



## **BANGKO SENTRAL NG PILIPINAS**

**OFFICE OF THE DEPUTY GOVERNOR  
FINANCIAL SUPERVISION SECTOR**

### **MEMORANDUM NO. M-2020-090**

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

**Subject : PHISHING AND OTHER SIMILAR SOCIAL ENGINEERING ATTACKS**

Phishing attacks remain to be one of the top cyber risks in the digital financial services landscape, especially in this time of the COVID-19 pandemic wherein the use of digital payments and financial services has significantly increased. Cybercriminals continue to utilize various platforms and tactics such as phishing emails, SMS phishing (smishing), SMS spoofing and voice phishing (vishing), including social media channels to gain unauthorized access to financial resources.

In view thereof, BSFIs are enjoined to revisit the recommended controls and measures in previous BSP Memoranda on Guidance on Management of Risks associated with Fraudulent E-mails or Websites<sup>1</sup>, SMS-Based Attacks Targeting Customers of Financial Institutions<sup>2</sup>, and other similar BSP issuances. BSFIs are also reminded to intensify information security awareness and education campaigns as a first line of defense against these phishing and social engineering attacks. Further, BSFIs should minimize risk exposure through employing defense-in-depth security strategies such as calibration of fraud management system rules and parameters, conduct of threat hunting exercises to detect unusual activities and takedown of phishing sites, among others.

Likewise, BSFIs should ensure that timely and appropriate consumer protection and redress mechanisms are in place. To preserve the banking public's trust and confidence in digital financial services, BSFIs are strongly advised to implement the following:

1. Consumer assistance helpdesk or hotline available 24 hours a day and 7 days a week (24x7)<sup>3</sup>;
2. Increased surveillance on online banking systems/activities during holidays or long weekends;
3. Facility to timely block/suspend accounts reported by clients/concerned parties or those tagged as fraudulent or suspicious; and
4. Procedures to resolve disputes arising from the use of the digital financial services within the established turn-around-time (TAT).

---

<sup>1</sup> Memorandum No. M-2015-025 dated 22 June 2015

<sup>2</sup> Memorandum No. M-2020-066 dated 19 August 2020

<sup>3</sup> In accordance with Appendix 115 of the MORB and Appendix Q-70/S-9/N-12 of the MORNBFI. Note that the operating hours may vary depending on the BSFI's risk management strategies.

Lastly, financial fraud resulting from phishing and other types of cyber-related crimes should be promptly reported to the BSP in accordance with Sections 148, 173 and 901 of the Manual of Regulations for Banks (MORB) and Sections 147-Q/145-S/142-P/126-N, Section 901-Q, Appendix Q-5/S-3/P-8/T-4, and Appendix N-1 of the Manual of Regulations for Non-Bank Financial Institutions (MORNBFi).

For information and guidance.

 Digitally signed  
by Chuchi G.  
Fonacier  
Date: 2020.12.12  
22:59:04 +08'00'

**CHUCHI G. FONACIER**  
Deputy Governor

12 December 2020