EMV CARD FRAUD LIABILITY SHIFT FRAMEWORK (ECFLSF)

(Appendix to Section 148 on IT Risk Management Systems)

I. Introduction

This document outlines the Bangko Sentral's guidelines implementing the EMV Card Fraud Liability Shift Framework (ECFLSF). Pursuant to Sec. 148 and *Appendix 112*, BSFIs should shift from the magnetic stripe (magstripe) technology to EMV-compliant cards, point- of-sale (POS) terminals and automated teller machines (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 01 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 ATMs, 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:

a. *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.

b. *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.

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

d. *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.

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

f. *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 112* as a state in which the chip cannot be used and another type of entry, such as magstripe, is used to complete a transaction.

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

h. *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).

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

j. *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

a. 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.

b. 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.

c. 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 complted	Issuer

The information provided above shall be considered as a general guide as each fraudalent 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

a. 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.

b. Cardholders' complaints and/or requests for chargeback as a result of counterfeit card shall be considered as complex complaint/request defined in Appendix 115 and hence, shall follow the standards provided in such regulations, except for the processing and resolution timeline which should be within ten (10) days instead of forty five (45) days.

c. 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.

(Circular No. 936 dated 28 December 2016)

Footnotes

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.