BANGKO SENTRAL NG PILIPINAS

MEMORANDUM NO. M-2022-015

OFFICE OF THE DEPUTY GOVERNOR
FINANCIAL SUPERVISION SECTOR

To : **ALL BSP SUPERVISED FINANCIAL INSTITUTIONS (BSFIs)**

Subject : **Recommended Control Measures Against Cyber Fraud and Attacks on Retail Electronic Payments and Financial Services (EPFS)**

As financial transactions increasingly shift to electronic or digital channels, attacks on retail customers using mobile and internet/web applications have risen. The most prevalent among the schemes employed are account takeover and social engineering attacks that involve phishing and its variations (e.g. smishing and vishing). These are intended to manipulate customers into disclosing sensitive personal and account information necessary to execute unauthorized transactions. Fraudsters are adept in exploiting legitimate application features and business rules as well as in bypassing layers of controls.

In view thereof, BSFIs should conduct continuing risk assessment of its product features, business rules and application controls, and implement appropriate enhancements and mitigation, as necessary. To ensure consistent and industry-wide approach in countering the aggressive phishing campaigns, BSFIs are advised to adopt the following supplementary control measures:

1. Removal of clickable links in emails or SMS sent to retail customers followed by an information campaign that the BSFI will no longer be sending clickable links.

2. Customer notification through existing mobile or email registered with the BSFI whenever there is a request to change a customer's mobile number, email address, or account credentials.
3. After the conduct of a thorough risk analysis and assessment, the implementation of the following controls:
    a. Mandatory fund transfer transaction notification to customers through SMS and/or email for transactions exceeding a predefined amount;
    b. Holding period or delay before activation of a new soft token on a mobile device; and
    c. Cooling-off period before the implementation of requests for key account changes such as those for the mobile number and email address.
4. Personalized SMS/Email OTP messages for device registration, fund transfer, and profile update, among others,
5. Restriction to any BSFI officer or representative from manually obtaining or inquiring about critical authentication information such as customer password and/or one-time password/pin (PIN).
6. Creation of dedicated and well-resourced customer assistance teams that deal with feedback on potential fraud cases on a priority basis.
7. Conduct of regular customer education campaigns against online scam and phishing schemes with mechanisms to monitor their effectiveness and relevance; and
8. Adoption of strong fraud surveillance mechanisms to ensure prompt responses in dealing with the growing threat of online scams.

The above recommendations are consistent with the risk-based approach espoused under existing regulations on IT risk management and financial consumer protection frameworks. These should supplement existing security controls including multi-factor authentication (MFA) implementation, calibration of fraud management system rules and parameters, conduct of threat hunting exercises, and takedown of phishing sites, among others.

Lastly, BSFIs are encouraged to collaborate and utilize existing information sharing platforms, such as the Bankers Association of the Philippines Cyber Incident Database (BAPCID), to facilitate fraud investigation and/or recovery of funds. In certain instances, BSFIs may need to seek assistance and cooperate with law enforcement authorities for prompt resolution of cybercrime cases, especially if these involve public safety and security, pursuant to the Cybercrime Prevention Act of 2012 and other relevant laws and regulations.

For information and guidance.

Digitally signed by
Chuchi G. Fonacier
Date: 2022.03.22
16:39:01 +08'00'

CHUCHI G. FONACIER

Deputy Governor

22 March 2022