Opening Remarks TB-CERT Cybersecurity Annual Conference 2022 Seminar

"Next Chapter: Building Trust and Collaboration"

Ms. Siritida Panomwon Na Ayudhya

Assistant Governor, Payment Systems Policy and Financial Technology Group

22 September 2022

Khun Chartsiri Soponpanit

Advisor to the Board, The Thai Bankers' Association,

Distinguished guests, ladies and gentlemen,

- A very good morning to you all. It is my great pleasure to be here with you today, and would like to thank TB-CERT for inviting me to this seminar **"Next Chapter: Building Trust and Collaboration"**.
- This is to emphasize the importance of cybersecurity collaboration building in financial sector and to strengthen cyber awareness and readiness of members and related agencies in Thailand.
- After covid-19 pandemic, we observe its impacts on everyone, the way of living, doing businesses, including the arrival of financial technology bring new innovative financial services and products. Many financial Institutions have transformed into digital organizations and provided varied online services to serve the need of people in the New Normal.
- However, transitioning into a digital organization is like two sides of the same coin. One is convenience, fast, and cost efficiency. But the other is that it might exposes cyber risks and become an opportunity for criminals to craft more sophisticated and complex attacks.
- According to the report from the Thailand's National Cyber Security Agency or NCSA, **more than 94% of organizations in Asia are prone to cyber-attacks in 2022** increasingly, especially in Thailand. Without a doubt, this is because Thai people embraces new digital financial services rapidly as the number of Mobile banking accounts in Thailand increase to more than 85 million accounts. Together with the fact that the financial sector is one of the main targets of cyberattacks, this circumstance is incredibly challenging for us.

- The evolution of cyber threats advances rapidly. Attacking patterns become more systematic with connected networks of hacker groups to exploit the target successively. In the past few years, **attacking trends also shifted to target more on the customer's side**, specifically digital fraud.
- For example, malicious groups stole victims' debit or credit card information to purchase online products. Or some groups of scammers, who disguised themselves as a legitimate agency, tricked people into giving out personal information or transferring money.
- Moreover, **criminals are continually developing new attack patterns** to penetrate vulnerabilities in business ecosystem. For instance, targeting IT vendors who gain access to data, systems or software of financial institutions and conduct lateral movement into the internal system of financial institutions instead of directly attacking financial institutions.
- Thus, financial institutions and organizations need to put in place **policies to protect, detect, respond, and recover anomaly events more promptly**, along with **collaborating and sharing information and experiences** with related organizations.
- By cooperating within the sector, with national, and international organizations, we can reduce risk of successful cyber-attack and digital fraud effectively, as well as build people's trust and lay groundwork for further development of financial services.
- As for the banking sector in Thailand, we have Thailand Banking Sector CERT or TB-CERT, who is a **key organization to drive collaboration and information sharing** between financial institutions, other CERTs and other international agencies both domestic and international.
- Moreover, last year, TB-CERT played a leading role in strengthening cybersecurity capabilities for the banking sector and financial sector in multiple significant areas which are:
    - **Promoting the information security of Critical Information Infrastructure (CII)** in accordance with Thailand's Cybersecurity Act
    - **Developing standards and cyber incident response processes** for a better countermeasure such as working with the Bank of Thailand to develop a Guideline for Application Programming Interface (or API) Technology Adoption in Financial Services and creating a responsive plan to deal with SMS scams with NCSA

- **Building up staff's readiness** to boost the financial sector's immunity to prevent, monitor, and cope with new cyber threats
- **And last but not least, promoting cyber awareness and cyber hygiene** for people and customers to prevent falling victim to cyber and social engineering attacks
- On behalf of the Bank of Thailand, I would like to express my deepest thanks to TB-CERT executives and working teams, and also every related organization for your contribution and collaboration along this journey.
- I wish you all a successful and fruitful event and in agreement that cybersecurity collaboration is crucial for dealing with cyber threats effectively. This will help building confidence and strong immunity for the financial system and digital economy for sustainable growth in Thailand.

Thank you.