



BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE DEPUTY GOVERNOR
SUPERVISION AND EXAMINATION SECTOR

MEMORANDUM NO. M-2015- 025

To : ALL BSP-SUPERVISED FINANCIAL INSTITUTIONS

Subject : GUIDANCE ON MANAGEMENT OF RISKS ASSOCIATED WITH FRAUDULENT E-MAILS OR WEBSITES

Phishing attacks and fraud perpetrated via other vectors continue to be a primary concern affecting the financial services industry. The steady increase in the number of incidents as reported by banks mostly involves unauthorized intra or interbank fund transfer facilitated via phishing e-mails received by clients. Since the clients are the direct target of said attacks, failure to address such concern may result to diminished trust and confidence of the public in the financial system, particularly the use of online banking products and services. Moreover, while incidents of this nature remain a small percentage of the total cybercrime losses of the industry, the cyber threat landscape continues to evolve with more sophisticated versions of these attacks, such as pharming and spear phishing, not far in the horizon. BSP-Supervised Financial Institutions (BSFIs) are therefore enjoined to adopt appropriate risk management practices to adequately prevent, detect and proactively manage fraudulent e-mails or websites.

A. RELEVANT PROVISIONS AND GUIDELINES

BSFI's are reminded that, as specified in Section 4.1.11 Website information and maintenance under Appendix 75f and Q-59f of the Manual of Regulations for Banks (MORB) and Manual of Regulations for Non-Bank Financial Institutions (MORNBFI), respectively, *"The BSFI should manage the risk associated with fraudulent emails or websites which are designed to trick its customers into revealing private details such as account numbers or e-services passwords."*

To manage the risks associated with fraudulent e-mails or websites, BSFIs should, at a minimum, observe the following controls as required by the regulations:

Recommended Control Measures	Pertinent Provisions
• Dynamic consumer awareness program	Since phishing and its more sophisticated versions are mostly external attacks and normally beyond the control of the BSFI's security measures, the key defense lies in an effective, dynamic and well-designed consumer awareness program, which should be regularly reviewed/evaluated by senior management⁴. Further, BSFIs should educate their clients on: • <i>"the risks of using online financial services before they</i>

⁴ Section 4.3.3 Consumer Awareness of Appendix 75f and Q-59f of the MORB and MORNBFI.

	<i>subscribe to such services. Ongoing education must be available to raise the security awareness of customers to protect their systems and online transactions (Annex A of Appendix 75f and Q-59f of the MORB and MORNBFI)";</i> • <i>"ways to ensure that they are communicating with the official website and that they will not be required to access the BSFI's transactional e-services portal through hyperlinks embedded in e-mails unless the website is validated by legitimate digital certificate (Section 4.1.11 of Appendix 75f and Q-59f of the MORB and MORNBFI)."; and,</i> • <i>"security measures that must be put in place to uphold their interests in the online environment (Annex A of Appendix 75f and Q-59f of the MORB and MORNBFI)."</i> Expectations on the electronic services consumer awareness program are further summarized in Annex C of Appendix 75f and Q-59f of MORB and MORNBFI.
• Confirmations and identity checks to significant transactions or activities	BSFIs are expected to implement additional authentication and authorization controls for sensitive transactions or activities, such as (a) <i>"enrollment in a new on-line service, large fund transfers, account maintenance changes, or suspicious account activity"</i> (Subsection 4.1.6 Application security of Appendix 75f and Q-59f) and (b) <i>"when customer requests a change in his account information or other contact details"</i> (Subsection 4.2.1. Administration of E-Services Accounts of Appendix 75f and Q-59f).
• Strengthened infrastructure and security monitoring; and,	As successful cyber-attacks via fraudulent e-mails or websites usually manifest in suspicious online transactions or unusual activities, BSFIs should put in place strong monitoring mechanisms and processes to detect and respond to potential breaches in a timely manner. Subsection 4.1.7 Infrastructure and security monitoring of Appendix 75f and Q-59f has highlighted features of an effective infrastructure and system monitoring process: • Sound monitoring system - <i>"A sound monitoring system should include audit features that can assist in the detection of fraud, money laundering, compromised passwords or other unauthorized activities";</i> • Response - <i>"The BSFI's monitoring staff should be promptly alerted by its monitoring mechanism if suspicious online transfers and unusual activities are initiated. In these cases, the BSFI should, as soon as practicable, check with the account holders of these</i>

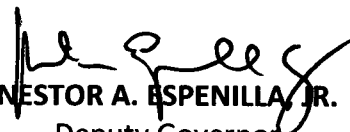
	<i>transactions or activities”; and,</i> • Consumer notification - <i>“Consideration should also be given to notifying personal customers immediately through an alternative automated channel (such as messages sent to mobile phones or e-mail accounts of customers) of online transfers made to unregistered third parties, online transfers exceeding certain amount limits, or detected unusual activities related to their accounts.”</i> For a more proactive approach, BSFIs should have mechanisms in place to monitor the external environment (e.g. surveillance of the existence of similar-looking/fraudulent websites) and take appropriate action when necessary. BSFIs have the option to avail the services of an external service provider if they do not have the expertise or capability to adequately manage external risks.
• Appropriate authentication techniques.	As part of consumer protection, BSFIs should also implement <i>“a mechanism to authenticate official website to protect customers from spoofed or faked websites. (Annex A of Appendix 75f and Q-59f: Online Internet Financial Services)”</i>. Dependent on the extent of services made available to client and its risk assessment, the BSFI should determine what authentication techniques to adopt to provide protection against cyber-attacks.

Given the evolving nature of the attacks and extensive potential damage of a successful widespread attack against the financial services sector, BSFIs are enjoined to proactively assess and institute resilience in their existing networks, security controls and customer awareness initiatives to preserve trust and confidence on the financial environment.

B. REPORTING REQUIREMENT

Incidents on fraudulent e-mails or websites perpetrated via phishing, pharming and other evolving forms of attacks involving the BSFIs or their clients should be reported to the BSP as prescribed under Section X177.8 and 4177Q.8/4196S.8/4193P.8/4196N.8 of the MORB and the MORNBFI.

For information and guidance.


NESTOR A. ESPENILLA, JR.
 Deputy Governor

22 June 2015