**BANGKO SENTRAL NG PILIPINAS**

OFFICE OF THE DEPUTY GOVERNOR
SUPERVISION AND EXAMINATION SECTOR

**MEMORANDUM NO. M-2017-018**

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

Subject : **Guidance on Managing Ransomware and Other Malware Attacks**

The subject guidance, previously communicated directly to BSFIs last 8 February 2017, is being re-issued in view of the recently reported global ransomware attacks.

*"With the alarming proliferation of ransomware, BSFIs are at an increased risk of loss or unauthorized disclosure of proprietary or sensitive information, operational disruptions, financial losses incurred to restore affected systems and reputational damage. Given the perceived anonymity of threat actors in perpetrating ransom payment schemes, ransomware remains a viable threat that is expected to evolve to more sophisticated and destructive forms, such as crypto-ransomware. Web-based applications, including legitimate cloud-based services, are particularly vulnerable to this type of threat.*

*In this regard, BSFIs are advised to heighten their vigilance and ensure that robust protection against ransomware is in place. BSFIs should provide multiple layers of defenses by implementing appropriate controls at the host, network, and endpoint level to prevent and detect malicious codes.*

*At a minimum, BSFIs should apply the "Least Privilege" principle in granting access to all systems and services and prohibit the download and use of unauthorized files and software (e.g., executable files and mobile codes), and access to doubtful websites. Other preventive measures include installation and timely update of anti-malware software provided by reputable vendors, periodic vulnerability scanning and effective patch management procedures for all critical systems and applications. To address the more sophisticated forms of ransomware, BSFIs should consider adopting advanced security solutions such as signature-less anti-malware solutions capable of analyzing abnormal behavioral patterns in network and system traffic flows. Likewise, application whitelisting which allows only specified programs to run and/or sandboxing technologies which can inspect incoming traffic such as e-mail attachments without compromising the production environment can be employed.*

*To mitigate the potential catastrophic impact of ransomware attacks, BSFIs should ensure that adequate back-up and recovery procedures for critical systems and data, including periodic testing to check the integrity thereof, are in place. Because back-ups may also be subject to attacks, BSFIs*

*should consider supplementing existing practices with cloud-based back-ups and/or back-ups using removable media or air-gapped facilities. Alongside these controls, BSFIs should strengthen user education and awareness to include employee safe practice procedures when using the email service and browsing the web.*

*If infected by a ransomware, BSFIs should refrain from paying or communicating with the malicious actor as this does not guarantee that ransomed and/or encrypted files will be released. Instead, paying ransom only encourages cyber criminals' illicit activities. BSFIs should proactively monitor the cyber-threat environment through robust, timely and actionable threat intelligence. Additionally, ransomware attacks should be covered by an established and well-tested incident response plan and procedures.*

*Finally, incidents involving cyber-extortion using ransomware, and other types of cyber-related crimes should be promptly reported to the BSP in accordance with Subsection X192.4 of the Manual of Regulations for Banks (MORB), as revised by Memorandum No. M-2016-014 dated 02 November 2016 and Section X177.8 of the MORB. In some instances, BSFIs may need to seek assistance and cooperate with 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."*

On top of the above-cited recommendations, BSFIs should continuously assess the cyber-threat landscape and adjust their information security programs, policies, processes, and capabilities accordingly. BSFIs may refer to leading security standards and frameworks set by standard-setting bodies, including specific inputs from their third-party service providers and security vendors, to effectively prevent, detect, respond to, and recover from these types of attacks.

**NESTOR A. ESPENILLA, JR.**
Deputy Governor

15 May 2017