



## BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE DEPUTY GOVERNOR  
FINANCIAL SUPERVISION SECTOR

### MEMORANDUM No. M-2020- 066

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

Subject : **SMS-Based Attacks Targeting Customers of Financial Institutions**

As the industry shifts to digital payments and financial services in response to the COVID-19 pandemic, cyberthreat actors remain relentless in propagating malicious activities against BSP Supervised Financial Institutions (BSFIs) and their clients. A predominant type of attack pertains to phishing campaigns which lure and defraud BSFI employees and customers to disclose user account credentials and sensitive information or to click malicious links.

The BSP's ongoing cyberthreat surveillance shows that these types of attacks are increasingly carried out through the Short Message Service (SMS) system, more known as text messages via mobile phones. In particular, SMiShing is a form of phishing activity where fraudsters trick the users to click or download a malicious link to acquire information such as passwords and/or one-time PINs (OTP) through SMS. The effectiveness of this attack relies on the attacker's ability to convince the customers that immediate action is required and to deceive that the message originate from a legitimate or trusted sender. Thus, SMiShing is normally executed in combination with SMS spoofing, wherein the SMS sender ID is altered so that the message appears to be coming from a financial institution or entity. Moreover, financial consumers can be easily victimized since the fraudulent messages are co-mingled with the previous genuine/legitimate messages from the BSFI.

All BSFIs are therefore reminded to further intensify information security awareness and education campaigns for their employees, clients, and other relevant stakeholders against SMS-based attacks such as SMiShing and SMS spoofing. Likewise, BSFIs should revisit multi-factor authentication (MFA) controls implementation to address inherent vulnerabilities and weaknesses arising from SMS-based sending of OTPs. Given the fast-evolving nature of these attacks, BSFIs should adopt multi-layer controls such as calibration of fraud management system rules and parameters and conduct of threat hunting exercises to detect unusual activities and takedown phishing sites, among others. Lastly, as part of the BSFIs' consumer protection program, customers' verification requests and complaints in relation to SMiShing and SMS spoofing incidents must be acted upon immediately to minimize financial losses.

For information and guidance.



**CHUCHI G. FONACIER**  
Deputy Governor

19 August 2020