BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE DEPUTY GOVERNOR
SUPERVISION AND EXAMINATION SECTOR

MEMORANDUM NO. M-2017-017

To : **ALL BSP-SUPERVISED INSTITUTIONS**

Subject : **REPORTED INCIDENTS OF FRAUDULENT E-MAILS AND WEBSITES**

In response to the growing concerns on cyber-attacks involving fraudulent e-mails and websites aimed at customers and employees of financial institutions, BSP-Supervised Financial Institutions (BSFIs) are advised to sustain resilience efforts and continue to perform rigorous risk assessments of their current technology environment. Further, BSFIs should ensure compliance with the following BSP issuances:

1. BSP Circular No. 958 dated 25 April 2017 – Adoption of Multi-Factor Authentication (MFA) Measures for Transactions Considered as Sensitive Communications and/or High-Risk; and

2. Memorandum No. M-2015-025 dated 22 June 2015 – Guidance on Management of Risks Associated with Fraudulent E-mails or Websites.

In addition to implementing risk-based authentication methods for customer accounts, BSFIs should also ensure adequate access control measures are in place for systems that support the provision of electronic products and services [e.g. authentication servers, application servers, domain name system (DNS) including domain registry services] regardless of whether these are managed internally or by a third-party service provider. For outsourced systems, BSFIs, as part of their outsourcing risk management framework, should have a sufficient level of assurance that the service provider is maintaining robust security controls.

Stronger authentication methods (other than the use of passwords) should be adopted for high-risk/sensitive systems that are managed by privileged users (e.g. network and system administrators). Accordingly, BSFIs should be guided by Item 3.2.3 (Security Administration and Monitoring) and Item 3.2.4 (Authentication and Access Control) of Appendix 75b of the MORB and Appendix Q-59b of the MORNBFI.

BSFIs should also be mindful of domain hijacking, whereby attackers modify a BSFI's domain name records to redirect users to unauthorized websites. In such cases, additional security measures such as registry lock feature[1] (for top-level domain) and MFA should be adopted.

[1] A measure which enforces manual verification and authentication of all change requests by the top level domain registrar

Further, BSFIs should actively promote a security conscious environment through security awareness and training programs for all personnel and, where relevant, contractors and third-party users in accordance with Item 3.2.10 (Personnel Security) of Appendix 75b of the MORB and Appendix Q-59b of the MORNBFI.

For compliance.

NESTOR A. ESPENILLA, JR.
Deputy Governor

10 May 2017