Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Cybercrime Prevention and Suppression Measures: Seizure and Suspension of Suspected Bank Account

Takrit Kaewtubtim [1], Punchada Sirivunnabood [2]

[1] Ph.D. candidate, Faculty of Social Sciences and Humanities Mahidol University, Thailand

[2] Assistant Professor, Faculty of Social Sciences and Humanities Mahidol University, Thailand

* **Corresponding Author:** takritk@gmail.com

ARTICLE INFO

Received: 18 Dec 2024

Revised: 15 Feb 2025

Accepted: 24 Feb 2025

ABSTRACT

This study is a qualitative research project that aims to review the laws and relevant measures concerning the prevention and suppression of cybercrime, including the assessment of operational procedures of involved agencies to identify existing problems and obstacles. The goal is to propose practical guidelines and preventive measures for tackling cybercrime, focusing particularly on the seizure and suspension of suspected bank accounts. The findings reveal that the Royal Decree on Measures for the Prevention and Suppression of Technological Crimes B.E. 2566 (2023) was enacted to address fraud involving technological means and the transfer of criminal assets. However, challenges remain, such as limited suspension periods, ambiguous legal conditions, delays in information exchange, and insufficient resources. This study proposes a four-step model for the suspension and seizure of suspected bank accounts in Thailand: (1) detection and alert of suspicious transactions, (2) verification and confirmation of information, (3) seizure and suspension of transactions, and (4) legal proceedings and account release. These steps are crucial for enhancing the sustainability of cybercrime prevention and suppression efforts in Thailand.

Keywords: Cybercrime prevention and suppression, seizure and suspension of suspected bank accounts, mule accounts

INTRODUCTION

The exponential growth in the use of digital technologies and the internet over recent decades has brought numerous advantages in communication, business operations, and information accessibility. However, this digital transformation has also introduced substantial challenges and threats, particularly in the form of cybercrime, which has evolved rapidly in both form and complexity. In the 21st century, cybercrime has become a major threat to national security, as criminals increasingly exploit the internet and digital technologies to target the information systems of private enterprises, governments, and international organizations (Nuredini, 2014), leading to significant financial losses and breaches of privacy (Kundi & Nawaz, 2014).In Thailand, the proliferation of cybercrime has led to the emergence of “mule accounts,” through which victims are deceived daily, resulting in widespread and high-value financial damage. This escalating threat has become an urgent issue for countries worldwide (The Thai Bankers' Association, 2023). In response, Thailand has undertaken efforts to combat cybercrime through the establishment of legal frameworks and coordinated action by relevant agencies.

In 2023, the Thai government enacted the Royal Decree on Measures for the Prevention and Suppression of Technological Crimes B.E. 2566 to protect citizens from fraud committed via telephone and computer systems, which are used as electronic tools or methods to perpetrate such crimes. Multiple agencies are involved in enforcing the provisions of this Royal Decree. Despite the existence of legal mechanisms to address mule accounts and online fraud, Thailand continues to face a knowledge gap and practical challenges that hinder the effectiveness of account seizure and suspension processes—particularly in investment fraud cases, such as hybrid scams, where perpetrators gain trust before persuading victims to invest. Statistics indicate that there have been 3,280 such cases with total damages exceeding 2.7 billion baht (Thairath Online, 2023), causing widespread public harm. These circumstances underscore the need for legal reform, technological advancement in monitoring systems, and the strengthening of inter-agency collaboration to improve the efficiency of suspected account seizure and suspension. Such measures are vital for minimizing public losses and preventing cybercrime.

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

OBJECTIVES

This study, therefore, aims to: (1) Review relevant laws and operational measures of agencies responsible for cybercrime prevention and suppression in cases involving the seizure and suspension of suspected bank accounts (2) Examine the operations of such agencies; (3) Identify legal enforcement and operational challenges; and(4) Propose preventive and suppressive measures specifically for suspected account seizure and suspension in cybercrime cases.

LITERATURE REVIEW

This study incorporates relevant concepts and theoretical frameworks to support its analysis. One of the primary frameworks is the theory of cybercrime, which Halder and Jaishankar (2011) define as criminal acts committed by individuals or groups against individuals, groups, or organizations, with the intent to cause harm. Such acts may include physical or psychological damage and are perpetrated through telecommunications networks. A “mule account” refers to a bank account or electronic account used, or likely to be used, for transactions associated with technological crimes.Additionally, the study draws upon theories in victimology, a discipline that examines the role of victims in the criminal process to better understand contributing factors and the impacts on those victimized (Mendelsohn, 1956, as cited in Elias, 1983). This framework helps explain why certain individuals are more prone to victimization than others. The self-protection theory is also relevant, emphasizing individual behaviors aimed at preventing victimization, alongside state, organizational, and societal efforts to develop secure systems. This approach supports the enhancement of financial security systems and the reduction of cybercrime (Travis Hirschi, 1969). Moreover, the social control theory, proposed by Hirschi (1969), posits that individuals are less likely to engage in criminal behavior when robust social control mechanisms—such as laws, enforcement agencies, and regulatory frameworks—are in place.From an organizational perspective, systems theory, as articulated by Ludwig von Bertalanffy (1968), serves as a conceptual model for improving institutional structures, promoting inter-agency cooperation, and integrating technology to counter cyber threats. According to this theory, a system cannot function effectively unless its components are appropriately interconnected. Another pertinent framework is Crime Prevention Through Environmental Design (CPTED), introduced by C. Ray Jeffery (1971), which emphasizes reducing crime opportunities through the strategic design of physical environments. Key principles include surveillance, access control, territorial reinforcement, maintenance, and defensible space design. This concept has been adapted for cybersecurity under the term CPTEP (Crime Prevention Through Environmental Planning for Cybersecurity), applying the same principles to IT infrastructure to enhance digital safety. Furthermore, the study draws from the work of Sorawit Boonmee (2023), who analyzed the mechanism of suspected account suspension within Thai society. The Royal Decree on Measures for the Prevention and Suppression of Technological Crimes B.E. 2566 established the Technology Crime Prevention and Suppression Committee, which sets out guidelines for cybercrime prevention and identifies agencies authorized to access and share relevant data. This framework has informed the development of the conceptual model used in this research on cybercrime prevention and suppression through the seizure and suspension of suspected bank accounts.

METHODS

This study employed a qualitative research methodology, involving 33 key informants divided into two groups:

Group 1: In-depth interview participants (15 individuals) aimed at studying the operations of relevant agencies and identifying problems and obstacles in the enforcement of laws concerning the seizure and suspension of suspected bank accounts. This group comprised:

(1) 7 representatives from financial institutions and payment service providers, including representatives from seven different banks and electronic payment system operators.

(2) 8 representatives from public sector agencies, selected from seven relevant government organizations.

Group 2: Focus group participants (18 individuals) participated in discussions to exchange views and define effective guidelines or measures for the seizure and suspension of suspected accounts. This group included:

(1) 7 executives from financial institutions and payment service providers, one from each of the seven selected institutions.

(2) 8 representatives from public sector agencies, selected from seven relevant organizations.

(3) 3 experts and academics, specializing in financial systems and payment operations, relevant legal aspects of

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

cybercrime prevention, and criminology.

The research was conducted in three phases:

Phases 1: Documentary Review, a comprehensive review of existing laws and measures related to cybercrime prevention and suppression, particularly those concerning the seizure and suspension of suspected bank accounts.

Phases 2: Field Study, investigation of agency operations and identification of issues and obstacles in the implementation of laws and measures through in-depth interviews and focus group discussions.

Phases 3: Policy Recommendation, development of proposed measures and guidelines based on an analysis of the identified problems, practical challenges, and agency operations, followed by expert consultation and feedback.

Data collected were analyzed using comparative analysis between informants, prioritizing and categorizing data based on various attributes. This information was then compared with relevant documents, theoretical frameworks, and literature, applying systematic analysis to establish relationships and linkages among the findings. The analysis followed a descriptive and content analysis approach, with the reliability of data validated through triangulation.

FINDINGS AND DISCUSSION

1. Review of Laws and Measures Related to Cybercrime Prevention and Suppression: Case of Seizure and Suspension of Suspected Bank Accounts

Thailand enacted the Royal Decree on Measures for the Prevention and Suppression of Technological Crimes B.E. 2566 (2023) as the principal legal framework concerning cybercrime prevention and suppression, particularly in cases involving the seizure and suspension of suspected bank accounts. The decree establishes clear guidelines for addressing technology-related fraud and the transfer of assets derived from criminal activity. Key provisions include the disclosure of information on suspicious accounts, the suspension of related transactions, and the reporting and prosecution of offenders, as well as the promotion of inter-agency cooperation (Narong Kulnitas, 2015).The primary objectives of the decree are as follows: (1) Immediate suspension or seizure of criminal accounts to support victims of online fraud;(2) Real-time tracking of resolution processes for affected victims;(3) Expedited return of funds to victims;(4) Enhanced efficiency in arresting, prosecuting, and expanding investigations—through the integration of digital technology for data coordination and prompt collaboration among all involved agencies upon notification from victims.This is consistent with the findings of Manatsanan Pinpitak (2023), who noted the promising implementation of the Royal Decree in addressing cybercrime challenges. A key feature of the decree is its provision empowering banks to immediately suspend suspicious transactions. In addition, several other relevant laws support this framework, including: The Anti-Money Laundering Act B.E. 2542 (1999), The Computer Crime Act B.E. 2560 (2017), and its amendment in B.E. 2564 (2021). The Royal Decree of 2023 thus serves as the core legal instrument that delegates authority to relevant agencies for account seizure and suspension. It clearly delineates the scope of authority for each agency and outlines a systematic procedural framework for enforcement.

2. Operations of Relevant Agencies in Cybercrime Prevention and Suppression: Case of Seizure and Suspension of Suspected Bank Accounts

The Royal Decree on Measures for the Prevention and Suppression of Technological Crimes B.E. 2566 serves as the central legal instrument, prescribing penalties for offenses involving mule accounts. It establishes a mechanism known as the "Committee on the Prevention and Suppression of Technological Crimes," chaired by the Minister of Digital Economy and Society, and composed of eight ex officio members. These include representatives from financial institutions and payment service providers who are authorized to exchange customer account and transaction information via a data-sharing system. Telecommunications providers are also authorized to exchange data. Additional members include the Royal Thai Police, the Anti-Money Laundering Office (AMLO), and agencies with access to shared data. The National Broadcasting and Telecommunications Commission (NBTC) is tasked with developing a centralized database containing essential user registration information for use in investigations and preventive measures. The decree operates as a control mechanism to reduce criminals' ability to directly reach victims, enhancing the role of the capable guardian through the account seizure and suspension process. Following its enactment, inter-agency cooperation has intensified, resulting in key developments such as:(1) The establishment of the Anti–Online Scam Operation Center (AOC). (2) The implementation of data exchange through the Central Fraud Registry (CFR) system.

However, the effective functioning of agencies involved in preventing and suppressing cybercrime—specifically in the seizure and suspension of suspected bank accounts—relies on multi-agency collaboration. Core roles are played by the Anti-Money Laundering Office (AMLO), the Bank of Thailand (BOT), and the Ministry of Digital Economy and

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Society (MDES) in monitoring, regulating, and preventing the use of mule accounts for cybercrime. Close cooperation between public and private sectors is critical in reducing cybercrime and enhancing the security of the national financial system. This approach is consistent with the Crime Triangle Theory, which posits that crimes occur when three elements converge: the offender, a suitable target, and the absence of a capable guardian. In cybercrime contexts, mule accounts are a vital conduit through which offenders operate. Victims are deceived into transferring funds into such accounts, which are then used to launder money through multiple transfers to obscure the criminal's trail.Arithat Kaewkorsana (2017) proposed a cybersecurity framework comprising: (1) Prevention (Identify & Protect),(2) Real-time Monitoring (Detect), and (3) Real-time Response (Respond).This model aligns with the NIST Cybersecurity Framework (National Institute of Standards and Technology, 2018) and the work of Jirapatch Phanthawornchai (2018), which outline a structure for cybersecurity composed of (1) Identify, (2) Protect, (3) Detect and (4) Respond.

3. Challenges and Obstacles in the Enforcement of Laws and Measures, Including the Operations of Agencies Involved in Cybercrime Prevention and Suppression: Case of Seizure and Suspension of Suspected Bank Accounts

Key challenges identified in the enforcement of relevant laws and the operations of responsible agencies include: The limited duration of account suspension, Ambiguity in legal provisions, Insufficient regulation of digital currencies, Delays in information exchange, andInadequate resources. Addressing these issues is essential to closing existing loopholes and reducing the opportunity for criminals to exploit the financial system as a tool for cybercrime. These challenges align with the Routine Activity Theory (RAT) by Cohen and Felson (1979), which asserts that crime occurs when a motivated offender encounters a suitable target in the absence of a capable guardian. Furthermore, Hirschi's (1969) Social Control Theory posits that individuals are less likely to commit crimes when robust social control mechanisms are in place. Similarly, the concept of victimology highlights that certain groups are more prone to victimization due to factors such as risky internet usage behavior, lack of cybersecurity awareness, or excessive trust in online banking systems—making them easy targets for deception. Therefore, the operations of government agencies such as the Royal Thai Police and the Anti-Money Laundering Office (AMLO) should prioritize public education on cyber risks, alongside efforts to develop technologies capable of detecting suspicious behaviors. This approach is consistent with the Social Control Theory, which emphasizes the importance of preventive measures and minimizing the likelihood of individuals becoming victims of cybercrime.

4. Guidelines and Measures for Cybercrime Prevention and Suppression: Case of Seizure and Suspension of Suspected Bank Accounts

This research proposes a structured four-step model for the suspension and seizure of suspected bank accounts in Thailand, comprising:(1) Detection and Alert of Suspicious Transactions.Using AI, machine learning, and the Central Fraud Registry (CFR) system to analyze abnormal transaction patterns and issue alerts for potential fraudulent activities. (2) Verification and Confirmation of Information.Government agencies and financial institutions examine transaction records, account registration data, and financial trails of suspected individuals to verify the legitimacy of the transactions. (3) Account Seizure and Transaction Suspension.Banks and regulatory authorities are authorized to suspend suspicious accounts within 7 days, with the condition that victims must file a formal complaint within 72 hours to extend the suspension period. (4) Legal Proceedings and Account Release Law enforcement agencies assess available evidence. If wrongdoing is confirmed, legal action is taken under relevant laws. If evidence is insufficient, the account must be released within the legally defined period. These measures are designed to enhance the effectiveness of law enforcement and crime prevention mechanisms, aligning with the Broken Windows Theory (Wilson & Kelling, 1982), which advocates for proactive enforcement to deter further criminal behavior.

Each responsible agency is assigned specific duties at every stage, as outlined in Table 1.

Table 1. Operational Responsibilities of Relevant Agencies in Cybercrime Prevention and Suppression — Case of Seizure and Suspension of Suspected Bank Accounts

Step	Agency	Responsibilities
1. Detection and Alert of Suspicious Transactions	- Financial Institutions - Electronic Wallet Providers - Telecommunications Providers - Anti-Online Scam Operation Center (AOC)	- Use AI and Machine Learning to analyze abnormal transactions - Report suspicious transactions to the Central Fraud Registry (CFR) - Provide public reporting services via Hotline 1441 (AOC)

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Step	Agency	Responsibilities
2. Verification and Confirmation of Information	- Royal Thai Police - Anti-Money Laundering Office (AMLO) - Bank of Thailand (BOT) - Ministry of Digital Economy and Society (MDES) - National Broadcasting and Telecommunications Commission (NBTC)	- Investigate suspicious transaction data in the CFR system - Request phone registration and financial transaction information from banks and telecom providers - AMLO analyzes financial trails
3. Account Seizure and Transaction Suspension	- Financial Institutions - Anti-Money Laundering Office (AMLO) - Technology Crime Suppression Division (TCSD) - Department of Special Investigation (DSI)	- Issue seizure orders for suspected accounts within 7 days - Suspend interbank transactions through the CFR system - Victims must report the incident within 72 hours to extend the seizure period
4. Legal Proceedings and Account Release	- Police - Anti-Money Laundering Office (AMLO) - Prosecutors - Criminal Court - Department of Special Investigation (DSI)	- If evidence of wrongdoing is found, proceed with prosecution under anti-money laundering and cybercrime laws - If no sufficient evidence is found within 7 days, the account must be released - AMLO handles money laundering cases, and the Bank of Thailand ensures financial institution compliance

The researcher synthesized a model to illustrate the process of cybercrime prevention and suppression, specifically in the case of account seizure and suspension, as depicted in Figure 1

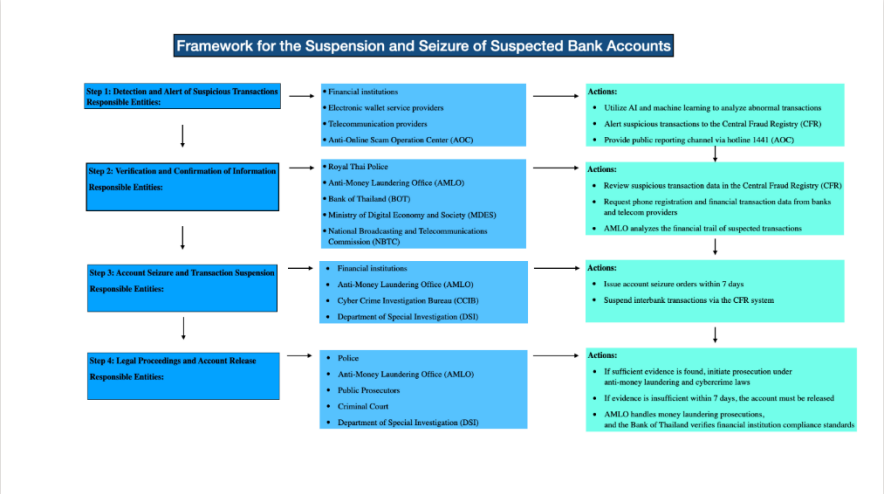

Figure 1 a model to illustrate the process of cybercrime prevention and suppression, specifically in the case of account seizure and suspension

CONCLUSION

The development of cybercrime prevention and suppression measures—specifically concerning the seizure and suspension of suspected bank accounts—in Thailand is primarily guided by the Royal Decree on Measures for the Prevention and Suppression of Technological Crimes B.E. 2566. This legislation aims to address technological fraud and the criminal transfer of assets. However, challenges remain, including the limited duration of account suspension, ambiguous legal conditions, delays in information exchange, and inadequate resources. To enhance the effectiveness of cybercrime prevention and suppression, both government and private sector entities must improve transaction monitoring mechanisms through the Central Fraud Registry (CFR). These improvements should

encompass cryptocurrency-related transactions and incorporate technologies such as e-KYC (electronic Know Your Customer) and biometric identification to reduce the use of mule accounts. Additionally, providing citizens with accessible channels for reporting incidents—such as through government applications—and utilizing AI-based fraud detection systems is essential. Furthermore, the regulatory scope should be expanded to include digital asset transactions and social media platforms to strengthen preventive capabilities. The study also recommends investment in cyber threat detection development and inter-agency collaboration to ensure long-term effectiveness in combating technological crime. This research presents a four-step model for the seizure and suspension of suspected bank accounts in Thailand:(1) Detection and alert of suspicious transactions (2) Verification and confirmation of information (3) Seizure of accounts and suspension of transactions and (4) Legal proceedings and account release. These measures contribute to sustainable and efficient cybercrime prevention and suppression efforts in the country.

NOTE ON ETHICAL ISSUE

This study was approved by the Human Research Ethics Committee in the field of Social Sciences, Mahidol University, Thailand, under approval number 2023/202.2911.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

REFRENCES

[1] Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44, 588–608.
[2] Elias, R. (1983). Victims: Crime victims and compensation in American politics and criminal justice. New Brunswick, NJ: Transaction Books.
[3] Halder, D., & Jaishankar, K. (2011). [Referenced in main text; full citation not provided].
[4] Hirschi, T. (1969). Causes of Delinquency. Berkeley: University of California Press.
[5] Jeffery, C. R. (1971). Crime Prevention Through Environmental Design. Beverly Hills, CA: Sage Publications.
[6] Kundi, A., & Nawaz, R. (2014). Digital revolution, cyber-crimes and cyber legislation: A challenge to governments in developing countries. Journal of Information Engineering and Applications, 4(4), 61–70.
[7] Ludwig von Bertalanffy. (1968). Passages from General System Theory. Retrieved from http://silvae.cfr.washington.edu/ecosystem-management-systems.html
[8] Manatsanan Pinpitak. (2023). Legal issues concerning the illicit opening of mule accounts in Thailand. Journal of Humanities and Social Sciences, Sisaket Rajabhat University, 7(1), 201–215.
[9] Narong Kulnitas. (2015). Models and measures for addressing cybercrime. Proceedings of the 6th National and International Research Conference, 224–237.
[10] National Institute of Standards and Technology. (2018). Cybersecurity Framework.
[11] Nuredini, A. (2014). Challenges in combating cybercrime. Mediterranean Journal of Social Sciences, 5(9), 592–599.
[12] Sorawit Boonmee. (2023). Call center scams: From economic to technological crimes. Journal of Science and Technology, Eastern Asia University, 17(5), 19–26.
[13] Thai Bankers' Association. (2023). DES joins hands with 5 agencies to launch Central Fraud Registry system. Retrieved from: https://www.tba.or.th/ดี-อี-เอส-จับมือ-5-หน่วยงาน.
[14] Thairath Online. (2023). Confiscated assets from Chinese crypto investors to be returned to 1,200 victims—First case. Retrieved from: https://www.thairath.co.th/news/local/central/2726195
[15] Travis Hirschi. (1969). Causes of Delinquency. Berkeley: University of California.
[16] Wilson, J. Q., & Kelling, G. L. (1982). Broken windows: The police and neighborhood safety. Atlantic Monthly, 249(3), 29–38.
[17] Jirapatch Panthawornchai. (2018). Cyber resilience framework development for cloud computing. Master's thesis, School of Information Technology, Sripatum University.
[18] Ariyatat Kaewkorsana. (2017). Army Cyber Center. Bangkok: Academic Office, Secretariat of the House of Representatives.