BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE GOVERNOR

CIRCULAR NO. 958
Series of 2017

Subject: **Amendments to Items 4.1.2 to 4.2.4 of Appendices 75f and Q-59f of the Manual of Regulations for Banks (MORB) and Manual of Regulations for Non-Bank Financial Institutions (MORNBFI), as well as to Subsection X177.9 of MORB and Subsections 4177Q.9, 4196S.9, 4193P.9 and 4196N.9 of MORNBFI– Authentication Controls**

The Monetary Board, in its Resolution No. 553 dated 30 March 2017, approved the following: 1) amendments to Item 4.1.2 Authentication of Appendices 75f and Q-59f of the Manual of Regulations for Banks (MORB) and Manual of Regulations for Non-Bank Financial Institutions (MORNBFI), respectively; 2) deletions of second paragraph in Item 4.1.6 Application Security, Item 4.1.8 Controls Over Fund Transfers, and Item 4.2.1 Administration of E-Services Accounts, of Appendices 75f and Q-59f of the MORB and MORNBFI, respectively; 3) Renumbering of Items 4.1.9 to 4.1.11 and Items 4.2.2 to 4.2.4 of Appendices 75f and Q-59f of the MORB and MORNBFI, respectively; and 4) amendments to Subsection X177.9 of the MORB, and Subsections 4177Q.9, 4196S.9, 4193P.9 and 4196N.9 of the MORNBFI. This is in response to the increasing propensity and sophistication of cyber-attacks involving fund transfers, payments, and other transactions via online channels. These amendments align existing regulations, to the extent possible, with leading standards and recognized principles on customer authentication.

Section 1. Items 4.1.2 to 4.2.4 of Appendices 75f and Q-59f of the MORB and MORNBFI, respectively, shall be amended to read as follows:

"4.1.2 ***Authentication.*** The BSFI should use reliable and appropriate authentication methods to validate and verify the identity and authorization of customers. Authentication is facilitated by the use of factors, which are generally classified into three basic groups:

a. Knowledge - Something the user knows (e.g., username, password, mobile PIN, card number, account number);
b. Possession - Something the user has (e.g., payment card, token, one-time password); and
c. Inherence - Something the user is (e.g., biometrics).

"As the number of factors increases, the window of compromise becomes more difficult. The use of single factor authentication alone is considered inadequate to address the risks inherent in sensitive communications and/or high-risk transactions. Thus, BSFIs should adopt multi-factor authentication (MFA) or use a minimum of two (2) factors in such instances. This requirement shall apply to online transactions where the

risk of compromise is heightened. Sensitive communications and/or high-risk transactions requiring MFA include, among others, the following:

a. Enrollment in transactional e-services;
b. Payments and transfers to third parties;
c. Online remittance, including those for pick-up at the BSFI branches or via door-to-door delivery;
d. Account maintenance, including change in account information and contact details; and
e. Use of payment cards (e.g., ATM, credit and debit cards) in e-commerce websites.

"For transactions that do not require real-time or near real-time authentication/authorization, BSFIs may also opt to use positive confirmation in lieu of MFA. Positive confirmation refers to any form of communication that will enable the BSFI to timely and accurately verify the identity of the requesting customer. The BSFI should use a different communication channel other than the one where the request originated from when confirming sensitive communications and/or high-risk transactions.

"The adoption of MFA techniques or positive confirmations for sensitive communications and/or high-risk transactions can increase customer confidence in e-services. In addition, it provides an opportunity for the customers to assist the BSFI in preventing and detecting fraudulent activity. Nevertheless, alternative and less stringent authentication procedures may be considered for the following:

a. Small-value payments or other low-risk transactions, provided the same are justified by a *transaction risk analysis*[1] and bounded by prudent thresholds established by the BSFI. The BSFI's methodology for setting the threshold should be adequately documented and independently validated at least annually;
b. Payments and transfers made to pre-enrolled merchants in the bills payment facility and those pre-registered recipients by the customer: *Provided,* That the BSFI employs a robust and reliable enrollment process for third party merchants and recipients; and
c. Transactions between two (2) accounts of the same customer at the same BSFI.

"As authentication methods continue to evolve, the BSFI should monitor, evaluate, and adopt sound industry practices to address current and changing risk factors. The authentication process should be consistent with and support the BSFI's overall security and risk management programs. An effective authentication process should have customer acceptance, reliable performance, scalability to accommodate growth and interoperability with existing systems and future plans as well as appropriate policies, procedures, and controls."

---

[1] *Transaction risk analysis* refers to the evaluation of risk related to a specific transaction taking into account various criteria including, but not limited to, customer behavioral transaction pattern, payee profile, nature of product/service to be acquired and transaction value.

"4.1.3 ***Non-Repudiation***[2]. x x x

"4.1.4 ***Authorization Controls and Access Privileges.*** x x x

"4.1.5 ***Confidentiality and Integrity of Information, Transactions and Records.*** x x x

"4.1.6. **Application Security.** The BSFI should ensure an appropriate x x x

Comprehensive and effective x x x

"4.1.7. ***Infrastructure and Security Monitoring.*** x x x

"4.1.8 ***Audit Trail.*** x x x

"4.1.9 ***Segregation of Duties.*** x x x

"4.1.10 ***Website Information and Maintenance.*** x x x

4.2 **Administrative and Management Controls**

"4.2.1 ***Service Availability and Business Continuity.*** x x x

"4.2.2 ***Incident Response and Management.*** x x x

"4.2.3 ***Outsourcing Management.*** x x x"

Section 2. All references to BSI in the following sections shall be changed to BSFI:

a. Section X177 and its subsections and the related appendices of the MORB; and
b. Sections 4177Q, 4196S, 4193P, and 4196N and their subsections and the related appendices of the MORNBFI.

Section 3. Subsection X177.9 of the MORB shall be amended to read as follows:

Subsection X177.9. *Sanctions and Penalties.* BSFIs should make available all policies and procedures and other documents/requirements related to the foregoing during on-site examination as well as provide copies thereof to the Bangko Sentral when a written request is made to determine their compliance with this Section.

Consistent with Sec. X009, the Bangko Sentral may deploy enforcement actions to promote adherence with the requirements set forth in Sec. X177 and its subsections and bring about timely corrective actions. Any violation of the provisions of this Section,

[2] Non-repudiation is a means of ensuring that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

its appendices and annexes, shall subject the BSFI and/or its directors, officers, and/or employees to the monetary and non-monetary sanctions, as provided under existing laws, Bangko Sentral rules and regulations. Enforcement actions shall be imposed on the basis of the overall assessment of BSFI's ITRMS. Whenever a BSFI's ITRMS is rated "1" pursuant to Subsection X177.4, the following additional sanctions may be imposed:

a. Suspension/revocation of authority to provide electronic products and services; and
b. Prohibition against offering/provision of new electronic products and services.

On the EMV migration requirement, BSFIs should endeavor to achieve full compliance within a period as may be allowed by the Bangko Sentral. Prior to full compliance, failure on the part of BSFIs to submit and implement their EMV migration plan shall be subject to additional enforcement actions pursuant to Section X009. On the requirement to adopt multi-factor authentication techniques for sensitive communications and/or high risk transactions pursuant to Item 4.1.2 of *Appendix 75f*, the Bangko Sentral may issue directives to improve authentication and authorization procedures for sensitive communications and/or high risk transactions, or impose sanctions to limit the level of or suspend any electronic products and services that are not compliant with such requirements.

Section 4. Subsections 4177Q.9/4196S.9/4193P.9/4196N.9 of the MORNBFI shall be amended to read as follows:

Subsection 4177Q.9/4196S.9/4193P.9/4196N.9. *Sanctions and Penalties.* BSFIs should make available all policies and procedures and other documents/requirements related to the foregoing during on-site examination as well as provide copies thereof to the Bangko Sentral when a written request is made to determine their compliance with this Section.

Consistent with Sec. 4009Q, the Bangko Sentral may deploy enforcement actions to promote adherence with the requirements set forth in Sec. 4177Q/4196S/4193P/4196N and bring about timely corrective actions. Any violation of the provisions of this Section, its appendices and annexes, shall subject the BSFI and/or its directors, officers, and/or employees to the monetary and non-monetary sanctions, as provided under existing laws, Bangko Sentral rules and regulations. Enforcement actions shall be imposed on the basis of the overall assessment of BSFI's ITRMS. Whenever a BSFI's ITRMS is rated "1" pursuant to Subsec. 4177Q.4/4196S.4/4193P.4/4196N.4, the following additional sanctions may be imposed:

a. Suspension/revocation of authority to provide electronic products and services; and
b. Prohibition against offering/provision of new electronic products and services.

On the requirement to adopt multi-factor authentication techniques for sensitive communications and/or high risk transactions pursuant to Item 4.1.2 of *Appendix Q-59f*, the Bangko Sentral may issue directives to improve authentication and authorization procedures for sensitive communications and/or high risk transactions, or impose

sanctions to limit the level of or suspend any electronic products and services that are not compliant with such requirements.

Section 5. ***Transitory Provision.*** The following provision shall be incorporated as a footnote to Item 4.1.2 of Appendices 75f and Q-59f of the MORB and MORNBFI, respectively:

BSFIs shall comply with the foregoing requirements on customer authentication by 30 September 2017. In this regard, a BSFI should be able to show its plan of actions with specific timelines, as well as the status of initiatives being undertaken to fully comply with the provisions of Item 4.1.2 of *Appendices 75f* and *Q-59f* of the MORB and MORNBFI, respectively, upon request of the Bangko Sentral starting May 2017. This transitory period, however, should not excuse BSFIs from immediately complying with the MFA requirements imposed by affiliated payment networks.

Section 6. ***Effectivity.*** This Circular shall take effect fifteen (15) calendar days following its publication in the Official Gazette or in a newspaper of general circulation.

FOR THE MONETARY BOARD:

NESTOR A. ESPENILLA, JR.
Officer-in-Charge

25 April 2017