Unofficial Translation*

EMERGENCY DECREE
ON MEASURES FOR THE PREVENTION AND SUPPRESSION OF TECHNOLOGICAL CRIMES, B.E. 2566 (2023)

———————

His Majesty King Maha Vajiralongkorn Phra Vajiraklaochaoyuhua
Given on the 9th Day of March B.E. 2566;
Being the 8th Year of the Present Reign.

His Majesty King Maha Vajiralongkorn Phra Vajiraklaochaoyuhua is graciously pleased to proclaim that:

Whereas it is expedient to have a law on measures for the prevention and suppression of technological crimes;

This Emergency Decree contains certain provisions in relation to the restriction of rights and liberties of a person, in respect of which section 26 in conjunction with section 32, section 36, section 37 and section 40 of the Constitution of the Kingdom of Thailand so permit by the virtue of law;

The justification and necessity for the restriction of rights and liberties of a person under this Emergency Decree is to protect honest people who have been deceived and lost their property by telephone calls or electronic means, which is a situation in which many people are being deceived each day and the damage value is very high, and therefore it is expedient to have measures to prevent and suppress all crimes of this kind immediately, which is an emergency of necessity and urgency which is unavoidable, in order to maintain national and public safety and national economic security and, in this regard, the enactment of this Emergency Decree duly complies with the conditions provided in section 26 of the Constitution of the Kingdom of Thailand;

By virtue of section 172 of the Constitution of the Kingdom of Thailand, an Emergency Decree is hereby enacted, as follows:

* Translated by Ms. Arriya Phasee under contract for the Office of the Council of State of Thailand. - Initial version - pending review and approval.

Section 1. This Emergency Decree is called the "Emergency Decree on Measures for the Prevention and Suppression of Technological Crimes, B.E. 2566 (2023)".

Section 2. This Emergency Decree shall come into force as from the day following the date of its publication in the Government Gazette. [1]

Section 3. In this Emergency Decree:

"technological crime" means an act or an attempt of committing an offence under the law on commission of offences relating to computer in order to defraud, extort or blackmail any person or in a manner likely to cause injury to any other person, or a commission of an offence of defraud, extortion or blackmail using a computer system as an instrument;

"financial institution" means a commercial bank and a State financial institution established by a specific law in accordance with the law on financial institution business;

"business operator" means an operator of a business under the law on payment systems.

Section 4. In order to prevent and suppress technological crimes, in the case where there is reasonable cause to suspect that a technological crime has been or may have been committed, the financial institution and business operator shall have a duty to disclose or exchange, between them, the information in relation to accounts and transactions of the concerned customer via an information disclosure or exchange system or process mutually agreed upon by the Ministry of Digital Economy and Society, the Royal Thai Police, the Department of Special Investigation, the Anti-Money Laundering Office and the Bank of Thailand.

For the purpose of implementing the objectives under paragraph one, the telephone network service providers, the providers of other telecommunication services or other related service providers shall have a duty to disclose or exchange, among them, the information of service provisions concerned via an information disclosure or exchange system or process mutually agreed upon by the Ministry of Digital Economy and Society and the Office of The National Broadcasting and Telecommunications Commission.

---

[1] Published in the Government Gazette Vol. 140, Part 18a, Page 1, dated 16th March B.E. 2566 (2023).

When the information has already been disclosed or exchanged under paragraph one or paragraph two, the person disclosing or exchanging such information shall immediately inform the Royal Thai Police or the Department of Special Investigation, as the case may be, and the Anti-Money Laundering Office, and after being informed, the Royal Thai Police, the Department of Special Investigation or the Anti-Money Laundering Office, as the case may be, shall have power to use such information for the purpose of preventing or suppressing technological crimes.

Section 5. In the case where there is reasonable cause to suspect that a technological crime has been committed and the information of user registration or computer traffic data is required to be obtained, the Royal Thai Police, the Department of Special Investigation or the Anti-Money Laundering Office, as the case may be, shall have power to order the telephone network service providers, the providers of other telecommunication services or other service providers relevant to such commission to disclose relevant information to the extent necessary, and after receiving such order, the telephone network service providers, the providers of other telecommunication services or other service providers relevant to such commission shall have a duty to submit such information to the person who gave the order within a period of time prescribed by such person.

Section 6. In the case where a financial institution or a business operator discovers reasonable cause by itself to suspect that, or receives information from the information disclosure or exchange system or process under section 4 that any deposit account or electronic money account has been used or may have been used to execute a transaction relating to technological crime or a predicate offence or an offence of money laundering under the law on money laundering control, the financial institution or business operator shall have a duty to suspend the transaction and inform financial institutions or business operators that accept the next transfer, together with entering the information into the information disclosure or exchange system or process under section 4 for all financial institutions and business operators that accept the transfer to be informed and temporarily suspend such transaction immediately for not more than seven days from the date of discovery of the suspicious cause or receipt of the notification, as the case may be, for verification, and inform a competent official authorised to prosecute a criminal case or the Secretary-General of the Money Laundering Control Board to conduct an examination.

In the case where a financial institution or a business operator receives notification of the incident under paragraph one from a competent official who is authorised to prosecute a

criminal case or the Secretary-General of the Money Laundering Control Board, the financial institution or business operator shall have a duty to suspend the transaction, together with entering the information into the information disclosure or exchange system or process under section 4 for all financial institutions and business operators that accept the transfer to be informed and suspend such transaction immediately, and then inform the persons concerned.

When the competent official who is authorised to prosecute a criminal case or the Secretary-General of the Money Laundering Control Board has conducted an examination and there is reasonable evidence for believing that the deposit account or electronic money account has been used for committing the offence, he or she shall proceed in accordance with law within seven days from the date of receipt of the notice of suspension of the transaction under paragraph one or the date of notification to the financial institution or business operator under paragraph two. If there is no reasonable evidence for believing that such deposit account or electronic money account has been used for committing the offence, he or she shall notify the results of the examination to the financial institution or business operator to cancel the suspension of the transaction.

After the period of time under paragraph three has elapsed, if the competent official who is authorised to prosecute a criminal case or the Secretary-General of the Money Laundering Control Board does not notify the results of the examination, the financial institution or business operator shall cancel the suspension of such transaction.

Section 7. In the case where a financial institution or a business operator is informed, by a victim who holds a deposit account or electronic money account, that a transaction has been executed by such deposit account or electronic money account and somehow is relevant to technological crime, the financial institution or business operator shall have a duty to temporarily suspend such transaction, together with entering the information into the information disclosure or exchange system or process under section 4 for all financial institutions and business operators that accept the transfer to be informed and suspend such transaction immediately, and inform the victim to file a complaint with an inquiry official within seventy two hours. After a complaint has been made, the inquiry official shall inform the financial institution or business operator accepting to execute the transaction for acknowledgement and the inquiry official shall consider taking action in relation to such deposit account and electronic money account within seven days from the date of receipt of the complaint. If no order of suspension of the transaction is issued within such period of time, the financial institution or business operator shall cancel the suspension of such transaction.

Section 8. Notification of information or evidence under section 6 and section 7 may be made by telephone or electronic means. If by telephone, the recipient shall record the information in writing, affix his or her signature and record the date and time of the receipt, together with sending a copy thereof to the informant as evidence.

A complaint for an offence relating to technological crime may be made with an inquiry official at any police station in the Kingdom or with the Cyber Crime Investigation Bureau, and may be made by electronic means which shall be deemed a valid complaint according to the Criminal Procedure Code. In conducting an inquiry or taking any action in relation to the commission of such offence, the inquiry official accepting the complaint, irrespective of the place at which he or she is stationed, or the inquiry official designated by the Commissioner-General of the Royal Thai Police shall be the responsible inquiry official who has power to conduct an inquiry and take actions in relation to the commission of such offence, irrespective of the place in the Kingdom in which such offence occurs.

Section 9. Any person who opens or allows other persons to use his or her deposit account, electronic card or electronic money account without the intention of using it for himself or herself or for the business with which he or she is involved or allows other persons to use or borrow a telephone number for his or her mobile phone service, while knowing or should have known that it would be used to commit an offence relating to technological crime or any other criminal offence, shall be liable to imprisonment for a term not exceeding three years or to a fine not exceeding three hundred thousand baht or to both.

Section 10. Any person who is engaged in procuring, advertising or propagating in any way to effect a purchase, sale, renting out or lending of deposit accounts, electronic cards or electronic money accounts to be used for committing an offence relating to technological crime or any other criminal offence, shall be liable to imprisonment for a term of two to five years or to a fine of two hundred thousand to five hundred thousand baht or to both.

Section 11. Any person who is engaged in procuring, advertising or propagating in any way to effect a purchase or sale of telephone numbers for a mobile phone service whose user has already been registered in the name of a particular person but cannot be identified, shall be liable to imprisonment for a term of two to five years or to a fine of two hundred thousand to five hundred thousand baht or to both.

Section 12. Disclosure, exchange, access as well as storage, collection or use of personal information under this Emergency Decree shall not be subject to the law on personal data protection, but the person who receives or possesses the information shall not disclose the same to other persons who do not have relevant duties.

Section 13. At the initial term, the Prime Minister shall appoint a committee consisting of the number of members as he or she sees fit to prescribe technological crime prevention and suppression guidelines and provide suggestions in relation to the suspicion under this Emergency Decree, as well as providing recommendation and consultation in relation to public authorities and relevant agencies' works for the execution of this Emergency Decree. In this regard, the Office of Permanent Secretary for the Ministry of Digital Economy and Society shall act as an administration unit of such committee and the Permanent Secretary of the Ministry of Digital Economy and Society shall appoint public officials of the Office of Permanent Secretary for the Ministry of Digital Economy and Society as secretary and assistant secretaries and the Commissioner-General of the Royal Thai Police may appoint public officials of the Royal Thai Police as assistant secretaries.

Upon expiration of a five-year period after this Emergency Decree comes into force, the Office of Permanent Secretary for the Ministry of Digital Economy and Society shall evaluate the necessity of the continuance of the committee under paragraph one for carrying out such duties and propose to the Council of Ministers for consideration and approval. In the case where it is necessary that the committee continue to exist, the Office shall also nominate an agency to act as an administration unit of the committee. In the case where the Office finds that it is not necessary that the committee continue to exist and the Council of Ministers resolves to approve the same, such committee shall be terminated from the date on which the Council of Ministers gives such resolution or the date prescribed by the Council of Ministers, as the case may be.

In the case where it is viewed that the committee under paragraph one should continue to exist, the Council of Ministers may require that the committee continue to perform its duties from time to time or permanently. In this case, the appointment and office term shall be in accordance with Rules prescribed by the Council of Ministers.

Section 14. The Prime Minister and the Minister of Digital Economy and Society shall have charge and control over the execution of this Emergency Decree.

Countersigned by:
General Prayut Chan-o-cha
Prime Minister

Remarks: The reason for enactment of this Emergency Decree is that whereas currently, technological methods are used to deceive the general public through various technological devices, causing people to lose a lot of property and the scammers have transferred the property obtained from such offences through the deposit accounts, electronic cards or electronic money accounts of other persons in rapid succession in order to conceal or disguise the offences. Each day, many honest people are being deceived and the damage value is very high, and such deception which is an offence is increasing, which affects a wide population and is extremely dangerous to the country's economic system. It is an emergency of necessity and urgency which is unavoidable. For the purpose of establishing measures to prevent and suppress such technological crimes in order to maintain national and public safety and national economic security, it is necessary to enact this Emergency Decree.