BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE DEPUTY GOVERNOR
SUPERVISION AND EXAMINATION SECTOR

MEMORANDUM NO.M-2014- 040

To : **ALL BSP-SUPERVISED INSTITUTIONS**

Subject : **CARD FRAUD AND SKIMMING ATTACKS**

Electronic payment cards (i.e., ATM debit, credit and prepaid cards) are still vulnerable to skimming attacks given the continued use of magnetic stripe technology. Pending migration of the entire payment card network to EMV[1] by 01 January 2017, electronic payment cards remain largely defenseless against modern fraud techniques unless multiple layers of protection are adopted by BSP-Supervised Institutions (BSIs).

To manage subject risk, BSIs are reminded to consider the specific controls to mitigate exposure from skimming attacks outlined under ***Annex "A"*** - Appendix 75f of Circular No. 808 dated 22 August 2013, namely:

- Installation or implementation of additional controls to ATM and POS machines, such as anti-skimming solution, tamper-resistant keypads or video surveillance;
- Establishment of detection process and alert mechanisms for timely and appropriate incident response and action; and
- Use of transaction alerts on withdrawals and other transactions exceeding certain defined thresholds.

Abovementioned controls highlight the BSI's need to (a) protect ATM and POS machines and (b) have proactive systems and processes in place to prevent, detect, manage or respond to card skimming incidents. Also, BSIs need to strengthen their customer awareness programs as a first line of defense against fraudsters reiterating the precautionary measures under ***Annex "C"*** - Appendix 75f of Circular No. 808.

A. SECURITY CONTROLS FOR AUTOMATED TELLER MACHINES (ATMs) AND POINT OF SALE (POS) DEVICES

BSIs shall put in place adequate safeguards as card skimming attacks may happen at various points in payment card processing, such as ATMs, payment kiosks and POS terminals. Following are the minimum security measures required for ATM facilities and POS devices pursuant to ***Annex "A"*** - Appendix 75f of Circular No. 808 with the corresponding additional recommended controls necessary given the evolving nature of the skimming attacks:

[1] EMV (stands for Europay, MasterCard and Visa) is a global standard for credit, debit and prepaid payment cards based on chip card technology. Chip cards are a more secure alternative to traditional magnetic stripe payment cards.

1. AUTOMATED TELLER MACHINES

Pertinent Provisions	Recommended Control Measures
• Locate ATM's in highly visible areas; • Provide sufficient lighting at and around the ATMs; and • Where ATM crimes (e.g., robbery, vandalism, skimming) are high in a specific area or location, the BSI should install surveillance camera or cameras which shall view and record all persons entering the facility. Such recordings shall be preserved by the BSI for at least thirty (30) days.	BSIs are expected to enhance their risk management processes to include the conduct of a thorough risk assessment, which considers, specific ATM model, ATM location, volume of transactions and such other factors necessary to identify those ATMs requiring additional controls. For those classified as high risk, installation of robust anti-skimming solutions and/or additional security devices and measures shall be necessary. The results of the risk assessment shall likewise be used to identify specific or vulnerable ATM models due for replacement.
• Implement ATM programming enhancements like masking/non-printing of card numbers.	Logical controls, such as transaction alert systems and/or notifications, shall also be considered by BSIs to ensure risks are appropriately mitigated or managed.
• Educate customers by advising them regularly of risks associated with using the ATM and how to avoid these risks; • Post a clearly visible sign near the ATM facility which, at a minimum, provides the telephone numbers of the BSI as well as other BSIs' hotline numbers for other cardholders who are allowed to transact business in the ATM, and police hotlines for emergency cases.	Consumer education remains one of the key defenses against fraud, identity theft and security breach. Concerned BSIs shall accordingly enhance their consumer awareness initiatives in response to the business environment. More than protection of the Personal Identification Number (PIN) and the measures outlined in ***Annex "C"*** - Appendix 75f of Circular 808, advisories on how to check for skimming devices shall also be released and posted in ATM premises.
• Conduct and document periodic security inspection at the ATM location.	Periodic security inspection is a necessary step to ensure that ATMs are not compromised. Other than security officers, BSIs shall consider requesting assistance of branch personnel in ensuring ATMs remain safe for the consumers. Inspection shall be documented and performed on a periodic basis, the frequency of which depends on the results of the risk assessment. To further promote confidence in the use of ATMs, BSIs shall post in their ATM premises information that ATM machines are regularly checked for the presence of skimming devices.

Pertinent Provisions	Recommended Control Measures
• Educate BSI personnel to be responsive and sensitive to customer concerns.	To manage reputational risk, adequate handling and containment of consumer concerns and complaints shall be undertaken by highly-trained BSI personnel. A well-defined customer complaint resolution process must be in place specifying prompt notifications as well as the conduct of investigations aimed at resolving issues and complaints within a reasonable timeframe.

2. POINT-OF-SALE DEVICES

Pertinent Provisions	Recommended Control Measures
• The party providing POS terminal must always increase the physical security around the vicinity of such POS terminal and on the POS terminal itself, among others, by using POS terminal that minimizes the possibility of interception on such terminal or in its communication network. • BSI deploying POS devices at merchant locations must familiarize the merchant with the safe operation of the device. The acquiring institution must ensure that the POS devices as well as other devices that capture information do not expose/store information such as the PIN number or other information classified as confidential. It must also ensure that a customer's PIN number cannot be printed at the point of sale for any reason whatsoever.	Similar to ATMs, physical security controls shall be in place for POS devices with the added concern on connectivity to minimize risk of interception in the established communication link. Risk assessment of POS terminals considering the location, volume and amount of transactions and other risk factors should also be undertaken. Likewise, POS devices shall be configured to assist in ensuring confidentiality of sensitive information so as to minimize opportunity for card skimming. In addition to physical and logical controls, BSIs should exercise proper oversight of their accredited merchants and enforce baseline controls in minimizing card skimming and fraud risks such as hiring practices and background checks of employees handling payment card processing.

B. PREVENTION, DETECTION, MANAGEMENTAND RESPONSE RELATIVE TO SKIMMING INCIDENTS

1. PREVENTION

Other than the minimum security requirements for ATMs and POS, ***Annex "A"*** - Appendix 75f of Circular No. 808 requires the study, analysis and assessment of ATM crimes to determine root cause and problem areas.

Lessons learned from BSI's or another BSI's experience shall be used to promote changes, measures or process improvements to prevent recurrence or occurrence of incidents to the BSIs.

2. DETECTION

In addition to consumer complaints handling, ***Annex "A"***- Appendix 75f of Circular No. 808 requires the implementation of fraud detection systems with behavioral scoring and correlation capabilities to identify and curb fraudulent activities even prior to completion of the transaction or knowledge of the consumer. The system will enable BSIs to effectively monitor actions by cardholders that deviate from usual card usage patterns which may subsequently lead to investigation.

3. MANAGEMENT AND RESPONSE

BSIs should establish processes necessary for the timely investigation and resolution of card fraud and skimming related cases. Such processes shall include determining, within a reasonable timeframe, the party liable for the loss and equitable compensation for affected customers once fraud has been established. Pursuant to this objective and ***Annex "A"*** - Appendix 75f of Circular No. 808, the BSP enjoins BSIs to implement collaboration and information sharing practices. Practices shall include sharing of CCTV video images whenever available, without extra financial charges, subject to data confidentiality agreements and related industry-wide policies and procedures. BSIs' policies and procedures should be harmonized to conform to this information sharing mechanism. Participation in industry collaboration and information sharing efforts such as the Inter-network Anti-Fraud Committee (IAFC) and the Information Security Officers' Group (ISOG) is also highly encouraged. In some instances, BSIs may need to seek assistance and cooperate with law enforcement agencies for prompt resolution of cybercrime cases, especially if these involve public safety and security.

BSIs that fail to adopt the abovementioned controls/measures to mitigate card fraud and skimming attacks may be subject to monetary and non-monetary sanctions provided under Subsection X176.9 of Circular No. 808.

For information and guidance.

CHUCHI G. FONACIER
Sector-in-Charge

3 October 2014