BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE GOVERNOR

CIRCULAR NO. 1213
Series of 2025

Subject : **Amendments to Regulations on Information Technology Risk Management to Implement Section 6 of the Anti-Financial Account Scamming Act (AFASA)**

The Monetary Board, in its Resolution No. 521 dated 22 May 2025, approved the amendments to Section 148 and Appendix 126 of the Manual of Regulations for Banks (MORB), Sections 147-Q/145-S/142-P/126-N and Appendices Q-79/S-11/P-9/N-15 of the Manual of Regulations for Non-Bank Financial Institutions (MORNBFI), and Section 201, Glossary of Terms, and Appendix 201-1 of the Manual of Regulations for Payment Systems (MORPS), to implement the information technology risk management-related portion of Section 6 of Republic Act (R.A.) No. 12010 or the "Anti-Financial Account Scamming Act (AFASA). These amendments are designed to fortify the existing regulatory framework and ensure more effective compliance with the provisions of the AFASA.

Section 1. Section 148 of the MORB and Sections 147-Q/145-S/126-N of the MORNBFI (IT Risk Management System) on IT controls implementation for electronic products and services shall be amended, as follows:

148/147-Q/145-S/126-N. INFORMATION TECHNOLOGY RISK MANAGEMENT[1]

"xxx

Definition of Terms. xxx

a. *Advanced persistent threat or APT* xxx

b. *Blacklist Screening* shall refer to a process of screening names, transactions and account activities against a database of entities or attributes (e.g. merchants, mobile devices, and IP addresses) flagged as unsecure, fraudulent, or involved in illegal activities.

c. *Bot Detection* shall refer to tools that prevent scripted attacks by identifying when a request or instruction likely originates from an automated program or bot through the analysis of user behavior and network data.

d. *Browser Automation* shall refer to a process of automatically performing operations on a web browser to allow users to automate repetitive or complex tasks such as filling out forms, clicking buttons, navigating web pages, or scraping data.

e. ~~b.~~ *Card skimming* xxx

[1] ~~BSFIs shall comply with the Enhanced Guidelines on Information Security Management within a period of one (1) year from 5 December 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 this Circular, upon request of the Bangko Sentral starting December 2017.~~

~~BSFIs shall comply with the foregoing standards until 31 December 2022. In this regard, BSFIs 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 Circular No. 1140 dated 24 March 2022, upon request of the Bangko Sentral starting 1 September 2022.~~

f. ~~c.~~ *Cloud computing* xxx
g. ~~d.~~ *Compromised state* xxx
h. ~~e.~~ *Cyber-threat* xxx
i. ~~f.~~ *Cybersecurity* xxx
j. ~~g.~~ *Data Breach* xxx
k. ~~h.~~ *Defense-in-depth* xxx

l. *Device Fingerprinting* shall refer to a technique used to identify and track a specific device based on its unique combination of hardware, software, and configuration attributes, among others.

m. ~~i.~~ *Distributed denial of Service (DDoS)* xxx

n. *Emulators* shall refer to software or hardware that allows a computer to perform the functions or execute programs defined for a different type of computer or device.

o. *Fraud Management Systems (FMS)* shall refer to a comprehensive set of automated and real-time monitoring and detection systems to identify and block disputed, suspicious, or other similar online transactions.

p. *Geolocation Monitoring* shall refer to the process of tracking the geographic or physical location of an electronic device used by a customer.

q. ~~j.~~ *Hacking* xxx
r. ~~k.~~ *Information security program (ISP)* xxx
s. ~~l.~~ *Information security strategic plan (ISSP)* xxx
t. ~~m.~~ *Information security risk management (ISRM)* xxx

u. *Jailbroken or Rooted Device* shall refer to a mobile device that has been modified to bypass the built-in restrictions and control or security mechanisms of the operating system, granting the user privileged access to the device's software and functionality.

v. *Kill Switch* shall refer to a facility that allows customers to immediately suspend their account and block outgoing financial transactions and prevent changes to account information.

w. ~~n.~~ *Malware* xxx

x. *Money Lock* shall refer to a security mechanism that allows customers to secure a portion of their funds, rendering it inaccessible for online or digital transactions.

y. ~~o.~~ *Pharming* xxx
z. ~~p.~~ *Phishing* xxx

aa. *Rate Limiting* shall refer to a security measure that restricts the frequency of requests or actions a user or system can perform within a specific timeframe to prevent brute-force attacks and ensure fair use of resources.

bb. ~~q.~~ *Reportable major cyber-related incidents* xxx

cc. *Screen Scraping* shall refer to a technique of extracting data from a website, application, or visual output by capturing and reading the information displayed on the screen.

dd. *Scripts* shall refer to a sequence of instructions, ranging from a simple operating system command to complex programming statements, which can be executed automatically by an interpreter.

ee. ~~r.~~ ***Security operations center (SOC)*** xxx

ff. *Session Management* shall refer to mechanisms for securely handling the creation, maintenance, and termination of user sessions in an information system. This includes processes for authenticating users, assigning session identifiers, monitoring session activity, and ensuring proper session termination to prevent unauthorized access.

gg. ~~s.~~ ***Spear phishing*** xxx
hh. ~~t.~~ ***Threat actor*** xxx
ii. ~~u.~~ ***Threat intelligence*** xxx

jj. *Transaction Velocity Checks* shall refer to a risk-based mechanism that monitors and analyzes the frequency, volume, and pattern of transaction data within predefined intervals to detect anomalies or similarities associated with fraudulent behavior.

kk. *Unsecure Merchants* shall refer to merchants that either do not implement secure industry-standard transaction authentication protocols or have a history of involvement in verified fraudulent financial transactions. This shall also include merchants that have demonstrated inadequate information security practices or have compromised or known vulnerabilities in their systems.

xxx

IT Risk Management System (ITRMS). xxx

c. *IT controls implementation.* xxx

(5) Electronic products and services. xxx

BSFIs should protect customers from fraudulent schemes done electronically. ~~Otherwise,~~ Failing to do so may erode consumer confidence ~~to use~~ in electronic channels as safe, secure, and reliable method~~of making~~s for financial transactions ~~will be eroded~~. To mitigate the impact of cyber fraud, BSFIs should adopt an aggressive security posture, ~~such as the following~~ including the following measures:

(a) xxx;
(b) xxx;
(c) xxx;

(d) Implement automated and real-time fraud monitoring and detection systems to identify and block disputed, suspicious, or fraudulent online transactions. xxx

BSFIs shall regularly assess the risks associated with their products and services to determine the appropriate measures for fraud prevention. BSFIs engaged in complex electronic products and services and handling high aggregate values of online transactions must adopt a robust Fraud Management System (FMS) capable of rapidly detecting, preventing, and

blocking disputed, suspicious, or other fraudulent transactions, including new and evolving fraud schemes.

For purposes of the succeeding provisions, complex electronic products and services shall refer to advanced electronic payment and financial services (EPFS) as defined under Sections 701/701-Q/401-S/114-P/401-N/404-T and high aggregate values of online transactions shall refer to average monthly network value of transactions of at least Seventy-Five Million Pesos (Php 75,000,000.00) for the last six (6) months.

To ensure robustness of their FMS, covered BSFIs shall implement all of the following essential fraud rules and mechanisms:

(i) *Transaction velocity checks or thresholds.* Monitoring the frequency of incoming and outgoing transactions within a specific time frame to detect unusually rapid activity, which may indicate fraudulent behavior. The FMS should be able to detect, and/or block transactions with unusual velocity, such as multiple, similar, simultaneous, or consecutive transactions, including those that might be facilitated through automated bots, malware, zero-day exploits, and other similar means or attack vectors. Additionally, risk-based thresholds or limits for the amount or volume of transactions, based on the risk profile of the consumer, may be imposed to detect and/or block usage outside the customer's normal spending patterns;

(ii) *Mobile device and account information changes.* Monitoring changes on the mobile device and account identifying information such as mobile number and email address, among others, which may indicate account takeover attacks. The FMS should be capable of analyzing subsequent transactions for fraud patterns and temporarily blocking transactions for a certain timeframe once suspicious activities are noted after the change;

(iii) *Geolocation monitoring.* Tracking the geographic location of transaction initiators to identify activities from unexpected locations. The FMS should be capable of stopping transactions outside the usual location or country, or triggering enhanced due diligence procedures, as necessary;

(iv) *Blacklist screening.* Analyzing transactions against databases of unsecure merchants, as well as account activities associated with mobile devices and IP addresses involved in fraudulent transactions. The FMS should include rules to block such transactions to prevent fraud exposure of customers; and

(v) *Behavioral Anomalies.* Detecting deviations from a user's typical behavior, such as spending patterns or login habits, which could indicate unauthorized access. This also includes deviations in collective transactional behavior such as the execution of multiple fund transfers with few or same recipients, or patterns of numerous transactions indicating

concentration to very few recipients with no business purpose.

To strengthen fraud detection and prevention, BSFIs shall leverage a combination of rule-based approaches, machine learning algorithms, and other technologies to adapt to evolving fraud tactics. Likewise, constant calibration of the FMS shall be enforced through continuous data analysis, risk assessments, adaptive rule adjustments, machine learning refinements, regular stress testing, independent review and audits, and proactive monitoring of fraud patterns, among others.

Detection through FMS is one of the grounds for BSFIs to temporarily hold funds subject of a disputed transaction and initiate a coordinated verification process. Moreover, BSFIs shall perform actions necessary to preserve the integrity of financial accounts involved in the disputed transaction. Hence, BSFIs shall establish and enforce clear and comprehensive policies, standards, and procedures on their FMS implementation to cover the following:

(i) Thresholds, parameters, and workflow in the FMS that would trigger the temporary holding of funds;
(ii) Actions to be taken when funds are temporarily held, including additional verification and/or authorization protocols, confirmation procedures, and other investigation procedures to assess veracity of the FMS trigger; and
(iii) Temporary holding of funds subject of a disputed transaction and coordinated verification as required under Sections 7 and 8 of the AFASA, Industry Protocol, and Bangko Sentral issuances implementing the same.

FMS requirement for Clearing Switch Operators (CSOs). CSOs of Automated Clearing Houses (ACHs) shall implement an FMS for monitoring and flagging suspicious and fraudulent transactions. Specifically,the CSOs shall have the necessary technical and operational capabilities to implement an FMS for retail ACH operations to strengthen fraud detection mechanisms within the payments industry.

(e) Financial accounts must be protected with security measures to mitigate risks such as cyberattacks, unauthorized access, and fraudulent transactions. These safeguards for financial accounts must include all of, but are not limited to, the following:

(i) Implementation of a 24-hour Transaction Pause Period (TPP) after applying key account changes, wherein customers will be restricted in performing financial transactions. Key account changes refer to modification in information deemed essential by BSFIs to secure access to a customer’s accounts. This includes, but is not limited to, updates to mobile number, email address, and registered/authenticated device used to access the account. BSFIs may opt to shorten the TPP or implement transaction restrictions/limits during the TPP, provided that strong authentication mechanisms are in place and the BSFI shall be fully accountable for the associated risks;

(ii) Restriction on installing mobile applications on unsecured devices, such as, but not limited to those with outdated systems, rooted or jailbroken devices, or emulators;

(iii) Prohibition of the use of unauthorized scripts or automation tools (e.g., screen scraping, browser automation) to access financial accounts and execute transactions through implementation of the following: behavioral analysis, rate limiting, session management, and bot detection, among others;

(iv) Proper authentication and integrity checks to ensure that transactions initiated from front-end applications accessible to customers are not altered prior to, or during transmission or execution in backend systems;

(v) Adoption of strong device fingerprinting, a technique that collects data about the device being used, along with the implementation of effective mechanisms to prevent spoofing of device identity; and

(vi) Limitation on the use of interceptable authentication mechanism (e.g. One-Time Pins [OTPs] via SMS and email). With the increasing prevalence of social engineering attacks aimed at obtaining login credentials, BSFIs should limit the use of authentication mechanisms that can be shared to, or intercepted by, third parties unrelated to the transaction.

The guidelines on the adoption of multi-factor authentication (MFA) are outlined in Appendix 79/Q-66. Moreover, BSFIs engaged in complex electronic products and services and handling high aggregate values of online transactions must adopt strong authentication mechanisms to ensure the integrity of customer-initiated transactions. These include any of the following:

aa. *Biometric authentication* – provides customer convenience and enhanced security as biometrics can be difficult to replicate or steal. Examples include fingerprint scanning, facial recognition, and voice recognition, among others;

bb. *Behavioral biometrics* – can track behavioral patterns, such as typing speed, mouse, or device movements. This can be implemented as part of continuous authentication and linked to anomaly/fraud detection;

cc. *Passwordless authentication* – eliminates traditional passwords but uses factors like biometrics, hardware tokens and cryptographic keys. An example is the use of Fast Identity Online (FIDO), a technical specification for online user identity authentication, allowing biological features or a FIDO security key to log in to online accounts; or

dd. *Adaptive authentication* – dynamically adjusts authentication process based on user's context, to cover factors such as location, device, and behavior. Upon detection of unusual activity, it can prompt additional verification steps or other actions, depending on risk appetite.

(f) Descriptive customer notification for account activities and financial transactions should enable customers to verify the legitimacy of activities on their accounts. Real-time notification should be sent through secure channels such as mobile apps, messaging apps, email, or SMS.

BSFIs should ensure that customer notifications contain clear and complete information, including the recipient identity (e.g., payee or merchant name or account number), transaction amount and currency, date and time, transaction type, reference number, and device or browser information, as applicable. Further, OTP messages should be personalized with sufficient transaction details. While sensitive information may be redacted, the notification must still allow the customers to accurately identify the transaction. At a minimum, notifications should be sent for withdrawal transactions, fund transfers exceeding a predefined threshold, merchant and bills payments, device registration, new login information or authentication methods, auto-debit arrangements, third party enrollments and fund transfer recipients, and profile updates.

(g) Mechanisms should be established to enable account holders to verify the identity of the recipient of fund transfers, ensuring that transactions are directed to the intended payee. In addition, BSFIs should ensure that off-us transactions adhere to an industry-wide, standardized approach that facilitates the secure and reliable method to exchange information necessary for payee verification. In implementing these controls, the BSFIs should ensure adequate safeguards against possible abuses and maintain continued compliance with relevant rules and regulations under the NRPS framework, as well as those governing secrecy of bank deposits and data privacy.

(h) Customers should be empowered with tools, knowledge, and support to actively protect their financial accounts. Therefore, digital platforms facilitating retail interbank fund transfers and other high-risk transactions, must offer all of the following features and functionalities:

(i) A self-service facility that enables account holders to suspend their account and block outgoing financial transactions, and prevent unauthorized changes to account information when fraud, compromise, or suspicious activities are detected ("kill switch"). The kill switch instructions must be properly authenticated and verified;

(ii) A mechanism to revoke account access or permissions for trusted devices, online merchants, third-party

applications, or electronic products and services. As the financial ecosystem becomes more interconnected, customers can access their accounts through various channels and link them to merchants or third-party applications, enhancing convenience but also increasing security risks. To address these risks, BSFIs should enable customers to manage permissions, allowing them to view, manage, and revoke external access to their financial accounts, thereby strengthening security and reducing potential threats;

(iii) A "money lock" feature that allows account holders to secure a portion of their funds, rendering it inaccessible for online or digital transactions. The locked funds cannot be moved or transferred digitally without first unlocking them, either through in-person verification at BSFI branches or strong authentication mechanisms through digital channels. This feature is designed to limit the customer's exposure to fraud or unauthorized transactions by safeguarding the locked portion of the account balance; and

(iv) Customizable transaction limits that enable account holders to mitigate fraud risks by setting restrictions on the number, value, or type of transactions that may be executed, provided, that these remain within the limits predefined by BSFIs. These limits may include daily transaction cap, maximum transfer amounts, withdrawal limits, online payment restrictions, and cross-border transaction thresholds, among others. To ensure the feature's effectiveness, any changes to transaction limits should require strong authentication and prompt customer notifications.

(i) BSFIs must establish sound controls and processes to prevent unauthorized (1) digital account onboarding; and (2) linking of a financial account to an online account.

(j) BSFIs must collect relevant transaction logs, protect them against unauthorized manipulation, and retain them with adequate back-up for a period of at least five (5) years, unless otherwise required by law or other regulations, or direction from the Bangko Sentral to retain them for a longer period. This ensures a detailed record of account activities that facilitates thorough investigation, coordinated verification, and analysis of fraudulent patterns.

Minimum information that must be captured in the transaction logs includes the following:

(i) Name and account number of sender/s;
(ii) Date and time of transaction/s;
(iii) Transaction amount and currency;
(iv) Name of receiving financial institution/s;
(v) Name and account number of recipient/s;
(vi) Unique transaction reference (e.g. Originating Financial Institution [OFI], CSO, Receiving Financial Institution [RFI] transaction reference);
(vii) Mode of payment instruction (e.g., PesoNet, Instapay, check, ATM transfer);
(viii) Mode of transaction authentication (e.g., device-based authentication, biometric, and password or pin, etc.);

(ix) Non-financial information (e.g., change of password and challenge question);
(x) Transaction channel (e.g., mobile, web, integration with partner etc.); and
(xi) Network, hardware, and software information (e.g. device fingerprint, device details, IP address, and/or browser information).

(k) BSFIs must not send clickable links or quick-response (QR) codes via email, instant messaging apps, or SMS, unless the sending of the link or QR code is prompted by a prior customer action, only provides information, or does not redirect to a website or web application that requires the user to input sensitive information or login credentials.

In addition, a shared accountability framework shall be adopted to strengthen strategies for safeguarding financial accounts. This framework underscores collective responsibility and collaboration among all parties involved in financial transactions – financial institutions, account holders, and third-party entities – thereby playing a critical role in mitigating risks of unauthorized transactions and determining liability for the losses.

(a) BSFIs shall comply with all applicable laws and regulations and ensure that adequate risk management systems and controls are in place, proportionate to the complexity of the electronic products and services offered;

(b) BSFIs should clearly and consistently inform their customers of their responsibilities in maintaining cyber hygiene practices, which include:

(i) Safeguarding digital financial accounts by utilizing and activating the security features provided by BSFIs;
(ii) Reading and understanding the terms and conditions for using the digital platform and actively engaging in the educational and awareness campaigns to help customers familiarize themselves with the platform's security features, understand the risks and common fraud schemes targeting financial consumers, and learn the strategies to mitigate such risks;
(iii) Avoiding disclosure of sensitive account information such as usernames, passwords, PIN codes, OTPs, authenticator code, or any other login credentials;
(iv) Warning against money mule offenses, including lending, or allowing others to use their financial accounts;
(v) Verifying website address, contact information, and mobile applications through official sources; and
(vi) Reporting suspicious, unauthorized, or fraudulent transactions promptly to the respective BSFIs and fully cooperating with the BSFIs' investigation and resolution process.

Further details about the consumer awareness program can be found in Section 4.3.3. and Annex C of Appendix 79/ Appendix Q-66; and

(c) BSFIs should enforce and regularly evaluate that third-party entities/service providers involved in financial transactions strictly adhere to contractual obligations on availability, information security, and cybersecurity, among others. Such

third-party entities/service provider are required to promptly respond and fully cooperate with the BSFIs in cases of fraud and cyber-related incidents. Furthermore, BSFIs should ensure the outsourcing arrangements, including the contract provisions, are compliant with applicable Bangko Sentral rules and regulations on outsourcing and vendor management.

Failure to perform the above duties and responsibilities may subject the BSFIs or third-party entities/service providers to liability for losses arising from fraudulent transactions.

Detailed guidelines/standards on Electronic Products and Services are shown in Appendix 79/Q-66.

d. *Risk measurement and monitoring.* xxx

xxx

Section 2. Appendix 126 of the MORB and Appendices Q-79/S-11/P-9/N-15 of the MORNBFI on National Retail Payment System Framework (NRPS) shall be amended, as follows:

xxx

D. Clearing Switch Operator (CSO)

xxx

1. Key Principles

   a. xxx.
   b. xxx.
   c. xxx.
   d. xxx.
   e. xxx.
   f. xxx.
   g. CSOs of ACHs shall implement a fraud management system (FMS) for monitoring and flagging suspicious and fraudulent transactions. Specifically, the CSOs shall have the necessary technical and operational capabilities to implement an FMS for retail ACH operations to strengthen fraud detection mechanisms within the payments industry.

Section 3. The Glossary of Terms in the MORPS shall include the following:

GLOSSARY OF TERMS

xxx

Fraud Management System (FMS) – refers to a comprehensive set of automated and real-time monitoring and detection systems to identify and block disputed, suspicious, or other similar online transactions, pursuant to Bangko Sentral regulations on information technology risk management.

xxx

Section 4. Section 201 of the MORPS shall be amended, as follows:

NATIONAL RETAIL PAYMENT SYSTEM FRAMEWORK

xxx

201.4 ***Specific rules applicable to transactions performed under the NRPS framework***. The following rules shall apply to retail payment transactions which are cleared and settled in accordance with the NRPS Framework:

a. Minimum requirements to offer Electronic Payment and Financial Service (EPFS). EPFS, which shall require Bangko Sentral approval in accordance with Sections ~~X~~701/~~47010~~ 701-Q/~~4641S~~ 401-S/~~4641P~~ 114-P/~~4641N~~ 401-N of the MORB/MORNBFI and Section 501 of the MORPS, refer to BSFI products and/or services that enable consumers to carry out or initiate payments electronically, financial transactions and other related services through a point of interaction. To offer EPFS, BSFIs shall conform to the following requirements:

   (1) xxx;

   (2) xxx;

   (3) xxx; and

   (4) BSFIs shall conform to Sections ~~X701/47010/4641S/4641P/4641N~~ 148/147-Q/145-S/142-P/126-N and Appendix 79/Q-66 of the MORB/MORNBFI on the IT Risk Management Standards and Guidelines ~~on~~ for electronic banking, electronic payment, electronic money and other electronic products and services ~~provided in Appendix 75f/Q-59f the MORB/MORNBFI~~.

Section 5. Appendix 201-1 of the MORPS on the NRPS Framework shall be amended, as follows:

xxx

~~d.~~D. **Clearing Switch Operator (CSO)**

xxx

~~c.~~ Key Principles
   (1) xxx.
   (2) xxx.
   (3) xxx.
   (4) xxx.
   (5) xxx.
   (6) xxx.
   (7) CSOs of ACHs shall implement a fraud management system (FMS) for monitoring and flagging suspicious and fraudulent transactions. Specifically, the CSOs shall have the necessary technical and operational capabilities to implement an FMS for retail ACH operations to strengthen fraud detection mechanisms within the payments industry.

Section 6. The existing footnote in Section 148/147-Q/145-S/142-P/126-N on the previous transitory provisions are hereby deleted. The following new transitory provision shall be incorporated as footnote to Section 148/147-Q/145-S/126-N as follows:

BSFIs shall comply with the standards provided in this Circular within one (1) year from its effective date.

Section 7. Effectivity Clause. This Circular shall take effect fifteen (15) calendar days following its publication in any newspaper of general circulation.

FOR THE MONETARY BOARD:

Digitally signed by Eli M. Remolona Jr.
Date: 2025.05.30 19:29:27 +08'00'

ELI M. REMOLONA, JR.
Governor