BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE GOVERNOR

CIRCULAR NO. 1019
Series of 2018

Subject: **Technology and Cyber-Risk Reporting and Notification Requirements**

The Monetary Board, in its Resolution No. 1723 dated 18 October 2018, approved the following amendments covering technology and cyber-risk reporting and notification requirements for Bangko Sentral supervised financial institutions (BSFIs). Subject requirements would enable the Bangko Sentral to have ready access to accurate, timely, and actionable information regarding BSFIs' technology risk profiles as well as the evolving cyber-threat environment for a more responsive, proactive and effective banking supervision.

Section 1. Subsections X177.5 of the MORB and Subsections 4177Q.5, 4196S.5, 4177P.5 and 4196N.5 of the MORNBFI, are hereby amended to include the following terminologies in the *Definition of Terms*:

Terminology	Definitions
Compromised State	A state wherein someone or something has maliciously broken into networks, systems and computers which raises doubt as to the integrity of information assets, such as, but not limited to, program files, image files, and operating system files.
Data Breach	An incident in which sensitive, protected or confidential data or information has potentially been viewed, stolen, leaked, used, or destroyed by unauthorized persons.
Hacking	Unauthorized access into or interference in networks, systems and computers without the knowledge and consent of the system/information owner.
Pharming	A form of cyber-attack that redirects a website traffic to another fake website to obtain user credentials and information.
Reportable Major Cyber-related Incidents	Any cyber-related incidents that meet the criteria for reporting/notification to the Bangko Sentral as laid out in Item a(2)(a)of Subsections X177.8/ 4177Q.8/ 4196S.8/4177P.8/4196N.8.
Spearphishing	A more advanced type of phishing attack which is customized to a particular target (e.g., executives, privileged users, etc.).
Threat Actor	A person, group or nation/state/government that carries out or intends to carry out damaging acts against another party. An advanced threat actor shall refer to a person, organized group, or nation/state/government that (a) possesses superior capabilities, resources and skills to launch sophisticated cyber-attacks; or (b) seeks military and/or intelligence information for cyber-espionage purposes.

Section 2. Subsections X177.8 of the MORB and 4177Q.8, 4196S.8 4177P.8, and 4196N.8 of the MORNBFI, are hereby amended to read as follows:

Subsection X177.8/4177Q.8/4196S.8/4177P.8/4196N.8. ***Reporting and notification standards.***

In line with the increased reliance on and adoption of technology by BSFIs, along with growing concerns on cybersecurity, BSFIs should submit regular and event-driven reports covering technology-related information as well as incidence of major cyber-attacks and operational disruptions. This will enable the Bangko Sentral to have an enhanced visibility on the changing IT risk landscape and to proactively ensure that the impact and risks arising from cyber-related incidents and operational disruptions are minimized and contained to avert potential systemic risks to the financial system.

a. Reporting requirement. BSFIs are required to submit to the Bangko Sentral the following reports/information:

(1) Periodic reports. BSFIs shall submit an Annual IT Profile, as listed in *Appendix 6*, electronically to the appropriate supervising department of the Bangko Sentral within twenty-five (25) calendar days from the end of reference year.

(2) Event-driven reports. BSFIs shall notify the Bangko Sentral upon discovery of any of the following:

(a) Reportable Major Cyber-related Incidents. These cover all events which may seriously jeopardize the confidentiality, integrity or availability of critical information, data or systems of BSFIs, including their customers and other stakeholders. Reporting of such incidents to the Bangko Sentral should form part of the incident management plan of BSFIs.

An incident is considered a reportable major cyber-related incident, if after assessing the nature of the incident or attack, the BSFI has determined that the same:

(i) resulted in an unauthorized access and infiltration into the BSFI's internal network (i.e., hacking, advanced persistent threats, presence of malware);
(ii) involved a system-level compromise (i.e., attacks on BSFI's core systems, as opposed to phishing attempts of individual clients);
(iii) affected a significant number of customer accounts simultaneously;
(iv) involved significant data loss or massive data breach;

(v) indicated spearphishing attacks targeting the BSFIs' directors, senior executives, officers, or privileged users;

(vi) resulted in the unavailability of critical systems/services (e.g., Distributed Denial of Service (DDoS) attack resulting in service outage);

(vii) inflicted material financial losses to the BSFIs, their customers and other stakeholders; or

(viii) has been suspected to be perpetrated by an advanced threat actor.

(b) Disruptions of financial services and operations. These include disruption of critical operations which lasts for more than two (2) hours due to internal and external threats, which may be natural, man-made or technical in origin. Such scenarios usually involve loss of personnel, technology, alternate site, and service providers. Causes of such interruptions include, but are not limited to, fire, earthquakes, flood, typhoon, long-term power outage, technical malfunctions, pandemics and other threats.

Security events/attacks which are normally prevented by security systems/devices need not be reported to the Bangko Sentral, except if the same involve significant financial value and/or multitude of customer accounts beyond BSFI's reasonable threshold levels. For instance, an attempt to fraudulently transfer funds involving large sums of money requires immediate notification to the Bangko Sentral as this can be a signal of impending attacks to other BSFIs.

b. Procedure for event-driven reporting. The following procedures shall be followed by BSFIs in reporting reportable major cyber-related incidents and/or disruptions of financial services and operations stated in Item a(2)of this Subsection:

(1) The BSFIs' Compliance Officer and/or BSFI-designated Officer shall notify the appropriate supervising department of the Bangko Sentral within two (2) hours from discovery of the reportable major cyber-related incidents and/or disruptions of financial services and operations stated in Item a(2) of this Sub-section, in accordance with *Appendix 6/Q-3/S-2/P-13/N-1* of the MORB/MORNBFI.

(2) The BSFIs shall disclose, at the minimum, the nature of the incident and the specific system or business function involved.

(3) Within twenty-four (24) hours from the time of the discovery of the reportable major cyber-related incident and/or disruption, a follow-up report should be sent to the appropriate supervising department of the Bangko Sentral through e-mail indicating the following, as applicable:

(a) nature of the incident;
(b) manner and time of initial detection;
(c) impact of the incident based on initial assessment (e.g., length of downtime, number of affected customers/accounts, number of complaints received, value of transactions involved);
(d) initial response or actions taken/to be taken (e.g., conduct of root cause analysis) with respect to the incident; and
(e) information if the incident resulted in activation of the Business Continuity Plan (BCP) and/or Crisis Management Plan (CMP).

c. Verification of root cause. Depending on the nature and severity of the reported incident/disruption, the Bangko Sentral may require BSFIs to provide additional information or updates until the matter is satisfactorily resolved. Likewise, the Bangko Sentral may conduct special examination or overseeing inspection, if necessary, to verify root cause of the incident, assess the impact to the BSFI and the financial system as a whole, identify areas for improvement to prevent recurrence of the incident, and promote enterprise and industry-wide operational resilience.

d. Compliance with reporting of crimes and losses. Compliance with event-driven report requirement shall not excuse BSFIs from complying with the existing rules on the reporting of crimes and losses under Subsection X192.4 of the MORB and *Appendix Q-3-c/S-2-a* of the MORBNBFI. Likewise, any cyber-related incident which does not qualify as a reportable major cyber-related incident and other disruptions arising from crimes and losses must be reported to the Bangko Sentral in accordance with the aforesaid regulations. Operational risk events which are covered under Item a(2) on the event-driven reporting and notification requirements shall no longer require separate reporting and notification pursuant to Subsection X179.10/4179Q.10/4198N.10 of the MORB/MORNBFI.

e. Information gathering. Should the conduct of in-depth studies and research on certain technology development or key area of concern relating to technology risk and cybersecurity be warranted, the Bangko Sentral, from time to time, may request BSFIs to submit specific data and information thereon through surveys, questionnaires or other means.

Section 3. Subsections X177.9 of the MORB and 4177Q.9, 4196S.9, 4177P.9, and 4196N.9 of the MORNBFI, are hereby amended to add the following penalty provisions:

Subsection X177.9/4177Q.9/4196S.9/4177P.9/4196N.9. ***Sanctions and penalties.*** Xxx

a. Non-compliance with the requirements in Item b of Subsection X177.8/4177Q.8/4196S.8/4177P.8/4196N.8 of the MORB/MORNBFI will be

subject to "High" penalty level monetary sanctions pursuant to Subsection X902.1/4902Q.1/4601S.1/4196N.9 of the MORB/MORNBFI. Consistent with Section X009/4009Q of the MORB/ MORNBFI, the Bangko Sentral may deploy applicable enforcement actions on the BSFI and/or its directors, officers, and/or employees for violations on this requirement.

b. Annual IT Profile and other periodic reports which have been considered as erroneous, delayed or unsubmitted shall be subject to the penalties for *Category B* reports under Subsection X184.3.

Section 4. Item d of Subsection X192.4 of the MORB is hereby amended as follows:

The following guidelines shall be observed in the preparation and submission of the report:

(1) The Branch or Head Office unit's Report on Crimes and Losses (RCL), as listed in Appendix 6, shall be submitted electronically to the appropriate supervising department of the Bangko Sentral within ten (10) calendar days from knowledge of the crime/incident.

(2) The RCL shall be submitted through the bank's head office unit and shall be certified correct by the compliance officer.

(3) Where a thorough investigation and evaluation of facts is necessary to complete the report, an initial report electronically submitted within the said deadline of ten (10) calendar days may be accepted: *Provided,* That a complete report is electronically submitted not later than twenty (20) calendar days from the termination of the investigation.

Moreover, an RCL considered as erroneous/ delayed/ erroneous and delayed/unsubmitted shall be subject to the penalties for *Category B* reports under Subsec. X184.3 but will not form part of the computation of demerit points of BSFIs for purposes of determining habituality.

Section 5. Subsections 4177Q.7/4196N.7, 4196S.7 and 4177P.7 of the MORNBFI are hereby amended as follows:

"xxx The guidelines on EMV Implementation are shown in *Appendix Q75/N-17/S-13/P-16* of the MORNBFI. The guidelines on EMV Card Fraud Liability Shift Framework (ECFLSF) are in *Appendix Q76/N-18/S-14 and P-17* of the MORNBFI. Detailed guidelines/standards on Electronic Products and Services xxx"

Section 6. Appendix 6/Q-3/S-2/P-13/N-1 of the MORB/MORNBFI, is hereby amended to include the following:

Category	Form No.	MOR Ref.	Report Title	Frequency	Submission Deadline	Submission Procedure/email Address
B	Unnumbered	Subsection X177.8/4177Q.8/4196S.8/4177P.8/4196N.8.	Reportable Major Cyber-Related Incidents	As incidents occur	Within two (2) hours upon discovery Within twenty-four (24) hours from discovery	citsg@bsp.gov.ph [1] citsg@bsp.gov.ph
B	Unnumbered	Subsection X177.8/4177Q.8/4196S.8/4177P.8/4196N.8.	Disruptions of financial services and operations.	As disruptions occur	Within two (2) hours upon discovery Within twenty-four (24) hours from discovery	citsg@bsp.gov.ph citsg@bsp.gov.ph

[1] For speedy identification, the email transmission should use the following required format as the subject:

<EDRN>underscore<eventtype>underscore<bank/NBQB name>underscore<reportstatus>underscore<yyyymmdd>.

EDRN refers to event driven reporting and notification. The event type will either be "**Cyber**" for major cyber-related reportable incidents or "**Disruption**" for disruptions of financial services and operations. The report status refer to either "**IM-Notice**", for the immediate notification upon discovery of the incident or "**Follow2**" for the follow-up report indicating the details as prescribed in the preceding section, e.g.,:

To: citsg@bsp.gov.ph
Subject: EDRN_Cyber_Bank A_IM-Notice_20180731

Section 7. The guidelines in the electronic submission and preparation of the Annual IT Profile Report and Report on Crimes and Losses are shown in Annexes A and B of this Circular, respectively.

Section 8. Effectivity. This circular shall take effect fifteen (15) calendar days after its publication either in the Official Gazette or in a newspaper of general circulation in the Philippines.

FOR THE MONETARY BOARD:

NESTOR A. ESPENILLA, JR.
Governor

31 October 2018

GUIDELINES ON EUROPAY, MASTERCARD AND VISA (EMV) IMPLEMENTATION
(Appendix to Subsection 4177Q.7/4196N.7/4196S.7/4177P.7)

A. Background

In response to the increasing sophistication of frauds perpetrated through magnetic stripe (magstripe), international payment networks have orchestrated the shift towards EMV chip-enabled card. The EMV is an interoperability standard for chip-bearing smart card technology defined by EMVCo in 1994, adoption of which has resulted to significant reduction in card frauds due to skimming[1] and counterfeiting.

To outpace and manage fraudsters' shift towards jurisdictions that are still using magstripe, Bangko Sentral supervised financial institutions (BSFIs) via Circular No. 808 dated 22 August 2013 were required to migrate their entire payment network to the more secure EMV chip-enabled cards.

B. Statement of Policy

It is the policy of the BSP to foster the development of safe, secure, efficient, and reliable retail payment systems, protect the integrity and confidentiality of customer accounts and information and uphold consumer protection.

C. Scope

These guidelines shall govern the migration to and implementation of EMV of all BSFIs with debit card issuing and acquiring functions. For credit card, only cash advance transaction at Automated Teller Machines (ATMs) shall be covered since other credit card transactions are governed by the rules of the international payment networks.

It is incumbent upon all affected BSFIs to ensure that other key players in the domestic payment network comply with these guidelines.

For purposes of the subject guidelines, payment transactions covered are limited to card present and contact transactions in ATMs, POS terminals and other similar devices. Guidelines governing card-not-present as well as contactless transactions shall be issued separately.

D. Definition of Terms

1. *EMV*, which stands for Europay, MasterCard and Visa, is a global standard for credit, debit and prepaid payment cards based on chip card technology. EMV chip-based payment cards, also known as smart cards, contain an embedded microprocessor, a type of small computer. The microprocessor chip contains the information needed to use the card for payment, and is protected by various security features. Chip cards are a more secure alternative to traditional magstripe payment cards.

[1] Skimming is the illegal copying of information from the magnetic stripe of a payment card to gain access to accounts.

Implementing EMV shall address the deficiencies inherent in magstripe by reducing fraud arising from counterfeit, lost and stolen card information through the following features:

a. Authentication of the chip card to ensure that the card is genuine so as to protect against counterfeit fraud for online-authorized transactions;
b. Digitally signing payment data for transaction integrity;
c. More robust cardholder verification to protect against lost and stolen card fraud for EMV transactions in all acceptance environments.

2. *Acquiring institution (acquirer)* is a bank or financial institution that processes credit or debit card transactions via ATM or POS terminals.

3. *Bangko Sentral Supervised Financial Institutions (BSFIs)* include banks, non-banks with quasi-banking function (NBQB), non-bank electronic money issuers and other non-bank institutions which under existing BSP rules and regulations and special laws are subject to BSP supervision and/or regulation.

4. *Co-branded cards* are Philippine-issued cards affiliated with international payment networks.

5. *Debit cards* are payment cards linked to bank deposit or prepaid/electronic money (e-money) accounts.

6. *Domestic payment network* includes BSFIs as well as other key players such as merchants, providers of ATMs, point-of-sale (POS) terminals and similar devices, card vendors, card personalization bureaus and domestic switches responsible for processing and handling domestic transactions.

7. *Domestic switches* refer to BancNet and Megalink.

8. *EMV chip liability shift* means that the liability and responsibility for counterfeit or fraudulent transaction shall shift to the BSFI who is not EMV-compliant.

9. *EMVCo* is the governing body that manages the EMV specification.

10. *Hybrid cards* are payment cards that have both EMV chip and magstripe.

11. *International payment networks* refer to the payment networks that have global establishment. For purposes of subject guidelines, recognized international networks shall refer to Visa, Mastercard, UnionPay, Diners/Discover, American Express, Japan Credit Bureau (JCB).

12. *Interoperability* refers to the ability of Philippine cardholders to transact at Philippine ATM and POS terminals, regardless of network affiliation or branding of the card.

13. *Issuing institution (issuer)* is a bank or non-bank financial institution that issues payment cards, whether proprietary or co-branded, to consumers.

14. *Payment cards* are cards that can be used by cardholders and accepted by terminals to withdraw cash and/or make payment for purchase of goods or services, fund

transfer and other financial transactions. Typically, payment cards are electronically-linked deposit, prepaid or loan/credit accounts.

15. *Philippine domestic EMV specification* refers to the specification or standards based on EMV that shall be adopted in the Philippine financial market for the proprietary or non-co-branded cards.

16. *Proprietary cards* are Philippine-issued cards without international payment network affiliation.

17. *Technical fallback* is a state in which a chip cannot be used and another type of entry, such as magstripe, is used to complete a transaction.

E. General Rules

In line with the declaration of policy, BSFIs, in migrating to EMV, shall consider the following:

1. BSFIs shall maintain interoperability of the domestic payment network;
2. The Philippine EMV Implementation shall use established EMV specification as follows:
   a. Issuers of proprietary cards shall use the Philippine domestic EMV specification; and
   b. Issuers of co-branded cards shall use the EMV specification of their affiliated international payment network.
3. At a minimum, all debit accepting devices shall acquire/accept Philippine issued proprietary cards using the Philippine domestic EMV specification of members/participants of the domestic switches;
4. The domestic payment network shall ensure continued interoperability and acceptance of Philippine EMV issued cards using the Philippine domestic EMV specification on Philippine EMV deployed acceptance devices;[2] and
5. BSFIs shall strengthen consumer protection by adequately handling and containing consumer concerns and complaints arising from fraudulent schemes done electronically.

F. The Philippine Domestic EMV Specification

With the main objectives of maintaining interoperability and reducing card fraud, BSFIs shall adopt a Philippine domestic EMV specification for proprietary cards. The domestic EMV specification should:

- Adopt the EMV specification according to EMVCo;
- Apply to ATM and domestic debit POS transactions;
- Support contact transactions;
- Support online card authentication to ensure that transactions are made using a valid card;

[2] Include EMV-compliant ATMs, POS terminals and other similar devices.

- Support online authorization to enable issuer to manage fraud and credit risk at the transaction level;
- Support online PIN cardholder verification method;
- Support technical fallback to magstripe in the interim, as provided in Section I of these guidelines, without prejudice to the issuer's decision to process/approve fallback transactions.

G. Minimum Operational Requirements

1. Issuing institutions shall:

   a. Ensure that they have the technical systems and network necessary to process and handle EMV transactions;
   b. Support EMV data elements in authorization messages;
   c. Define chip cards feature, functionality and interface capability;
   d. Enhance risk management systems to leverage chip;
   e. Determine the card migration strategy;
   f. Update customer support and operational systems to support chip cards;
   g. Be certified for network interfaces and card personalization by a certification body organized by BSFIs pursuant to these guidelines;
   h. Replace card base; and
   i. Educate the consumers.

2. Acquiring institutions shall:

   a. Ensure that card-accepting devices are EMV-certified to support the acquiring and routing of Philippine-issued debit cards using the Philippine domestic EMV specification;
   b. Ensure that PIN-entry devices are Payment Card Industry PIN Transaction Security (PCI-PTS)[3] compliant; and
   c. Enable a debit POS environment that supports online PIN for Philippine-issued debit cards.

3. Domestic switches shall:

   a. Establish infrastructure and systems that are EMV-compliant and able to support switched EMV transactions from domestic interconnected networks;
   b. Ensure continued support to existing transaction sets and functions provided to consumers;
   c. Enhance efforts to educate their members on EMV collaboration and seek effective alignment of strategy and design principles; and
   d. Ensure continued ability to support, in the interim, transactions in magstripe format subject to liability shift policies acceptable to BSP, the standards of which shall be covered in subsequent guidelines.

---

[3] A security requirement of the Payment Card Industry (PCI) regarding testing of PIN-entry devices using predefined standards to get certification.

H. Detailed Guidelines, Policies and Processes

BSFIs shall agree on and implement detailed technical and operational requirements, policies and procedures that are acceptable to the BSP, the standards of which shall be covered in subsequent guidelines, and aligned with subject EMV Implementation Guidelines, covering but not limited to the following:

1. Philippine Application Identifier (AID);
2. Single Common AID, Single Common Card Personalization Profile and Single Common Terminal Configuration for domestic transactions;
3. Transaction routing;
4. Testing and certification
5. Dispute and fraud risk management; and
6. Other processes affected by the EMV migration.

I. Hybrid Card, Fallback Function and EMV Liability Shift

While the EMV infrastructure and environment are in the process of achieving full stability, hybrid cards may still be acceptable as a fallback option in cases when the EMV chip or terminal is unable to process domestic chip transactions. In this regard, BSFIs shall formulate a liability shift framework that is acceptable to the BSP.

J. Updated EMV Migration Plan

Any changes arising from the aforementioned guidelines shall be incorporated in the EMV Migration Plan and all affected BSFIs shall resubmit their updated plan to BSP's Core Information Technology Specialist Group (CITSG) within sixty (60) calendar days from the date of the Circular.

All BSFIs shall support migration to EMV standards. Consequently, all cards issued and card-accepting devices should be EMV-compliant.

EMV CARD FRAUD LIABILITY SHIFT FRAMEWORK (ECFLSF)

I. Introduction

This document outlines the Bangko Sentral's guidelines implementing the EMV Card Fraud Liability Shift Framework (ECFLSF). Pursuant to Subsection X177.7 and Appendix 108 of the Manual of Regulations for Banks (MORB), Bangko Sentral Supervised Financial Institutions (BSFIs) should shift from the magnetic stripe (magstripe) technology to EMV-compliant cards, POS terminals and ATMs. The immediate impact and benefit on the adoption of EMV technology is the reduction in card fraud resulting from counterfeit or skimming attacks.

While migration efforts to shift to EMV technology are ongoing, the use of magstripe in payment cards and/or card-accepting devices shall be allowed subject to card fraud liability shift. This means that the BSFIs which have not yet or have partially adopted the EMV technology shall be held responsible for losses associated with the use of a counterfeit card in a card-present environment.

II. Statement of Policy

It is the policy of the Bangko Sentral to foster the development of safe, secure, efficient and reliable retail payment systems, protect the integrity and confidentiality of customer accounts and information and uphold consumer protection.

Towards this end, the Bangko Sentral requires all concerned BSFIs to migrate to a more secure payment technology and sets forth subject principles for allocation of card fraud liability with the aim of ensuring compliance of the different retail payment system participants with the Bangko Sentral's EMV migration requirement. Pending full migration to the EMV technology, the ECFLSF shall likewise accelerate the dispute resolution and restitution process for customers who have valid claims arising from counterfeit fraud or skimming attacks.

III. Applicability and Scope

These guidelines shall apply to all BSFIs with debit and credit card issuing and acquiring functions and shall govern the allocation of liability associated with fraudulent transactions arising from counterfeit cards beginning 1 January 2017, subject to the conduct of proper investigation by the concerned participant/s of the payment card network. The coverage shall be limited to **card-present** and **contact transactions** of Philippine-issued payment cards used domestically in automated teller machines (ATMs), point-of-sale (POS) terminals, and other similar devices routed to either domestic or international payment networks.

Consequently, the ECFLSF shall not apply to card-not-present and contactless transactions. Furthermore, foreign-issued payment cards used domestically and Philippine-issued payment cards used abroad shall not be covered as these are already subject to the existing liability shift and chargeback rules of the international payment networks.

IV. Definition of Terms

For purposes of these guidelines, the following definitions shall apply:

1) *Acquiring institution (Acquirer)*, is a bank or non-financial institution that processes credit or debit card transactions via ATMs, POS terminals, and other similar devices.
2) *EMV compliant device or terminal* is a device or terminal that has, or is connected to, a contact chip card reader, has an EMV application, certified, and is able to process EMV transactions.
3) *Co-branded cards* are Philippine-issued cards affiliated with international payment networks.
4) *Counterfeit card* is an imitation or falsification of a genuine magstripe card or EMV chip card with track data copied from a hybrid EMV card.
5) *Debit cards* are payment cards linked to bank deposit or prepaid/electronic money (e-money) accounts.
6) *Fallback to magstripe transaction* occurs when the chip on the card is not being read by a terminal. This is similar to *technical fallback*, which is defined in Appendix 108 of the MORB as a state in which the chip cannot be used and another type of entry, such as magstripe, is used to complete a transaction.
7) *Hybrid cards* are payment cards that have both EMV chip and magstripe.
8) *International payment networks* refer to the payment networks that have global establishment. For purposes of subject guidelines, recognized international networks shall refer to Visa, Mastercard, UnionPay, Diners/Discover, American Express, Japan Credit Bureau (JCB).
9) *Issuing institution (Issuer)* is a bank or non-bank financial institution that issues payment cards, whether proprietary or co-branded, to consumers.
10) *Payment cards* are cards that can be used by cardholders and accepted by terminals to withdraw cash and/or make payment for purchase of goods or services, fund transfer and other financial transactions. Typically, payment cards are electronically-linked to deposit, prepaid or loan/credit accounts.

V. Guiding Principles

1) The adoption of EMV technology is designed to reduce and mitigate risks arising from counterfeit card fraud. While it remains virtually impossible to create a counterfeit EMV card that can be used to conduct an EMV payment transaction successfully, the presence of magstripe in a hybrid EMV card makes it still vulnerable to counterfeit attacks.

2) A BSFI that has enabled the most secure EMV options shall be protected from financial liability arising from losses on counterfeit card fraud. The liability for this type of fraud shall shift to the BSFI which is not or is partially compliant with the EMV migration requirement.

3) To resolve the issue on the allocation of card fraud liability using the guidelines described herein, the involved parties (such as issuer, acquirer, and payment network) should, first, characterize the fraud committed, and then, assess the technology being employed, in light of the applicable payment network rules. The

party supporting EMV technology will prevail and in case of a technology-tie (neither or both parties are EMV compliant), the liability for fraudulent transactions generally remains with the Issuer.

VI. Allocation of Card Fraud Liability

The allocation of liability for counterfeit card fraud is summarized in the following table:

	Card Capabilities	Acceptance Device Support	Scenario	Liability
1	Magnetic stripe only	Magnetic stripe only	Magnetic card transaction was completed	Issuer
2	Magnetic stripe only	EMV compliant	Magnetic card transaction was completed	Issuer
3	EMV compliant hybrid card	Magnetic stripe only	Magnetic card transaction was completed	Acquirer[1]
4	EMV compliant hybrid card	EMV compliant	Fallback transaction; Magnetic card transaction was completed	Issuer

The information provided above shall be considered as a general guide as each fraudulent transaction shall be separately investigated on. Likewise, the domestic and international payment networks may come up with other scenarios and probable conditions that illustrate how liability is assigned on counterfeit card fraud using different combinations of card and acceptance device capabilities. However, the resolution of such scenarios/conditions should follow the principles espoused in these guidelines.

VII. Consumer Protection and Complaints Handling and Resolution

1) The participants in the domestic payment network (such as issuer, acquirer, and payment network) should collaborate and devise detailed rules and procedures including arbitration mechanisms to operationalize the ECFLSF. Accordingly, a body responsible for strictly implementing the above-mentioned detailed rules and procedures on ECFLSF should be constituted.

2) Cardholders' complaints and/or requests for chargeback as a result of counterfeit card shall be considered as complex complaint/request defined in Appendix 110 of the MORB and hence, shall follow the standards provided in such regulations, except for the processing and resolution timeline which should be within 10 days instead of 45 days.

3) Issuers and Acquirers should ensure that affiliated international payment networks align their existing liability and chargeback rules with the ECFLSF insofar as Philippine-issued payment cards used in the domestic payment environment are concerned.

---

[1] When an Acquirer accepts a magstripe card that was counterfeited with track data copied from an EMV compliant hybrid card and the counterfeit card is used at a device/terminal that is not EMV-compliant, resulting in a transaction to be successfully processed, the Acquirer is liable for any chargeback resulting from such fraud.

Guidelines on the Submission of Information Technology (IT) Profile Report

In order to build the baseline information of IT systems of Philippine banks and to risk profile the complexity of IT operations based on technology-related products and services offered, delivery channels, and processes involved, all banks are required to accomplish and submit annually an IT Profile Report as of 31 December of the reference year.

In accordance with Sec. X177 of the Manual of Regulations of Banks (MORB) on Technology Risk Management, the following shall be observed in the submission of the IT Profile Report:

1. The IT Profile reporting template can be accessed at http://www.bsp.gov.ph/frp/templates. Reports shall be submitted on an annual basis within twenty-five (25) calendar days from the end of reference year. (Attached as Annex A is sample format of IT Profile Report.)

2. The IT Profile report shall be submitted electronically to the following e-mail addresses:

E-mail Address	Type of Reporting Institution
sdckb-itprofile@bsp.gov.ph	Universal/Commercial Banks (U/KBs)
sdctb-itprofile@bsp.gov.ph	Thrift Banks (TBs)
sdcrb-itprofile@bsp.gov.ph	Rural/Cooperative Banks (R/CBs)

3. The following format shall be used for the subject of the e-mail: "ITPROFILE <bankname>,<reference period>", e.g.:

To	: sdctb-itprofile@bsp.gov.ph
cc	:
Subject	: ITPROFILE <bankname>, 31 December 20yy

4. The certification, duly notarized and signed by the authorized official of the reporting institution, shall be sent within the prescribed submission deadline to the Director of the BSP Supervisory Data Center (SDC) via facsimile at (632) 708-7554 or 708-7558.

5. Within the same period prescribed in Item 1, institutions which are unable to transmit their IT Profile Report electronically may submit the same report in compact disc (CD), together with the aforementioned certification, through messengerial or postal services. Said report shall be submitted to the following:

   The Director
   Supervisory Data Center
   Bangko Sentral ng Pilipinas
   11th Floor, Multi-Storey Building
   BSP Complex, A. Mabini Street
   Malate, Manila 1004

6. The IT Profile Report template and other relevant attachments are also available upon request at the BSP Supervisory Data Center through the above-mentioned e-mail addressed and/or postal address.

ANNEX B

Guidelines on the Electronic Submission of the Report on Crimes and/or Losses (RCL)

Pursuant to existing regulations prescribing the reporting of cyber related fraud as well as other crime related incidents to the BSP and in line with on-going initiatives of maximizing available Information Technology infrastructure for regulatory reporting, the following guidelines shall be observed in submitting the RCL:

1. Reportable incidents shall be transmitted electronically using the data entry template (DET) prescribed for the updated RCL. The prescribed DET and its supporting Control Prooflist (CP) for the Initial Report and Final Report, respectively, and the User Guide as relevant reference for accomplishing the DET can be downloaded from http://www.bsp.gov.ph/ses/reporting_templates or requested directly from the Supervisory Data Center (SDC). The Control Prooflist for the initial and final RCL need not be notarized.

2. The updated RCL reporting structure and its corresponding DET considered the reportable cyber fraud incidents as well as other incidents required under Subsections X177.8 and X192.4.

3. The DET for the RCL (DET-RCL) together with the corresponding scanned CP in Portable Document Format (PDF) signed by the authorized official of the reporting bank shall be electronically transmitted within the existing deadline prescribed for Initial Report and Final Report, as the case may be, to the following prescribed e-mail addresses:

Type of Institution	E-mail Address
Universal and Commercial Banks	sdckb-rcl@bsp.gov.ph
Thrift Banks	sdctb-rcl@bsp.gov.ph
Rural and Cooperative Banks	sdcrb-rcl@bsp.gov.ph

4. The following format shall be used for the subject of the e-mail:

<report name>space<bank name>space<control no.>space<report status>, e.g.:

To : sdctb-rcl@bsp.gov.ph (example for thrift banks)
Subject: RCL <Bank A> 102016-0001 INITIAL

using the following required format for the filenames:
<reference no.>_<report status>.<file extension>, e.g.:

- RCL_000250_102016-0001_INITIAL.xls and
- RCL_000250_102016-0001_INITIAL.pdf

5. Each email transmission shall correspond to only one (1) DET-RCL file as multiple RCL cases in a single email transmission will be automatically rejected, thus considered unsubmitted. Each DET-RCL transmission shall be accompanied by its corresponding CP as described in item 3. DET-RCL files which are transmitted without the required CP shall be deemed unsubmitted.

6. Hard copy submission of the RCL shall no longer be accepted. Nevertheless, within the same prescribed period, banks that are unable to transmit electronically may submit their DET-RCL and its accompanying CP in compact discs (CD) through messengerial or postal services. The DET-RCL and its accompanying CP shall be submitted to:

The Director
Supervisory Data Center (SDC)
Bangko Sentral ng Pilipinas
11th Floor, Multi-Storey Building
BSP Complex, A. Mabini Street
Malate, Manila 1004

7. Report submissions that do not conform to the above prescribed procedures shall not be accepted and will be considered non-compliant with the BSP reporting standards as provided under Section X184. It likewise follows that only files prescribed by the BSP for the RCL shall be accepted as compliant with the existing reportorial requirements subject to validation and applicable penalties for erroneous, delayed, or unsubmitted reporting.