No. 10/2023

The Bank of Thailand issues additional measures to combat financial fraudulent activities.

Mr. Sethaput Suthiwartnarueput, Governor of the Bank of Thailand (BOT) emphasizes the magnitude of fraudulent activities nowadays which evolve in many forms such as short message service (SMS), call-center gang, fraud loan and money-siphoning application. This causes financial loss to people and affects their confidence in digital banking which may lead to wider impact on financial services in the future.

The BOT does recognize the situation and has persistently collaborated with related organizations, both inside and outside the financial sector, to "prevent, detect and respond" against fraudsters and help financial fraud victims. The BOT has urged all financial institutions to speed up in taking steps to safeguard their customers, and coordinated with the National Broadcasting and Telecommunication Commission as well as the Ministry of Digital Economy and Society, and the Thailand Banking Sector Computer Emergency Response Team (TB-CERT), to block fraudulent SMS.

However, the current measures must be strengthened, in particular the evolution of fraudulent forms, the increasing volume of mule accounts, and the lengthy process for freezing suspicious accounts. In this light, the BOT introduces additional measures to combat financial fraudulent activities from the end-to-end process. All financial institutions are required to comply with the same minimum standards, considering the balance between managing risk and promoting digital financial services as follows;

1. Preventive measures to curb fraudsters' access to customers. All financial institutions are required to ban sending links in SMS or email and ban sending links requesting personal information such as usernames, passwords and ID numbers via social media. For each mobile banking application, the mobile banking users are limited to have one username and can use only one device. Each mobile banking transaction must be prior notified to the user. The mobile banking security system must be constantly upgraded, the biometric authentication is required, for example, a facial scan is needed to verify identity for opening a new bank account through banking application (non-face-to-face) or

conducting digital money transfer of more than 50,000 baht per transaction or changing daily transfer limit to over 50,000 baht. The daily withdrawal or transfer limit will be determined properly upon customers' risk profile and could be changed if necessary, where identity verification is strictly required.

2. Detective and monitoring measures which enable the financial institutions to mitigate losses and reduce the use of mule accounts. Under this measures, the BOT will set criteria in detecting and monitoring suspicious transactions and the financial institutions are required to report suspicious transactions to the Anti-Money Laundering Office and to have in place the near real-time system which can detect suspicious transactions and temporarily freeze the transactions upon being detected.

3. Responsive measures. All financial institutions are required to set up a hotline call center as a separate channel available twenty-four hours for financial fraud victims to contact, and to be responsive when the loss occurs from the financial institutions.

In this regard, the BOT has urged all financial institutions to promptly implement all the measures. Some have already been done, most of the rest is targeted by March 2023. The BOT will also evaluate the effectiveness and review the measures from time to time to ensure the measures are still up to date and in line with situations.

Above all, the BOT's measures marks only one steppingstone for tackling fraudulent financial activities. The comprehensive framework to combat financial frauds needs the enforcement of the Royal Decree on Cybercrime Prevention and Suppression. The Royal Decree would empower the data sharing on suspicious transactions between financial institutions and relating authorities, also, the immediate block of any suspicious transactions by financial institutions and the imposing apparent penalty against those involving with mule accounts, as well as strengthening collaboration of related organizations for more concrete

Bank of Thailand

9 March 2023

Further information: Technology Risk Supervision Department

Tel : +66 (0) 2283 6574 , +66 (0) 0 2356 7695

E-mail : ITSupervision@bot.or.th