Issue 25 | May 2023

SIAM PREMIER
INTERNATIONAL LAW OFFICE LIMITED

New Cybercrime Decree bring in Banks and other Payment Service Providers as Key Allies in Fighting Cybercrime

Maythawee Sarathai, Partner; Rawat Chomsri, Partner; Kesara Summacarava, Senior Associate

On 17 March 2023, the Royal Decree on Measures for Prevention and Suppression of Technology Crimes B.E. 2566 (2023) ("**Cybercrime Decree**") became effective after its publication in the Royal Gazette. The purpose of the Cybercrime Decree is to provide enhanced protection to individuals against losses resulting from fraudulent activities conducted via online, telephone and other electronic means.

Specifically, it seeks to protect victims, while empowering banks and authorities to better combat online scams and other illegal online activities, particularly from the illegal use of bank accounts, electronic cards or electronic wallets for money-laundering (where the account holder has been procured to open such accounts, commonly known in Thai as "horse accounts" or "mule accounts").

There are three ways in which the Cybercrime Decree protects and empowers these parties: through suspension of suspicious accounts, the sharing and exchange of information, and the introduction of increased penalties.

Suspension of Transactions

The Cybercrime Decree sets forth the obligation for banks and payment service providers to temporarily suspend transactions of accounts suspected of being used for cybercrime or money laundering for up to seven days. Suspicion may arise from victims alerting banks or payment service providers, or the banks or payment service providers' own reasonable suspicions. In the future, banks or payment service providers may also receive relevant information thorough the data sharing/exchanging system or procedure to be designated by the relevant authorities pursuant to the Cybercrime Decree.

The bank or payment service provider must inform the victim to file a police complaint within 72 hours of such report or alert. After the compliant is made, the inquiry officer shall notify such bank or payment service provider and shall consider whether to take action in relation to such account within seven days from the date of receipt of the complaint. If no further suspension is ordered within such 7 days from the relevant officer, the suspension must be cancelled by such bank or payment service provider.

Obligation to Share Information of Accounts and Transaction Suspected of Cybercrime Involvement

Banks and payment service providers are required to share or exchange data regarding accounts and transactions suspected of being used in the perpetration of a cybercrime among themselves via the data sharing and exchanging system or procedure to be designated by the relevant authorities pursuant to the Cybercrime Decree. Furthermore, the relevant mobile service providers and/or telecom operators are also required to share or exchange data via such system or procedure.

After such data sharing, the data provider shall immediately notify the Royal Thai Police or the Department of Special Investigation (DSI), as the case may be, and the Anti-Money Laundering Office (AMLO), who shall, upon receipt, have the authority to use such data for protection, prevention and suppression of cybercrime.

Note that the sharing, exchanging, accessing, retaining and collecting of any personal data under the Cybercrime Decree are not subject to the Thailand's Personal Data Protection Act B.E. 2562 (2019), provided the data recipient or controller shall not disclose personal data to an unrelated person/party.

For more information, please contact:
Maythawee Sarathai I Partner: maythawee@siampremier.com
Rawat Chomsri I Partner: rawat@siampremier.com
Kesara Summacarava I Senior Associate: kesara@siampremier.com
Or Tel: +66 2 646 1888

SIAM PREMIER
INTERNATIONAL LAW OFFICE LIMITED

SIAM PREMIER
INTERNATIONAL LAW OFFICE LIMITED

26/F The offices at Central World No. 999/9
Rama I Road, Pathumwan, Bangkok 10330

Tel: +66 (0) 2646 1888
Email: spi-info@siampremier.com