CHANDLER
MORI HAMADA

Newsletter

April 21, 2025

# Efforts to Combat Cybercrime: New Emergency Decrees on Cyber Crime and Digital Assets Implemented


Panupan Udomsuvannakul
Partner
panupan.u@morihamada.com

Koraphot Jirachocksubsin
Counsel
koraphot.j@morihamada.com


The Thai Cabinet has recently approved two significant draft Emergency Decrees, namely, the amendment to the Emergency Decree on Measures for the Prevention and Suppression of Technology Crimes B.E. 2566 (2023) (the "**Amended 2023 Emergency Decree**"), and the amendment to the Emergency Decree on Digital Asset Business Operation B.E. 2561 (2018) (the "**Amended Digital Assets Decree**"), aimed at bolstering the country's legal framework against technology-related crimes. These new laws, proposed by the Ministry of Digital Economy and Society (the "**MDES**") and approved by the Office of the Council of State, are designed to address the growing threat of cybercrime and regulate digital asset business operations more effectively.

The primary objective of the Amended 2023 Emergency Decree is to strengthen the legal framework in order to effectively combat technology-related crimes. The amendment aims to address the inadequacies of current legal enforcement, expedite the process of victim restitution, and impose stricter penalties on offenders. By doing so, these laws seek to mitigate public suffering, reduce social issues, and protect the Thai economy from the adverse impacts of cybercrime. The Amended Digital Assets Decree seeks to regulate digital asset businesses which offer services to Thai consumers from abroad.

CHANDLER
MORI HAMADA

# Key provisions of Amended 2023 Emergency Decree

1. **Amendments to Definitions:**
    - The term "business operator" now includes digital asset businesses under the Digital Asset Business Operation Act, while definitions for "digital asset wallet" and "electronic money account" have also been added.
2. **Enhanced Authority for State Agencies and Service Providers:**
    - The National Broadcasting and Telecommunications Commission (the "NBTC") and mobile service providers are empowered to temporarily suspend suspicious mobile numbers suspected of being used in cybercrime activities. This measure targets SIM cards used in criminal activities and aims to disrupt the communication channels of fraudsters.
    - Financial institutions and telecom providers are tasked with preventing illegal transfers and freezing mule accounts. This includes monitoring transactions and taking proactive steps to block accounts suspected of being involved in fraudulent activities.
3. **Data Disclosure and Exchange:**
    - Provisions have been added to allow disclosure and exchange of digital asset wallet numbers. The Securities and Exchange Commission (the "SEC") is designated as the regulatory agency that oversees digital asset businesses through data exchange mechanisms.
4. **Tech Crime Prevention Measures:**
    - Procedures have been introduced to screen out messages that are clearly scams, such as online gambling invitations or fraudulent investment promotions, without requiring users to click on any links.
5. **Victim Restitution:**
    - Specific procedures are established for the Transactions Committee under the Anti-Money Laundering Act to expedite refunds to victims without waiting for final court verdicts.
    - All procedures and criteria for returning funds to victims will be outlined in ministerial regulations. If no claims are made within 10 years, or if excess funds remain, the money will be transferred to the Anti-Money Laundering Fund, without affecting the rights of the original owners to reclaim it.

6. **Increased Penalties:**
    - There are stricter penalties for various technology-related offenses, including up to 5 years in prison and fines of up to THB 5 million for buying or selling personal data. This aims to deter individuals and organizations from engaging in misuse or misappropriation of data.
    - Penalties for online gambling offenders and those laundering criminal proceeds via cryptocurrencies include up to 1 year in prison and fines of up to THB 100,000. These measures target the financial incentives behind cybercrime and aim to reduce its prevalence.
    - There are also penalties for individuals who sell or register SIM cards with incomplete or incorrect information, knowing they could be used in tech crimes.
7. **Telecom Service Suspension and Data Removal:**
    - Agencies such as the Royal Thai Police, Department of Special Investigation (DSI), Anti-Money Laundering Office (AMLO), or the Cybercrime Operations Center can notify and request the NBTC to order telecom providers to suspend services used for technology crimes.
    - Authorized officers may order the removal or blocking of illegal computer data from systems if digital asset businesses operate without proper licenses.
8. **Private Sector Responsibility:**
    - Private entities must provide evidence of their compliance with regulatory standards to avoid liability for damage caused by tech crimes. This provision will ensure that businesses take proactive measures to prevent cybercrime and are held accountable for their role in safeguarding digital transactions.

The Amended 2023 Emergency Decree was published in the Royal Gazette on April 12, 2025 and came into full force and effect the following day.

## Key provisions of Amended Digital Assets Decree

This law also came into effect the day after its publication in the Royal Gazette on April 12, 2025. It includes a provision requiring digital asset businesses, which operate outside of Thailand but offer services to people in Thailand, to obtain proper licenses under Thai law.

The criteria for deeming whether services are offered to users in Thailand include the following:

- The service is partially or fully displayed in the Thai language.
- Payments can be made in Thai Baht.
- Payments are accepted via Thai banks or electronic accounts.
- Transactions are governed by Thai law or are subject to the jurisdiction of Thai courts.

The enactment of these draft Emergency Decrees marks a pivotal step in Thailand's efforts to combat cybercrime. As cybercriminals continue to employ increasingly sophisticated tactics, these enhanced legal measures are crucial for protecting the public and the economy from the detrimental effects of online fraud and data misappropriation and misuse. The swift implementation of these laws will be instrumental in ensuring justice for victims and maintaining the integrity of Thailand's digital landscape. By addressing the inadequacies of current legal enforcement and introducing comprehensive measures to prevent and suppress technology-related crimes, Thailand is taking a significant step towards a safer and more secure digital future.

Chandler Mori Hamada will closely monitor these legal developments and keep you informed of any updates. If you have any questions in relation to the issues raised in this newsletter, please contact the authors listed above.