Developing Guidelines for the Prevention and Suppression of Online Fraud Crimes: Guidelines for Law Enforcement by Police Officials in the Investigation.

Dithapart Borwornchai, Subhorn Kitchombhu, Manasnan Kanthasi
Thaksina Mektraitrat, Phimphoj Nhomchopphitak, Pipat Janruam, Isarawut Aonnom,
Sutham Cheuaprakhobkit and Worasorn Netthip
*Faculty Division, Royal Police Cadet Academy, Mahidol University
And Srinakharinwirot Univetsity
Email: teacherjack_58@hotmail.com

Received June 03, 2025 Revise July 16, 2025 Accepted July 17, 2025

Abstract

The rapid evolution of communication technology and the internet has transformed access to online platforms, offering both convenience and increased susceptibility to online fraud. This research investigates the operational conditions and challenges faced by law enforcement agencies in Thailand regarding the enforcement of laws related to online fraud. Employing a comprehensive methodology that includes document analysis, in-depth interviews with victims and police officials, and focus group discussions, the study identifies critical factors contributing to the victimization of individuals, including a lack of awareness and the deceptive tactics utilized by criminals. Findings reveal significant barriers within law enforcement, such as limited personnel and specialized expertise, insufficient investigative tools, and coordination delays with financial institutions. Furthermore, legal inconsistencies hinder effective prosecutions and deter victims from reporting incidents. To address these challenges, the research advocates for the establishment of specialized task forces dedicated to online fraud, streamlined processes for rapidly freezing implicated bank accounts, and enhanced collaboration across jurisdictions and sectors. The study emphasizes the need for ongoing training and resources to strengthen law enforcement responses to online fraud, alongside community awareness programs to empower individuals against potential scams. Ultimately, this research aims to contribute to the formulation of effective practices and policies for combating online fraud, fostering a safer digital environment for consumers and restoring trust in law enforcement as an effective guardian against technological crimes. Recommendations in Terms of Practical Should to be Promote Public Awareness Campaigns: Launch nationwide awareness programs aimed at educating the public about online fraud prevention. These initiatives should focus on informing citizens about common scams, safe online behaviors, and the importance of verifying the credibility of online transactions.

Keywords: Developing Guidelines, Prevention and Suppression, Law Enforcement, Investigation; Online Fraud

Introduction

The evolution of communication technology and the internet has significantly enhanced the population's access to online platforms. While engaging in activities within these online spaces offers convenience and rapid communication, it can inadvertently lead individuals to become victims of crime. Conversely, criminals exploit various online avenues to commit certain types of offenses, facilitating easier access to potential victims in ways that far exceed traditional face-to-face methods. One such offense is online fraud, which results in

substantial losses for victims, affecting both their property and inherent rights. Furthermore, the ramifications include heightened feelings of insecurity regarding online safety among users and diminished confidence in law enforcement authorities' capability to prevent and address incidents of online fraud (Drew, J.M. 2020; Diarmaid, H., & Chad, W. 2021; Danquah, P., & Longe, O., 2011).

The Thai Criminal Code B.E. 2499 (1956) defines fraud as the act of a criminal involving the provision of false or incomplete factual information to victims with fraudulent intent, resulting in direct or indirect benefits to the perpetrator. This definition is broad and can be interpreted to encompass incidents not only in face-to-face interactions between victims and criminals but also in today's society, where increased access to computers and the internet allows various crimes, including fraud, to manifest in online spaces (Buil-Gil, D., & Zeng, Y., 2021).

Forms of computer-based fraud may include social media scams that typically require interaction in online environments from both the offender and the victim. Examples include romance scams, selling products with no intention of delivering them or delivering substandard goods to customers, soliciting investments in nonexistent multi-level marketing schemes, investing in gold and foreign currencies, or engaging in Ponzi schemes. Additionally, fraudulent activities may also occur through the unilateral access of criminals to victims via the internet. For instance, using Voice over IP (VoIP) technology to contact victims over the phone to deceive them into surrendering their property, such as in cases involving call center gangs tricking individuals into believing they are suspects in drug cases or DHL scams regarding undelivered mail. All these activities fall within the legal definition of fraud as stipulated by the law. Furthermore, the forms of criminal acts and the benefits sought by criminals may change over time, including the acceptance of digital currency as a form of benefit (Atul, B., Lhato, J., & Alka, R, 2018).

The reasons for falling victim to online fraud can arise from various personal factors. It can be said that victims often lack awareness of the criminals' deceptive tactics. This includes technological scams; for instance, criminals may sometimes leverage their expertise to create fake websites to mislead victims into providing important financial information. They may also use technology to spoof phone numbers to contact or message victims, among other tactics. Additionally, scams can occur during interpersonal interactions. For example, if a victim tends to be gullible, compassionate, or trusts strangers too easily, criminals may exploit this by utilizing principles known as social engineering (Abas, S.N. et al., 2017; Bandler, J., & Merzon, A., 2020) to establish familiarity during the interaction, leading the victim to place their trust and belief in the scammer. Moreover, criminals might simulate the behaviors of officials from various agencies to instill fear in victims, thus coercing them into compliance.

At the societal level, the government plays a crucial role in formulating policies to prevent and combat crimes affecting the public, including remediation efforts. The impacts arising from online fraud not only undermine trust in the effectiveness of state officials involved in cybersecurity but also affect the economic system at both household and national levels. Therefore, the mechanisms employed by the government to address cybersecurity issues must be established and implemented in a timely manner to genuinely resolve the problems faced by the public. This encompasses both policy and legal dimensions, such as disseminating information about criminal scams to create immunity against victimization, fostering cooperation among different organizations to collect cyber evidence, and establishing clear operational guidelines and accountability for agencies handling online fraud cases to reduce public confusion. These measures are essential to reduce the incidence of

online fraud victimization (Abas, S.N. et al., 2017; Drew, J. M. 2020; P., & Longe, O., 2011; W., & Diarmaid, H., 2019).

The phenomenon of online fraud can be explained through various criminological theories. In terms of victimization, according to victimology, victims of online fraud may be considered "victims of technology" or individuals affected by technological advancements. This aligns with descriptions provided by Routine Activity Theory, which suggests that victims may lead lifestyles that inadvertently create opportunities for criminals to commit offenses (W., & Diarmaid, H., 2019; Emami, C., et.al., 2020; Khruakham, S. 2015). For instance, victims often shop online without verifying the credibility of the seller or may purchase directly without intermediaries, making them susceptible to exploitation due to this lack of diligence or protective measures.

Additionally, through the lens of Strain Theory, while the theory typically addresses criminals seeking to possess assets to gain social acceptance through illegal means (Innovation in Modes of adaptation), such pressures can also be relevant to victims of online fraud. For example, victims may engage in online gambling, participate in investment schemes, or join unregulated collective investments without realizing they are being deceived (Jaishankar, K. 2007; Jaishankar, K. 2008; Khruakham, S. 2015).

From the criminal perspective, online fraud can also be analyzed through Rational Choice Theory, which discusses how criminals weigh the factors that facilitate criminal activity against the potential consequences they may face (Junger, M.,et.al.., 2020; Kshetri, N. 2013; Seksan Khruakham, S. 2015). If criminals possess the expertise to deceive or evade through technology and conceal evidence, they may choose to commit offenses given the high potential rewards compared to the relatively minor penalties if apprehended.

Lastly, in the context of state crime prevention, ineffective measures that lag behind technological advancements, legal limitations, or other factors regarding the state's ineffectiveness in preventing online fraud may correspond with Deterrence Theory. This theory posits that effective crime prevention by the authorities-whether general or specific-must occur rapidly, with severe penalties appropriate to the crime, and definitive punishments for criminals; otherwise, crime will persist and potentially increase. There is a need for further research to assess how well these criminological theories, both discussed and undiscovered, can explain the phenomenon of online fraud, predict crime trends, and guide adjustments in strategies aimed at reducing such incidents (Kai, L. et.al.2023; Liang, H., & Xue, Y., 2010; Khruakham,S. 2015).

According to the statistics of reported cases by the National Police Agency, there were a total of 781 cases of fraud committed through computer systems within the Thai jurisdiction in 2021 (Cyber Crime Investigation Bureau, 2021). Although the National Police continuously surveys and compiles crime statistics, these figures have deficiencies as they only reflect the statistics of cases reported to the police. The actual number of criminal cases may be higher. These causes can broadly be divided into two main categories: those related to victims and those concerning the police officials themselves.

For victims, the reasons may stem from individual awareness, such as not realizing they have fallen victim to fraud (Drew, J. M. 2020; Liang, H., & Xue, Y., 2010). They may lack experience or knowledge about the reporting process, or they may perceive the incident as insignificant or ordinary. In some instances, victims may feel they can handle the situation themselves or fear retribution from the criminals (Tarling R., & Morris, K, 2010; Michail, G. 2014). Additionally, victims may have a lack of trust in the law enforcement process, feeling that reporting a crime is cumbersome, believing that the police are unable to help, feeling

neglected regarding their case, harboring personal dislike or fear of police officers, or having had negative experiences with the justice system (Tarling R., & Morris, K 2010).

Regarding police officials, the discrepancy between the actual number of criminal cases and the recorded statistics may arise from instances where reports have been filed, but the police have not logged the data into the statistics sent to the National Police Agency. Such statistics do not reflect victims' awareness of the crimes that occur, potentially mitigating the chances of becoming a victim. Moreover, this situation underscores the challenges faced by police officers in effectively preventing and combating online crime in a sustainable manner (Maras, , M. H. 2016; Moore, R. 2012).

Although the issue of online fraud is commonly observed in Thai society through various media, there are also private sector measures in place aimed at preventing individuals from becoming victims of such crimes. These measures include posting warnings on personal online media, forming groups on Facebook to share information about criminal scams, or creating websites to verify personal information of offenders, such as their names and bank account numbers (e.g., https://www.blacklistseller.com). While these initiatives leverage the online world to enhance self-protection against online crime, they do not necessarily guarantee that the collected information is complete or free from malice. Therefore, some actions to combat online fraud may still require accurate information and support from government authorities (Cyber Crime Investigation Bureau, 2023).

In the past, while law enforcement officials have consistently pursued cases against criminals involved in online fraud alongside other criminal cases in society, specialized units have been established to specifically address issues related to technology crimes. The Cyber Crime Investigation Center has implemented online reporting channels to facilitate consumers. Furthermore, the Technology Crime Suppression Division is authorized to temporarily halt account transactions when consumers realize they have been scammed or defrauded online. Victims are encouraged to promptly report the incidents to the Cyber Crime Investigation Center, as stated in the National Police Agency Order No. 77/2565 concerning the reporting and management of technology-related crime cases through electronic systems. This order empowers the Technology Crime Suppression Division to temporarily freeze transactions to accounts where victims have transferred money. Therefore, if victims report to the Cyber Crime Investigation Center within approximately three hours of being deceived, there is a relatively high chance of recovering their funds.

However, the issue of online fraud continues unabated, with no signs of decline. Hence, a purely reactive approach is insufficient. In addition to addressing incidents after they occur, there must be additional mechanisms to enhance law enforcement efforts in tackling online fraud proactively. This includes promoting public awareness of the various forms of online scams. Consequently, raising awareness about these threats within Thai society is essential to reduce the incidence of victimization in online fraud cases (Bank of Thailand, 2024).

In terms of crime prevention, inadequate governmental measures that lag in keeping pace with technological advancements, coupled with existing legal constraints, may reflect inadequacies in deterring online fraud. The investigation issues further highlight the challenges faced by law enforcement in effectively addressing these crimes. The Deterrence Theory suggests that effective crime prevention strategies are vital; without swift enforcement of appropriate penalties, criminal activities may persist and increase. Thus, there is an urgent need for ongoing research to ascertain which criminological theories accurately elucidate the dynamics of online fraud and investigate how these issues impact enforcement, aiding in the prediction of crime trends and the formulation of effective reduction strategies.

This research study aims to understand the issues surrounding online fraud within Thai society and the obstacles faced in the enforcement of laws, based on the current realities. The intention is to gather in-depth information that will lead to the development of suitable practices for legal enforcement and the creation of educational materials for the public to prevent such problems. This will enhance the effectiveness and efficiency of enforcing laws related to online fraud and promote public awareness of these threats, enabling individuals to safeguard themselves sustainably against becoming victims of online fraud.

Literature review

Concepts and Theories

Anonymity Theory

Anonymity Theory helps explain online fraud by highlighting how the lack of identifiable information impairs self-awareness and rational decision-making, leading to impulsive and often aggressive behaviors. This lack of identity diminishes personal accountability and can result in behavioral changes, commonly seen in deindividuation scenarios like being in a crowd or wearing a disguise (Rayanin, R. 2024). Burkell, J. (2006) categorizes anonymity into three types: Identity Protection (non-disclosure of one's name), Visual Anonymity (not being seen), and Action Anonymity (actions can't be traced back to the individual). Studies, such as one by Omernick E., & Sood, S. O. (2013), show that anonymous users tend to engage more online, though identified users offer comments with more relevance and fewer profanities. Misoch, S. (2015) describes anonymity simply as "namelessness" and explains that it reduces perceived responsibility for actions, intersecting with privacy issues. While laws may require identity disclosure in some cases, anonymity complicates accountability in digital spaces. In the physical realm, identification methods like Social Security Numbers, driver's licenses, and passports are commonly used to establish identity, ensuring a balance between anonymity and necessary accountability.

Protection Motivation Theory

Protection Motivation Theory (PMT) serves as a vital framework for preventing online fraud by elucidating the factors that induce fear in individuals. It identifies three key variables: Perceived Severity of the threat, Perceived Vulnerability, and Response Efficacy, later incorporating Self-Efficacy. The interaction of threat appraisal (assessing the threat) and coping appraisal (evaluating the ability to manage it) fosters changes in intention and behavior (Anderson C. L., & Agarwal, R. 2010; Johnston A. C., & Warkentin, M., 2010). These appraisals are crucial in predicting safety behaviors and adopting technology for protection, significantly affecting security behaviors in both workplaces and homes (Chenoweth,et.al., 2009).

A distinguishing feature of PMT is its emphasis on self-control, providing alternatives when traditional methods to counter undesired behaviors are insufficient. Individuals must foster self-belief to engage in preventive actions. While self-efficacy is theoretically distinct from barriers, those with high self-efficacy are better equipped to navigate challenges, as opposed to individuals with low self-efficacy who may find barriers overwhelming. Ultimately, the interplay between response efficacy and self-efficacy enhances the likelihood of appropriate responses while mitigating perceived response costs, such as discomfort and inconvenience, leading to more effective coping strategies (Johnston A. C., & Warkentin, M. 2010).

Law Enforcement Theory

Law Enforcement Theory emphasizes the strategic deployment of uniformed police officers within communities to effectively reduce crime. It suggests that while the primary responsibility for controlling, preventing, and suppressing crime rests with law enforcement, individuals and agencies outside the police serve supportive roles by providing information and assistance (Suradainai, U. 2018; Thasanchaigul,N. 2005; Athikomnantha, P. 1982).

Additionally, this theory highlights the lawful exercise of police authority. Law enforcement actions must adhere to legal frameworks, and officers are empowered to act against crimes under these laws (Athikhomnantha, P. 1982; Boonyopas, V. & Phanwicit, S. 2014). It aligns with Deterrence Theory, asserting that effective law enforcement can create fear of punishment, thereby reducing criminal behavior (Khanti, P. 2010; Sutheesorn, S.2011).

Victimology

Theories of Victimization is a prominent framework used to explain crime prevention strategies. Within this group of theories, the victimization process is described through three key theories:

1) Routine Activities Theory posits that crime statistics are a product of opportunities for crime, where crime occurs due to three elements: a target, an opportunity, and a motive. Regularly occurring daily activities make it easier for criminals to observe and plan their offenses, identifying certain individuals who may be more susceptible to becoming victims.

2) Theory of Imitation explains that criminal behavior stems from imitation, particularly among individuals who are closely related; they tend to mimic each other's actions and often look up to those in higher social status.

3) Types of Victims: Criminologists have classified various victim types by utilizing knowledge from psychology, sociology, and biology to explore the relationship between crime and victims. They note that victims can emerge from diverse groups, including minors (The young), women (The Female), the mentally defective and other mentally deranged persons, or acquisitive individuals (The Acquisitive person). These groups may exhibit vulnerability or differing experiences as victims (Khanti, P. 2010; Sutheesorn, S.2011).

Cyber Criminology

Online fraud targeting the elderly has become a significant concern, as evidenced by a study conducted by Nildum, K. (2020) in Chiang Rai province. The research revealed that many elderly individuals fell victim to pyramid schemes, followed by ATM transaction scams, while religious-based frauds were the least common. After being defrauded, most elderly victims tended to post their experiences on social media rather than report the incidents to the police, with very few attempting to recover their losses on their own. This highlights a concerning pattern of consumer deception, where elderly individuals are particularly susceptible to fraudulent schemes due to their lack of awareness and the allure of easy returns.

Further studies, such as those by Thongrawiwong, K. (2021), focus on online romance scams that exploit emotional trust, leading to financial deception. Additionally, Kanthawong, W. (2020) examined foreign exchange speculation scams, often termed Forex scams, which are prevalent on social media platforms promising quick riches. The rapid exchange of information facilitated by modern technology has made these scams more accessible, resulting in victims often refraining from reporting their losses due to perceived leniency in law enforcement.

To effectively combat these evolving online crimes, which now integrate advanced technology into their mechanisms, a robust legal response is necessary. The criminological theory of deterrence emphasizes that effective crime prevention requires swift and stringent punitive measures to deter offenders (Sutthiyothin, N. 2011). Ultimately, the transition to

cybercrime, involving scams and deceptions through the internet, underscores the need for continued research and comprehensive strategies to protect vulnerable populations (Sawitree, S. 2017).

Research Methodology

The research on Developing Guidelines for the Prevention and Suppression of Online Fraud Crimes: Guidelines for Law Enforcement by Police Officials in the Investigation employed a comprehensive methodology structured into five key steps. Initially, the study aimed to analyze and synthesize relevant knowledge concerning the problems and patterns of online fraud, factors contributing to victimization, and the challenges faced by law enforcement agencies.

This was achieved through document research, in-depth interviews with both victims and law enforcement personnel, and focus group discussions to gather diverse perspectives. In the second phase, the research shifted focus to the design and development of practical implementation strategies and educational media aimed at raising public awareness and supporting law enforcement efforts. Workshops were conducted with experts and stakeholders to draft suitable practices conducive to combating online fraud effectively. The third step involved evaluating these practices and educational materials through practical trials, gathering feedback from target populations, including police officers and the general public, on usability and effectiveness. The fourth phase centered on refining the proposed guidelines and learning media based on insights gained from trials, ensuring that the final products met the needs of both law enforcement officials and the public.

Finally, the dissemination step aimed to promote the developed guidelines through seminars and dialogues, engaging various stakeholders, including police, policymakers, and community representatives. The iterative nature of this research methodology highlighted the importance of collaboration and community involvement in addressing the complexities of online fraud, ultimately striving for a cohesive and informed approach to prevention and enforcement in this evolving area of crime. By fostering a collaborative environment and leveraging qualitative insights, the research aims to contribute significantly to strengthening the response to online fraud within society.

Research Results

1. Limited Personnel and Expertise

Limited personnel and expertise within law enforcement agencies significantly hinder the ability to effectively investigate and combat fraud. As fraud schemes grow in complexity and sophistication-often leveraging advanced technology and multifaceted tactics-agencies must be equipped with a sufficiently trained workforce capable of addressing these challenges. Unfortunately, many law enforcement units face resource constraints that limit their capacity to recruit, retain, and train personnel specialized in fraud investigations.

The lack of dedicated fraud investigators can result in overwhelming caseloads for existing staff, making it difficult to thoroughly examine each case. Officers trained primarily in traditional criminal investigations may not possess the specific skills required to unravel financial crimes, which often involve intricate financial systems, digital platforms, and a deep understanding of regulations. This gap in expertise can lead to inefficient investigations, missed opportunities for early intervention, and ultimately, a reduced likelihood of prosecution for fraudsters.

Moreover, as fraud continues to evolve, so too must the skill sets of law enforcement personnel. Continuous training in emerging fraud trends, cybercrime techniques, and regulatory compliance is essential to keep investigators informed and effective. Enhancing partnerships with academic institutions, industry experts, and technology firms can provide law enforcement agencies with access to valuable resources and training opportunities.

In conclusion, addressing the challenges posed by limited personnel and expertise is crucial for bolstering fraud investigations. By investing in specialized training, recruiting skilled personnel, and fostering collaborative relationships, law enforcement agencies can enhance their capabilities, protect victims, and uphold the integrity of financial systems in an increasingly digital world.

2. Insufficient Tools and Systems for Investigation

Insufficient tools and systems for investigating fraud can severely impede the effectiveness of law enforcement and regulatory agencies tasked with combating these complex crimes. In an era where fraudulent activities have become increasingly sophisticated, the need for advanced technological solutions and streamlined processes is more critical than ever. Traditional investigative methods may fall short in the face of rapidly evolving fraud tactics that leverage digital platforms, making it essential for agencies to adopt more effective tools.

The absence of integrated data analytics systems hampers investigators' ability to uncover patterns in fraudulent activities. Analysts require access to comprehensive databases that consolidate information from multiple sources, including financial institutions, law enforcement databases, and digital service providers. Without these resources, investigators may struggle to identify links between cases or detect trends that signal larger fraud operations.

Moreover, inadequate training on existing tools can further hinder investigations. Even when agencies have access to modern technology, officers may lack the skills necessary to utilize these tools effectively, leading to missed opportunities for early detection and intervention. As fraudsters increasingly exploit sophisticated techniques, it is imperative that agencies invest in both state-of-the-art tools and ongoing professional development.

In conclusion, addressing the shortcomings of investigative tools and systems is vital to improving the fight against fraud. By investing in advanced technologies, enhancing data-sharing capabilities, and ensuring adequate training for personnel, agencies can empower investigators to more effectively identify, investigate, and prosecute fraudulent activities, ultimately protecting consumers and maintaining trust in financial systems.

3. Delays in Coordination with Banks and Digital Service Providers

Delays in coordination with banks and digital service providers can significantly hinder investigations into fraudulent activities, posing substantial risks to both financial institutions and their customers. These delays often arise from inefficiencies in communication, as well as complications related to integrating various technological systems and complying with legal regulations.

When fraud is suspected, timely and coordinated action between banks and digital service providers is essential. However, ambiguities in communication can lead to misunderstandings about the necessary steps to take, resulting in slower responses to potential threats. Moreover, the intricate nature of financial fraud cases often requires collaborative efforts across multiple platforms, and delays in this coordination can allow fraudsters to exploit vulnerabilities for longer periods.

Regulatory compliance further complicates matters. Both banks and digital service providers are required to adhere to strict guidelines concerning data security and reporting.

While these regulations are designed to protect consumers, they can also slow down the process of investigating suspicious activities. A lack of immediate access to essential data can prevent swift action, allowing fraudulent transactions to slip through the cracks.

Additionally, prolonged delays can erode customer trust. If clients perceive that their financial institutions or service providers are not acting promptly to investigate fraudulent activities, they may lose confidence in their security measures. To combat these issues, fostering clear communication and collaboration between all stakeholders is imperative. Investing in advanced technology solutions that facilitate real-time data sharing and streamlining investigative workflows can help ensure a more effective response to fraud.

4. Legal limitations and Inconsistencies in the Justice Process

Legal limitations and inconsistencies in the justice process can significantly impede effective investigations into fraudulent activities, ultimately affecting the ability to hold perpetrators accountable. These limitations often stem from varying laws and regulations across jurisdictions, which can create challenges in gathering evidence and prosecuting cases. When fraud occurs, the legal framework surrounding the investigation may limit the actions that law enforcement agencies and financial institutions can take, resulting in delayed responses and inadequate measures to prevent further illicit activities.

Inconsistencies in the justice process further complicate matters. Different courts may apply laws differently, leading to disparities in how fraud cases are treated and prosecuted. This can lead to situations where similar fraudulent activities receive varying levels of scrutiny and consequences, undermining the overall deterrence effect of the law. Additionally, gaps in legal definitions surrounding fraud can hinder efforts to categorize and prosecute emerging forms of fraud, especially in the fast-evolving digital landscape.

Moreover, victims of fraud often face significant hurdles in seeking justice. Lengthy legal procedures and complex bureaucratic processes can discourage victims from reporting incidents or pursuing claims, resulting in a lack of data for law enforcement agencies to understand the full scope of the problem. To improve the situation, fostering collaboration between legal authorities, financial institutions, and technology providers is essential. Streamlining legal processes and enhancing communication can create a more cohesive response to fraud, ensuring that justice is served more effectively and efficiently.

5. Excessive Workload on Officers

Excessive workload on law enforcement officers can significantly hinder the effectiveness of investigations into fraud, leading to substantial gaps in the detection and prosecution of fraudulent activities. When officers are overwhelmed with a high volume of cases, their ability to thoroughly investigate each incident diminishes, resulting in potential fraudsters slipping through the cracks. The complexity of fraud cases adds another layer of difficulty; these investigations often require extensive analysis, coordination with financial institutions, and a deep understanding of both criminal behavior and relevant laws.

As officers juggle numerous demands, prioritization of cases becomes a necessity. Unfortunately, this often leads to fraud cases being deprioritized due to perceived lower immediacy compared to violent crimes or urgent public safety issues. Consequently, victims of fraud may feel that their concerns are not taken seriously, which can erode public trust in law enforcement agencies. Additionally, the lack of adequate resources, including staffing and technological support, exacerbates the problem, as officers find themselves ill-equipped to handle the intricacies of fraud investigations.

Addressing this issue requires a multifaceted approach. Law enforcement agencies need to advocate for increased funding to allow for specialized fraud investigation units and

enhance training for officers. Additionally, adopting advanced technologies that automate data analysis and streamline reporting can alleviate some of the burdens on officers. By creating a more manageable workload, agencies can empower officers to focus more effectively on fraud investigations, ultimately improving outcomes for victims and society at large.

6. Lack of Integrated Coordination among Agencies

The lack of integrated coordination among various agencies poses significant challenges in effectively investigating and combatting fraud. With multiple entities involved-such as law enforcement, financial institutions, regulatory bodies, and digital service providers-fragmented communication can lead to inefficiencies that hinder timely action against fraudulent activities. Each agency may operate under different protocols and priorities, resulting in a disjointed approach that allows fraudsters to exploit vulnerabilities.

When agencies fail to share crucial information and resources, investigations can become prolonged and ineffective. For instance, if a financial institution uncovers suspicious transactions but does not efficiently relay this data to law enforcement, the opportunity to halt a fraudulent scheme may be lost. Additionally, different jurisdictions may lack consistent policies or legal frameworks regarding fraud, further complicating collaborative efforts to take swift action against perpetrators.

The absence of a unified strategy can also lead to inconsistent enforcement of laws, creating an environment where fraud may thrive. Victims of fraud often feel frustrated and powerless when they perceive that agencies are not working together to address their concerns, which can erode trust in the justice system. To combat these challenges, fostering a culture of collaboration is imperative. Establishing interagency task forces focused on fraud prevention can facilitate improved communication and resource sharing. Leveraging technology to create centralized databases for fraud-related data can enhance investigative efficiency and strengthen the overall response to fraudulent activities, ensuring a more coordinated effort to protect consumers and uphold the integrity of the financial system.

7. Establish Specialized Task Forces with a Focus on Online Fraud

Establishing specialized task forces dedicated to investigating online fraud is essential in today's digital landscape, where fraudulent activities are increasingly sophisticated and pervasive. With the rapid growth of e-commerce, social media platforms, and digital transactions, fraudsters have more opportunities than ever to exploit vulnerabilities, making it imperative for law enforcement and regulatory agencies to adopt targeted approaches to combat this evolving threat.

These specialized task forces can bring together experts from various fields, including law enforcement personnel, cybercrime specialists, financial analysts, and technology professionals. By collaborating in this way, these teams can leverage diverse skill sets and knowledge bases to enhance the effectiveness of their investigations. Task forces can develop standardized protocols for reporting, investigating, and prosecuting online fraud cases, ensuring a consistent and efficient response across jurisdictions.

In addition, these dedicated units can focus on training law enforcement agencies in the latest fraud detection techniques, including the use of technology such as AI and data analytics to identify patterns and anomalies indicative of fraudulent activities. By investing in ongoing education and resources, task forces can stay ahead of emerging trends in online fraud, enabling proactive rather than reactive strategies.

Moreover, fostering collaboration with digital service providers and financial institutions is crucial. By sharing information and best practices, task forces can create a robust network that empowers all stakeholders to combat online fraud more effectively. Ultimately, the establishment of specialized task forces focused on online fraud will enhance

investigative capabilities, build public trust, and contribute to a safer digital environment for consumers and businesses alike.

Figure 1: Statistics on Online Fraud Case Reports from the Royal Thai Police
Source: Cyber Crime Investigation Bureau (2024). Online

8. Streamline processes for rapidly freezing bank accounts related to fraud

Streamlining the processes for rapidly freezing bank accounts implicated in fraud is crucial for mitigating financial losses and safeguarding victims. In instances of suspected fraud, time is of the essence; immediate action can significantly reduce the potential damage caused by fraudulent transactions. However, many financial institutions face bureaucratic hurdles and lengthy procedures that delay the freezing of accounts, allowing fraudsters to drain resources before corrective actions can be implemented.

By developing efficient protocols that facilitate rapid response, banks and law enforcement agencies can work collaboratively to enhance their fraud prevention efforts. This may include establishing clear guidelines for when to freeze accounts, training staff on how to identify potential fraud indicators efficiently, and utilizing technology to expedite the process. Implementation of automated systems and real-time communication channels can enable swift information sharing between banks and law enforcement, ensuring that urgent requests to freeze accounts are handled promptly.

Additionally, creating a centralized reporting mechanism can help streamline the process. When financial institutions have access to a unified platform where fraud cases can be reported and addressed collaboratively, banks can act faster to protect affected accounts. Regular drills and training sessions should also be conducted to ensure all personnel are familiar with the procedures and responsive to emerging situations.

Ultimately, by expediting the freezing of fraudulent accounts, financial institutions can minimize the impact on victims and enhance overall trust in the banking system. A proactive and coordinated approach is essential in tackling the ever-evolving landscape of fraud in today's digital economy.

9. Encourage collaborative investigations across jurisdictions and sectors

Encouraging collaborative investigations across jurisdictions and sectors is vital for effectively tackling fraud in today's interconnected world. Fraudulent activities often transcend geographical boundaries and involve multiple parties, making isolated efforts insufficient. By fostering collaboration among various law enforcement agencies, regulatory bodies, and financial institutions, investigators can pool resources, share intelligence, and coordinate actions that enhance the robustness of fraud investigations.

Collaborative investigations enable agencies to address the complexities of modern fraud schemes that utilize sophisticated tactics and technology. For instance, when fraud involves international networks or online scams that manipulate financial systems across borders, a unified response becomes essential. Joint task forces can facilitate streamlined communication, allowing for rapid data sharing and more comprehensive investigative techniques that leverage the unique strengths and expertise of each participant.

Furthermore, establishing partnerships between public and private sectors can amplify the effectiveness of fraud prevention efforts. Financial institutions, technology companies, and government agencies can work together to develop shared platforms for reporting and analyzing fraudulent activities. This not only enhances situational awareness but also fosters a culture of vigilance and accountability.

Additionally, training programs and knowledge-sharing initiatives can empower investigators with the tools and insights necessary to recognize emerging fraud trends and appropriate responses. By cultivating a collaborative environment, stakeholders can act swiftly to detect, investigate, and mitigate the impact of fraud, ultimately contributing to a more secure financial ecosystem for consumers and businesses alike. Effective collaboration not only enhances investigative outcomes but also builds public trust in the systems designed to protect them from fraud.

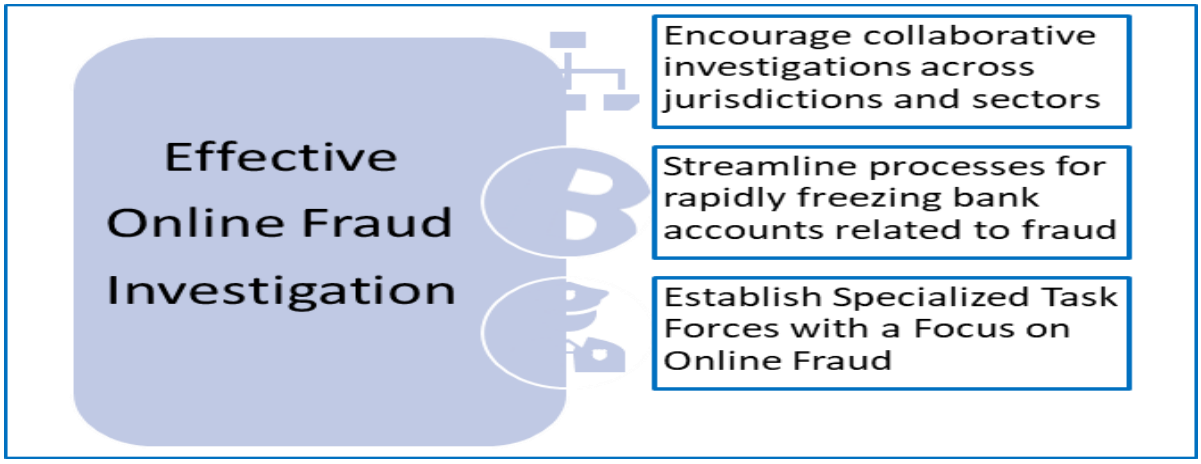

Figure 2: Effective online fraud investigation

Research Discussion

The ongoing evolution of communication technology and the internet has dramatically increased accessibility to online platforms, leading to both conveniences and heightened risks of online fraud. The research indicates that individuals often fall victim due to a lack of awareness about the deceptive tactics employed by criminals, including social engineering and sophisticated scams. Notably, the Thai Criminal Code's expansive definition of fraud encompasses a range of digital offenses, including social media scams and investment fraud schemes. The implications of falling victim to online fraud extend beyond financial losses,

undermining public trust in law enforcement's ability to prevent such crimes and exacerbating feelings of insecurity regarding online safety.

Key findings revealed several operational challenges faced by law enforcement in combating online fraud, including limited personnel with specialized expertise, insufficient technological tools, and delays in coordination with financial institutions. These factors hinder effective investigations and leave victims feeling neglected. Moreover, legal inconsistencies and excessive workloads contribute to prolonged investigative processes, further diminishing the capacity of agencies to respond to fraud promptly.

The establishment of specialized task forces dedicated to online fraud is crucial, as is the streamlining of processes for quickly freezing bank accounts implicated in fraudulent activities. By fostering collaboration across jurisdictions and sectors, law enforcement agencies can enhance their investigative capabilities and develop a more integrated approach to tackling online fraud. Implementing comprehensive training and resources to keep pace with the evolving landscape of fraud is vital for ensuring that law enforcement can effectively mitigate victimization and uphold public trust in digital commerce.

The findings underscore the necessity for ongoing research and the adaptation of criminological theories to inform strategies that address the complexities of online fraud, ultimately contributing to the development of effective prevention and response measures.

Recommendations

Recommendations in Terms of Policy

1. Establish Comprehensive Cybersecurity Framework: Develop a national cybersecurity strategy that includes defined roles and responsibilities for law enforcement, financial institutions, and digital service providers. This policy framework should emphasize collaboration and information sharing among all stakeholders to enhance the country’s ability to prevent and respond to online fraud.

2. Create Specialized Cybercrime Units: Establish specialized task forces within law enforcement agencies focused exclusively on investigating online fraud and cybercrime. These units should comprise trained personnel with expertise in digital forensics, cyber law, and financial crime to improve investigative capabilities.

3. Enhance Training Programs for Law Enforcement: Implement continuous training and professional development programs for law enforcement officers on emerging fraud trends, digital investigations, and the use of advanced technologies for fraud detection. Partnerships with academic institutions and private sectors, including tech companies, can provide valuable resources and training opportunities.

4. Streamline Reporting and Response Mechanisms: Develop clear protocols for rapidly freezing bank accounts implicated in fraudulent activities. Establish a centralized reporting system that allows victims to report incidents easily while facilitating timely communication between financial institutions and law enforcement.

5. Improve Legal Frameworks: Review and amend existing laws to address gaps in the legal definitions and prosecution of online fraud, ensuring that legislation remains relevant in the face of evolving technology and complex fraud schemes. Legal reforms should also streamline the reporting process for victims and enhance protections for those who come forward.

6. Promote Public Awareness Campaigns: Launch nationwide awareness programs aimed at educating the public about online fraud prevention. These initiatives should focus on informing citizens about common scams, safe online behaviors, and the importance of verifying the credibility of online transactions.

7. Foster Collaboration with Private Sector: Encourage public-private partnerships to develop innovative solutions for combating online fraud, including technology-driven tools for fraud detection and prevention. Financial institutions and tech companies should work together to enhance security measures and share data on fraudulent activities.

8. Conduct Regular Assessments of Fraud Trends: Establish mechanisms for the ongoing collection and analysis of data on online fraud incidents. This information should guide policy adjustments and inform the development of targeted prevention strategies based on current trends and emerging threats.

9. Encourage Citizen Participation in Reporting: Implement incentives for citizens to report online fraud cases, such as anonymous reporting options or recognition programs for those who contribute to successful investigations. This can empower individuals and foster a proactive community approach to fraud prevention.

10. Support Victim Recovery Initiatives: Develop programs that assist victims of online fraud in recovering lost funds and provide psychological support services to help mitigate the emotional impact of fraud. Government initiatives should aim to restore trust in financial systems and encourage reporting of fraud cases.

Recommendations in Terms of Practical

1. Develop Specialized Cybercrime Units: Establish dedicated units within the Royal Thai Police focused on cybercrime, particularly online fraud. These units should include personnel with expertise in digital forensics, cybersecurity, and financial investigations to address the complexities of online offenses effectively.

2. Enhance Training and Capacity Building: Implement a comprehensive training program for police personnel that focuses on the latest technologies, investigative techniques, and emerging trends in online fraud. Regular workshops and courses should be conducted in collaboration with technology experts and cybersecurity firms.

3. Improve Interagency Coordination: Establish protocols for seamless collaboration between the Royal Thai Police and other agencies, including financial institutions and regulatory bodies. Regular joint exercises and meetings can enhance intelligence sharing and facilitate quicker responses to fraudulent activities.

4. Adopt Advanced Investigative Tools: Invest in state-of-the-art investigative tools and technologies that enable real-time tracking of online fraud activities. This should include data analytics software, digital forensics tools, and platforms for monitoring online transactions and activities associated with fraud.

5. Enhance Public Reporting Mechanisms: Create user-friendly online portals and hotlines for victims to report incidents of online fraud easily. Ensure that the reporting process is efficient, responsive, and allows for anonymous submissions to encourage more victims to come forward.

6. Establish Rapid Response Teams: Develop rapid response teams within the cybercrime units that can act quickly to freeze suspected fraudulent accounts and secure evidence before it is lost. This could involve establishing immediate communication channels with financial institutions to halt fraudulent transactions swiftly.

7. Conduct Public Awareness Campaigns: Actively participate in public awareness initiatives aimed at educating citizens about the risks of online fraud and promoting safe online practices. Collaborate with community organizations to disseminate information on recognizing scams and reporting fraud.

8. Enhance Legal Coordination: Work closely with legal authorities to ensure that police have a clear understanding of the legal frameworks surrounding online fraud. This

includes staying updated on changes in laws and regulations that may affect investigations and prosecutions.

9. Utilize Data-Driven Approaches: Implement a data-driven strategy for addressing online fraud by collecting and analyzing data on trends, types of fraud, and victim demographics. This information can help tailor policing strategies and allocate resources more effectively.

10. Implement Collaborative Investigations: Foster partnerships with both local and international law enforcement agencies to conduct joint investigations into large-scale online fraud operations that cross borders. This can enhance resource sharing and cooperative planning for tackling sophisticated fraud networks.

11.Evaluate and Adapt Strategies Regularly: Establish a system of regular review and evaluation of anti-fraud strategies and initiatives. Collect feedback from officers and the community to assess the effectiveness of current approaches and make necessary adjustments.

References

Abas, S. N.,et.al.. (2017). Social engineering. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2*(6), 1109–1114. https://www.ijsrcseit.com

Anderson, (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613–643. https://doi.org/10.2307/25750669

Atul, B., Lhato, J., & Alka, R. (2018). Information security: Exploring the association between IT receptivity and cyber crime victimization. *FIIB Business Review, 4*(1), 1-12. https://doi.org/10.1177/2455265820150109

Athikhomnantha, P. (1982). *Sociology of crime and punishment.* Bangkok: Ramkhamhaeng University.

Bandler, J., & Merzon, A. (2020). *Cybercrime investigations: A comprehensive resource for everyone* [PDF]. Taylor & Francis Group. https://www.taylorandfrancisgroup.com

Bank of Thailand. (2024). Types of fraud. Online. https://www.westernunion.com/th/th/fraudawareness/fraud-types.html

Buil-Gil, D., & Zeng, Y. (2021). Meeting you was a fake: Investigating the increase in romance fraud during COVID-19. *Journal of Financial Crime.* https://doi.org/10.1108/JFC-02-2021-0042

Burkell, J. (2006). *Anonymity in behavioural research: Not being unnamed, but being unknown.* Faculty of Information and Media Studies, The University of Western Ontario.

Boonyopas, V. & Phanwicit, S. (2014). Economic crime. Bangkok: Nititham.

Chad, W., & Diarmaid, H. (2019). Civilianising specialist units: Reflections on the policing of cyber-crime. *Criminology & Criminal Justice, 22*(4), 354-370. https://doi.org/10.1177/1748895819874866

Chenoweth, et.al. (2009). Application of protection motivation theory to the adoption of protective technologies. In *Proceedings of the Hawaii International Conference on System Sciences* (1–10).

Cyber Crime Investigation Bureau. (2021). *Cyber Crime Investigation Bureau.* https://www.thaipoliceonline.com/

Cyber Crime Investigation Bureau. (2023). *Cyber Crime Investigation Bureau.* https://www.thaipoliceonline.com/

Danquah, (2011). An empirical test of the space transition theory of cyber criminality: Investigating cyber crime causation factors in Ghana. *African Journal of Computing & ICT, 2*(1), 37–48.

Diarmaid, H., & Chad, W. (2021). Perceptions of police training needs in cyber-crime. *International Journal of Police Science & Management, 24*(1), 27–36. https://doi.org/10.1177/146135572110365

Drew, J. M. (2020). A study of cybercrime victimization and prevention: Exploring the use of online crime prevention behaviors and strategies. *Journal of Criminological Research, Policy and Practice.* https://doi.org/10.1108/JCRPP-12-2019-0070

Emami, C., et.al.(2020). Predicting online fraud victimization in Australia. *Trends & Issues in Crime & Criminal Justice, 603,* 1–9.

Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology, 1*(1), 1–6.

Jaishankar, K. (2008). Space transition theory of cyber crimes. In F. Schmallager & M. Pittaro (Eds.), *Crimes of the internet* (283–301). Prentice Hall.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549–566. https://doi.org/10.2307/25750712

Junger, M.,et.al.. (2020). Fraud against businesses both online and offline: Crime scripts, business characteristics, efforts, and benefits. *Crime Science, 9*(1), 1–15. https://doi.org/10.1186/s40163-020-00130-2

Kai, Let.al. (2023). Telecommunication and cyber fraud victimization among Chinese college students: An application of routine activity theory. *Criminology & Criminal Justice.* OnlineFirst. https://doi.org/10.1177/17488958221146144

Kanthawong, W. (2020). Economic crime: Currency exchange rate speculation fraud. *Journal of Social Sciences, Srinakharinwirot University, 23*(1). http://ejournals.swu.ac.th/index.php/JOS/article/view/12906/10586

Khanti, P. (2010). *Criminology theory: Principles of applied research and policy.* Bangkok: Sunet Film.

Khruakham, S. (2015). *Criminology, criminal justice, and the justice system*. Nakhon Pathom: Phetkasem Printing.

Kshetri, N. (2013). *Cybercrime and cybersecurity in the global south.* Palgrave MacMillan Publishers.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems, 11*(7), 1–16. https://doi.org/10.17705/1jais.00231

Maras, M. H. (2016). *Cybercriminology.* Oxford University Press.

Michail, G. (2014). Video-based learning and open online courses. *International Journal of Emerging Technologies in Learning (iJET), 9*(1), 4–7. https://doi.org/10.3991/ijet.v9i1.3296

Misoch, S. (2015). Stranger on the internet: Online self-disclosure and the role of visual anonymity. *Computers in Human Behavior, 50,* 60–65. https://doi.org/10.1016/j.chb.2015.02.027

Moore, R. (2012). *Cyber crime: Investigating high-technology computer crime.* Routledge.

Nildum, K. (2020). Methods of deception, communication channels, and experiences of being deceived by online scammers among the elderly in Chiang Rai Province. *Journal of Communication, Chiang Rai Rajabhat University.* https://so01.tci-thaijo.org/index.php/CRRUJC/article/view/241670

Omernick, E., & Sood, S. O. (2013). The impact of anonymity in online communities. In *Proceedings of the 2013 International Conference on Social Computing, Behavioral-Cultural Modeling, and Prediction* (526–535).

Rayanin, R. (2024). Anonymity. Faculty of Psychology, Chulalongkorn University. Online. https://www.psy.chula.ac.th/th/feature-articles/anonymity

Suksri, S. (2020). *Cybercrime and computer crime law* (2nd ed.). Bangkok: Thammasat University, Project for Textbooks and Teaching Materials, Faculty of Law.

Suradainai, U. (2018). Victimization in educational institutions: A case study of Chulalongkorn University (Master's thesis, Chulalongkorn University). Bangkok.

Sutheesorn, S. (2011). *Criminology.* Bangkok: Thammasat University Press.

Sutthiyothin, N. (2011). *Criminology theory.* Faculty of Law, Sukhothai Thammathirat Open University.

Tarling, R., & Morris, K. (2010). Reporting crime to the police. *British Journal of Criminology, 50*(3), 474–490. https://doi.org/10.1093/bjc/azq014

Thasanchaigul, N. (2005). *Crime (Prevention: Control).* Nonthaburi: Pornthip Printing.

Thongraviwong, K. (2021). Applying the Computer Crimes Act B.E. 2550 (2007) amended B.E. 2560 (2017) to romance fraud conducted through computer systems. *Ratchathani Journal, 15*(39). https://so05.tci-thaijo.org/index.php/RJPJ/article/view/249221