidnappers typically conduct minimal surveillance to identify a victim who appears to have enough money to make the crime worthwhile and who seems vulnerable to an ambush [9].

3.2 Planning and Preparation

While express kidnappings involve less meticulous planning, compared to high-value kidnappings, some level of preparation still occurs. Kidnappers choose locations where potential victims are likely to be found, such as ATMs, upscale hotels, shopping areas, or entertainment districts. They also plan their method of ambush by lurking near these sites in 'gypsy' cabs [2, 9]. Gypsy cabs are unlicensed and unregulated taxis that operate outside of the legal taxi system. They are typically vehicles that appear to function as regular taxis but lack the official permits, insurance, and oversight required for legitimate taxi services. Gypsy cabs are often found in areas where there is high demand for transportation but limited availability of licensed taxis, making them an attractive option for unsuspecting passengers [9].

3.3. Deployment

The actual kidnapping is swift and opportunistic. Once a suitable target is identified, the kidnappers move quickly to carry out the ambush [5]. This could involve confronting the victim near isolated ATMs, intercepting them in a vulnerable location, pulling them into an alley with the help of an accomplice or using unlicenced cabs to take them to another location [9].

3.4. Escape, Suicide, or Survive

After securing the victim, the kidnappers usually force them to withdraw money from ATMs or demand money to be transferred into several accounts. The process is designed to be fast, minimising the chances of law enforcement intervention [3, 9].

3.5. Exploitation

As a result of advances in anti-fraud mechanisms and daily limits on ATM transactions and transfers, the kidnappers must keep the victim close for application authentication and verification. They will sometimes hold the victim longer to avoid exceeding the daily limit and try the transactions the next day. The cycle ends with the kidnappers fleeing the scene after obtaining the ransom or valuables [9].

The South African NFO is aware of the increasing number of express kidnappings and has published recommendations to customers on how they can potentially avoid becoming victims.

4. The National Financial Ombud's Recommendations

The recommendations published by the NFO are as follows [1–3]:

- Be cautious when posting online.
- Consider duress insurance.
- Do not draw unwanted attention to yourself.
- Vary your daily routine as often as possible.
- Consult your bank.
- Consider investment options.

'Be cautious when posting online': This recommendation burdens the individual to avoid becoming a target. It overlooks the need for broader societal and systemic interventions, such as better law enforcement, regulatory oversight of social media, and efforts to address the root causes of criminal behaviour, like poverty and inequality [5].

'Consider duress insurance', 'Consult your bank', and 'Consider investment options': These recommendations assume a level of financial stability that many potential victims may not have as express kidnappers are opportunistic. They do not necessarily target high-net-worth individuals [3]. This can create a sense of insecurity or inadequacy in those who cannot afford such measures while potentially increasing the sense of vulnerability among those with significant assets.

While insurance can provide a financial safety net, it also commodifies safety and security, potentially creating a two-tier system where only those who can afford such policies are adequately protected.

Insurance fraud is a potential issue with this recommendation; fraudsters could exploit their insurer by staging their kidnapping and pretending that any actions or payments were made under duress [4].

'Do not draw unwanted attention to yourself' and 'Vary your daily routine as often as possible': These types of advice can subtly imply that it is the victim's responsibility to avoid being targeted.

These recommendations may overshadow the fact that the responsibility for crime lies solely with the perpetrators. Such guidance might also reinforce the idea that victims could have prevented the crime by being more cautious.

One way FSPs can track fraudulent behaviour on a customer's account is through routine monitoring of account activity and behaviours, and some of the routines include which ATMs and stores the person frequents. Varying this routine can negatively impact FSPs dealing with potential fraudulent transactions [4, 10].

While the recommendations given by the NFO have drawbacks and hints of victim-blaming, these have positive aspects that can be beneficial, such as advocating for awareness, caution, and digital literacy, particularly in environments where express kidnappings are likely to happen. The recommendations also encourage preparedness from a financial and legal point of view; knowing one's options can help manage risk [1].

Some FSPs use mechanisms such as behavioural tracking on their platforms as a form of fraud detection. The next section discusses technologies that FSPs use to protect their customers.

5. FSP Technological Advancements

Some FSPs' mobile apps have state-of-the-art security features, such as geo-fencing and user behavioural tracking [5]. These features protect the user and quickly notify the FSP when there is reason to believe there is unauthorised or fraudulent behaviour on a client's account.

5.2. Detection of Anomalous Behaviour

Financial apps can use machine learning (ML) and artificial intelligence (AI) algorithms to analyse users' normal behaviour patterns, such as the time of day they typically access the app, their usual transaction amounts, and the devices or locations from which they typically login. If the app detects deviations from these patterns, it can flag the activity as suspicious [4, 10].

Behavioural tracking can incorporate multiple contextual factors before allowing a transaction to proceed [11]. The app might consider the user's device, location, transaction history, typing speed, or interaction patterns to assess whether the transaction is legitimate [4].

5.2. Geo-Fencing

Some apps can use geo-fencing to block transactions based on locations not within the user's usual area, and only certain non-critical functionality will be allowed outside of the user's safe zones [11]. This reduces the risk of unauthorised transactions during an express kidnapping, where kidnappers might force the victim to perform transactions from an unfamiliar location [4].

Upon detecting such anomalies, the app can immediately alert the user through SMS, call, or email, allowing them to confirm or deny the transaction. The app may automatically freeze the account or require additional authentication if the user does not confirm the transaction [3].

Under duress, the kidnappers may request the victim to confirm the transactions. The NFO advises that measures like declining or delaying the processing of transactions could result in harm or even the victim's loss of life, which would not be a justifiable outcome, compared to financial protection such as insurance [3].

Geo-fencing, in this instance, can be used to turn off certain features of the app when a user is outside of their trusted zones. Certain accounts can be de-linked from the app and will not be visible or accessible. Withdrawal and transfer limits can be reduced without the option to increase them if these requests and transactions are made outside of the trusted geographical locations set up by the user and their routine [11].

There are technological features that people can use now to minimise the financial loss resulting from express kidnappings, depending on their smartphone and the FSP they bank with. The next section covers features that banking customers can use to minimise the impact of express kidnappings.

6. Current Technological Features to Reduce the Financial Impact of Express Kidnappings

Financial apps typically show all the linked accounts that belong to the customer with that specific FSP.

6.1. Hidden Accounts

These apps allow users to hide certain accounts by following a few steps in the app's settings. It is important to note that these accounts are not de-linked from the app but are hidden.

Kidnappers familiar with that FSP's mobile app will likely look for hidden accounts [12]. Users are advised not to hide all their accounts, only those with large amounts of money, so the kidnappers will not be incentivised to look for other accounts in the app [12].

6.2. De-link Accounts

People with access to business and other non-personal accounts or high net worth are advised to de-link those accounts from their banking apps [3]. They should rather go to the physical FSP branch to transact or use investment platforms that do not transact online but through a banker or a broker. This solution reduces the convenience of being able to transact online. Still, it makes the accounts more secure because the transaction must occur at a specific place, and there is typically a lengthy process that requires multiple people to access the money. The overhead of these accounts does not fit the modus operandi of express kidnappers [1, 2].

Change the App Name and Icon: One way to prevent kidnappers from accessing funds on a smartphone is to change the app's name and icon to something random, such as a non-financial or utility app, such as a weather app or a game. Some apps, including FSP, allow the name and icon to be changed natively. App names and icons can also be changed using third-party mobile applications on Android and iPhone Operating Systems (iOS).

This change is simple, but it is an effective security measure in areas where express kidnappings are common. This is because the changed app icon and name may not immediately alert the kidnapper about the presence of a financial app on the device. The victim can always claim that they do not have financial apps on the device or that their money is saved with investment institutions, as the NFO advises [1].

The issue with this approach is that several apps have a finite set of app icons and names a user can choose from; not all operating systems and native implementations of this feature are fully customisable, so kidnappers with prior knowledge of the implementation would know to first look for the set of app names and icons when they cannot find the original app icon and name [3].

Third-party applications allow for full customisation but have more of a learning curve and steps to get it done. The recommendation is

to use third-party icons and name-changing applications; that way, even kidnappers with knowledge of the app would potentially have to open every app on the device to find the banking app.

6.3. Hide Apps

A step further would be hiding the app in a separate operating system on the device. Android15 has a new 'Private Space' feature that allows smartphone users to hide sensitive apps previously available through third-party apps [12]. Samsung has had it since the GalaxyS21 called the 'Secure Folder', a security platform that offers robust protection for sensitive data stored on Samsung devices. It integrates hardware and software to create a secure environment and allows users to make duplicate apps. It is essentially a virtual machine running on the device, and it is accessed through an app that uses a custom icon and name to avoid easy detection. The icon Android devices using Android15 will have a similar native secure environment [12].

IOS users can hide apps on their devices. This feature removes the app from the home screen and will not appear in search results, making it seem like the app is not installed on the device. It is also possible to hide an entire page of apps [12]. This approach suffers from the same issues as changing the app icon. Kidnappers who know about the operating system will start by looking for hidden apps or app pages. The Samsung solution has a limited number of app icons. However, third-party apps can be used for more variety.

6.4. Use Multiple FSPs

By maintaining multiple accounts across different service providers, individuals can limit the amount of money readily accessible in an FSP's app. If one app is compromised, the kidnappers may only gain access to a limited number of accounts, reducing the financial impact.

6.5. Diversification of Financial Products

Keeping credit cards, debit cards, and other financial products with different FSPs can spread out the risk, with products like credit cards typically having more security and fund protection features. One FSP might be used for day-to-day expenses, while another for savings, making it harder for kidnappers to access all the distributed financial resources.

It is worth mentioning that getting multiple products can come at a higher cost than keeping all the services and products with one FPS.

6.6. Recovery Efforts

From the point of finding the victim during captivity, one should enable features that will allow family and trusted friends to find them if they should ever get kidnapped; iOS has 'FindMyiPhone', and Android has 'FindMyDevice' [13]. Because the smartphone needs to be connected to the Internet for the kidnappers to transact, either via mobile data or Wi-Fi, family and friends should be able to track the whereabouts of the device and can share it with law enforcement.

Many smartphones have built-in emergency SOS features. For example, rapidly pressing the side button five times on iPhones can automatically call emergency services and send your location to pre-selected emergency contacts. Android devices have similar features that can be configured under 'Emergency SOS' settings [13]. These features are designed to be activated discreetly, potentially allowing the victim to call for help before the kidnappers can find and take the smartphone.

These recovery efforts may not be very useful if the victim is not held captive for an extended period, which is typically what happens in express kidnappings [1].

The next section looks at possible additions to the above-mentioned features, including experimental solutions and those not already used on online financial platforms.

7. Recommended Features for FSP Adoption

Apart from hiding accounts, de-linking accounts, and hiding financial apps, this paper proposes creating credentials that automatically notify the FSP when used. This can be a different biometric or a username and password combination that will login to the app and only show accounts with small amounts of money. Even when the original credentials have all the apps-linked accounts and functionality, the FSP is alerted when the victim logs in and can monitor activity and flag any accounts where money is transferred.

The victim's location can be traced and sent to law enforcement agencies. Suppose the kidnappers are using the victim's device. In this case, the app can discreetly use the front-facing camera and microphone to

record the kidnapper's face and events during the transactions on the app. The video captured by the app can be used to identify the kidnappers and be potentially used as evidence in court.

7.1. Duress Detection

FSPs should prioritise calling clients when the system suspects fraudulent activity. Typically, the FSP representative on the phone will ask the client authentication questions [1]. FSPs should set up duress questions and answers for clients; instead of only getting authenticated or not, there should be another option where the client is authenticated under duress.

Advancements in technology can allow the FSP to detect duress through voice during the client authentication process [14].

The transactions should be allowed to go through, or partially so, but the point is that the FSP will be aware that the client is under duress and will take the necessary precautions.

It should be noted that since the FSP's terms and conditions state that the institution is not liable for any transactions that happen on a customer's account before they are notified, the recommendations in this paper make it so that the FSP is notified as soon as the victim logs in that they are under duress. Therefore, all transactions should be deemed fraudulent or unauthorised. These recommendations may potentially not be implemented by FSP because the institution would now be liable to refund the client after the fact, and this refund could be enforceable by the NFO, should the client's complaint get that far.

The recommendations offered above are meant to reduce the financial loss of express kidnappings and are aimed at catching the kidnappers. These recommendations should be implemented so that it is extremely difficult to cheat and thus disincentive fraud.

To compensate for the potential refunds, FSP should institute an account fund insurance; this insurance premium can be added to the account's monthly fee. Any legitimate case of express kidnapping would be paid out from that insurance scheme.

7.2. Risk versus Benefits

While the proposed cybersecurity measures offer significant potential for mitigating financial losses during express

kidnappings, their implementation introduces certain risks and operational challenges. Understanding these trade-offs is critical for both FSPs and end-users before large-scale adoption. This analysis examines the recommended solutions (i.e. duress detection, geo-fencing, anomaly detection, and app obfuscation) mentioned earlier against two key dimensions:

- *Benefits*: The positive impact on security, user safety, and fraud prevention.
- *Risks and challenges*: Technical, operational, ethical, and user-experience concerns that may arise from adoption.

This analysis will help stakeholders weigh the practicality and feasibility of integrating these solutions into the existing financial ecosystems while minimising unintended consequences, such as privacy violations, false positives, or system misuse.

The adoption of duress detection mechanisms provides a critical advantage by enabling real-time alerts to FSPs when users are coerced during transactions. This feature could reduce financial losses and expedite law enforcement intervention, potentially saving lives [14]. However, the implementation carries significant risks, including false positives that may occur when stress is detected in legitimate transactions, leading to unnecessary account freezes or alerts. Additionally, the use of voice-based or behavioural cues introduces privacy concerns and requires strong safeguards against misuse [14].

Geo-fencing technology enhances security by restricting high-value transactions to predefined safe zones, significantly reducing the likelihood of unauthorised transfers during express kidnappings [11].

Table 2. **Recommended Solutions' Benefits versus Risks.**

Recommended solution	Benefits	Risks/challenges
Duress detection	Immediate alert, law enforcement activation	False positives, privacy concerns
Geo-fencing	Immediate alert, law enforcement activation	Can fail if victim is in safe zone
Anomaly detection	Early detection of fraudulent actions	Data privacy and compliance with protection regulations
App obfuscation	Reduce kidnappers' access to large sums of money	If discovered, could escalate violence
Camera/microphone activation	Evidence collection, assists investigation	Major privacy and legal implications

Despite this benefit, geo-fencing could fail in scenarios where kidnappers force victims to operate within their usual locations or where GPS accuracy is compromised [11]. Moreover, strict enforcement might inconvenience legitimate users travelling outside trusted zones, potentially causing customer dissatisfaction [3].

Machine learning-based anomaly detection is another powerful solution that identifies unusual account activity based on behavioural patterns, such as transaction time, amount, or device type [4, 10]. Its primary benefit lies in early detection of fraudulent actions, improving response times and reducing financial damage [10]. However, such systems require extensive data for training, raising concerns about data privacy and compliance with protection regulations [4]. Additionally, high sensitivity in detection models can result in operational inefficiencies due to false alarms [4].

Measures like app obfuscation, hidden accounts, and secure folders significantly decrease the probability of kidnappers accessing critical financial applications [12]. These techniques are of relatively low-cost and easy to implement on user devices. Nevertheless, their effectiveness depends on user awareness and technical ability [12]. Furthermore, if kidnappers are aware of these methods, they may escalate violence to force victims to reveal the concealed applications, introducing physical risks [1, 3].

Camera and microphone activation during duress events offers unparalleled investigative benefits by capturing evidence that can assist in identifying perpetrators [14]. However, this approach is ethically complex and legally sensitive because it involves covert recording without explicit consent, which could violate privacy laws in several jurisdictions [7]. To mitigate these risks, encrypted storage, transparent consent mechanisms, and strict access controls must accompany such implementations [7, 14].

7.3. Ethical and Privacy Concerns

Integrating advanced cybersecurity solutions raises critical ethical and privacy concerns that must be addressed before deployment. These issues primarily include user consent, surveillance, and data security. Covert activation of cameras and microphones during duress situations, while highly beneficial for collecting evidence, could violate individual privacy rights and data protection regulations without clear user consent [7]. Such measures may conflict with local and international laws, including provisions under data privacy frameworks, like the Protection of Personal

Information Act (POPIA) [15] in South Africa and the General Data Protection Regulation (GDPR) [15] in Europe. To mitigate these risks, FSPs must adopt explicit opt-in consent, transparent usage policies, and secure data storage mechanisms, such as end-to-end encryption [7, 14].

Using geo-fencing and behavioural tracking introduces the possibility of constantly monitoring users' movements and financial habits, which, if mismanaged, could lead to profiling or misuse of personal data [11]. While these technologies enhance security, the perception of over-surveillance could erode customer trust in financial institutions. Addressing this requires implementing data minimisation principles, where only essential data is collected, and ensuring that location-based data is anonymised and purged periodically after analysis and use [4, 11].

Machine learning-based anomaly detection relies heavily on user behavioural data to identify suspicious activities [4, 10]. Such data aggregation could expose users to identity theft or fraud if compromised. This underscores the need for robust security protocols, including strong encryption, strict access controls, and regular security audits, to ensure data integrity and confidentiality [10].

Duress detection systems leveraging voice analysis or biometric signals present ethical dilemmas concerning informed consent and accuracy [14]. False positives during authentication could lead to unnecessary account freezes, customer inconvenience, and reputational harm for financial institutions. To counter these risks, FSPs must establish clear accountability mechanisms and allow users to opt out of certain high-intrusion features without compromising basic account security [14].

While these advanced security mechanisms can significantly reduce financial risks associated with express kidnappings, their implementation must align with ethical principles of autonomy, transparency, and proportionality. Balancing security with privacy is essential to ensure that protective measures do not result in unintended harm or regulatory violations.

8. Conclusion and Future Work

Express kidnappings pose a significant threat, not just to personal safety but also to financial security in South Africa. As criminals increasingly leverage technology to exploit victims, robust, proactive solutions are critical. The financial sector must

continue to innovate and strengthen security measures like those covered in this paper, such as anomalous behavioural tracking, duress detection, and real-time fraud detection. As discussed in this paper, the recommendations from the NFO of South Africa are not without issues. However, they provide a good starting point where

Integrating technology and awareness can help educate people on securing their digital identities and using the advanced features of banking apps and smartphones.

This paper explored how advanced cybersecurity measures in financial institutions can mitigate the risks associated with express kidnappings. These cybersecurity mechanisms can assist financial institutions in dealing with financial losses. Another goal of this paper is to promote advanced cybersecurity solutions for use in banking applications, with a focus on financial loss due to express kidnappings.

The NFO has warned that FSP would be forced to pay money back to victims of express kidnappings if it is found that the FSP could have done more to help the victim [1]. The adoption of technology-driven solutions discussed in this paper could significantly reduce the financial impact of express kidnappings, providing both protection and peace of mind to potential victims and FSPs.

As part of our future work, we will implement the proposed solutions we have described in this paper and evaluate how effective they would be in reducing the financial losses associated with express kidnappings. To date, we have already developed systems that aim to reduce the financial loss because of express kidnappings, using mechanisms such as facial recognition for anomaly detection during the login process, typing speed analysis for pin and password typing, and the potential for using the heart rate from companion apps running on wearable devices, such as smart watches. The current work is exploring the pros and cons of these mechanisms and evaluating them in the real world and collect user feedback on user-friendliness, learning curve, intrusion of privacy, and so on.

Acknowledgements

We thank the anonymous reviewers for their valuable comments, which helped us to improve the content, organisation, and presentation of the paper.

References

[1] N. Moodley. (Aug. 14, 2024). *Ombudscheme sounds alarm over rise in 'express kidnappings' as bank security tightens*. [Online]. Available: https://www.dailymaverick.co.za/article/2024-08-14-ombud-scheme-sounds-alarm-over-rise-in-express-kidnappings/. [Accessed: 10 Sep. 2024].

[2] BusinessTech. (Jun. 4, 2024). *Warning over 'express' kidnapping in South Africa*. [Online]. Available: https://businesstech.co.za/news/lifestyle/775200/warning-over-express-kidnapping-in-south-africa/. [Accessed: 11 Sep. 2024].

[3] MyBroadband. (Jul. 7, 2024). *Kidnapping payment conundrum in South Africa*. [Online]. Available: https://mybroadband.co.za/news/security/543413-kidnapping-payment-conundrum-in-south-africa.html. [Accessed: 10 Sep. 2024].

[4] S. Palvel. (Sep. 15, 2023). *Anomaly detection in financial transactions*, Medium. [Online]. Available: https://subashpalvel.medium.com/anomaly-detection-in-financial-transactions-e895847e99d3. [Accessed: 12 Sep. 2024].

[5] M. Maras, J. Arsovska, "Understanding the intersection between technology and kidnapping: A typology of virtual kidnapping," *International Criminology*, vol. 3, no. 2, pp.162–176, 2023, doi: 10.1007/s43576-023-00091-4.

[6] Population Matters. (2024). *Kidnappings per country 2024*. World Population Review. [Online]. Available: https://worldpopulationreview.com/country-rankings/kidnappings-per-country. [Accessed: 12 Sep. 2024].

[7] United Nations Office on Drugs and Crime (UNODC). *Countering kidnapping and extortion*. [Online]. Available: https://www.unodc.org/unodc/en/terrorism/expertise/countering-kidnapping-and-extortion.html. [Accessed: Sep. 15, 2024].

[8] I. Bello, I.M. Jamilu, "An analysis of the causes and consequences of kidnapping in Nigeria," *African Research Review*, vol. 11, no. 4, pp. 134–143, 2017, doi: 10.4314/afrrev.v11i4.11.

[9] S. Stewart. (Nov. 18, 2022). *Kidnapping part 3: Express kidnapping*, TorchStone. [Online]. Available: https://www.torchstoneglobal.com/express-kidnapping/. [Accessed: 11 Sep. 2024].

[10] G. Folino, C. Otranto Godano, F.S. Pisani, "An ensemble-based framework for user behaviour anomaly detection and classification for cyber security," *The Journal of Supercomputing*, vol. 79, no. 11, pp.11660–11683, 2023, doi: 10.1007/s11227-023-05049-x.

[11] Y. Shevchenko, U. Reips, "Geofencing in location-based behavioral research: Methodology, challenges, and implementation," *Behavior Research Methods*, vol. 56, pp. 6411–6439, 2024, doi: 10.3758/s13428-023-02213-2.

[12] N. Ndlovu. (Jul. 9, 2024). *Banking app kidnappings: How to hide your apps*, TechCentral. [Online]. Available: https://techcentral.co.za/banking-app-kidnappings-hide-your-apps/247637/. [Accessed: 10 Sep. 2024].

[13] L. Savvides. (Jun. 20, 2024). *I compared Apple's FindMyNetwork and Google's FindMyDevice: Here's the clear winner*, CNet. [Online]. Available: https://www.cnet.com/tech/mobile/i-compared-apples-find-my-network-and-google-find-my-device-heres-the-clear-winner/. [Accessed: 12 Sep. 2024].

[14] E.J. van Rensburg, R.A. Botha, B. Haskins, "Identifying duress through voice during speaker authentication," Proceedings. 2023 *International Conference on Electrical, Computer and Energy Technologies (ICECET),* Cape Town, South Africa, 2023, pp. 1-5, doi: 10.1109/ICECET58911.2023.10389204.

[15] K. Lebea, W.S. Leung, "What data are your smart home devices collecting?" in *Intelligent sustainable systems*. *Selected papers of international conference on WorldS4 2024*. *Lecture notes in networks and systems*, vol. 1180, A. Nagar, D.S. Jat, D. Mishra, A. Joshi, Eds. Singapore: Springer, 2025, pp. 175–185, doi: 10.1007/978-981-97-9559-8_15.