BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE GOVERNOR

CIRCULAR NO. _____
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. ___ dated ___, approved the amendments to Section 148 of the Manual of Regulations for Banks (MORB) and Sections 147-Q/145-S/142-P/126-N of the Manual of Regulations for Non-Bank Financial Institutions (MORNBFI), in furtherance of strengthening the implementation of Republic Act 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 Act.

Section 1. Section 148 of the MORB and Sections 147-Q/145-S/142-P/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/142-P/126-N. INFORMATION TECHNOLOGY RISK MANAGEMENT

"xxx

Definition of Terms. The terms used in the Section are defined as follows:

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

b. *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.

c. *CAPTCHA or Completely Automated Public Turing test to tell Computers and Humans Apart* shall refer to an interactive feature added to web forms to distinguish humans from automated

agents. It requires users to complete tasks that are difficult for automated systems to complete.

d. *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.

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

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

g. *Geolocation Monitoring* shall refer to a method of monitoring the geographic or physical location of an electronic device used by a customer.

h. *Insecure Merchants* shall refer to merchants who either do not implement any of the 3D Secure (3DS) protocols for transaction authentication or have a history of involvement in verified fraudulent financial transactions.

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

j. *Kill Switch* shall refer to a mechanism that allows a customer to immediately suspend their account and block outgoing financial transactions, and prevent changes to account information.

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

l. *Screen Scraping* shall refer to a technique of extracting data from a visual output or website/application's user interface by reading or capturing the information displayed on the screen.

m. *Scripts* shall refer to a sequence of instructions, ranging from a simple list of operating system commands to full-blown programming language statements, which can be executed automatically by an interpreter.

n. *Transaction Velocity Checks* shall refer to a mechanism that monitors the frequency of transaction data elements within certain intervals to look for anomalies or similarities with known fraud behavior.

xxx

5. Electronic products and services. xxx

BSFIs should protect customers from fraudulent schemes done electronically. Failing to do so may erode consumer confidence in electronic channels as safe and reliable methods for financial transactions. To mitigate the impact of cyber fraud, BSFIs should adopt an aggressive security posture, including the following measures:

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

(d) Implement automated and real-time fraud monitoring and detection systems xxx

BSFIs engaged in complex digital products and services, or handling high volumes or high aggregate values of online transactions must adopt a robust Fraud Management System (FMS) capable of rapidly detecting and preventing fraudulent transactions, including new and evolving fraud schemes. BSFIs should regularly assess the risks associated with its products and services to determine the appropriate measures for fraud prevention. To ensure robustness of their FMS, BSFIs may employ any or a combination of rule-based, machine learning, and other technologies.

BSFIs shall also 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, alert, 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, 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 insecure 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.

(v) **Behavioral Anomalies.** Detecting deviations from a user's typical behavior, such as spending patterns or login habits, which could indicate unauthorized access.

Detection through FMS is one of the grounds for BSFIs to temporarily hold funds and initiate a coordinated verification process. Moreover, BSFIs shall perform acts as may be legally warranted to preserve the integrity of the financial account. Hence, BSFIs shall establish and enforce clear and comprehensive policies, standards, and procedures on its FMS implementation to cover the following:

(i) Thresholds and parameters in the FMS which would trigger 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 and coordinated verification as required under Section 7 and 8 of the AFASA and BSP issuances implementing the same.

FMS at the ACH Level. The implementation of an FMS at the Automated Clearing House (ACH) level shall be undertaken as a central point for monitoring and flagging suspicious and

fraudulent transactions at scale, thereby ensuring enhanced security and trust across the entire financial ecosystem. Specifically, the ACH shall engage Clearing Switch Operators (CSOs) with capability to implement an FMS for retail ACH operations to strengthen the fraud prevention mechanisms within the industry.

(e) Financial accounts must be protected with robust security measures aligned with the BSFI's risk profile 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 Hold Period after applying key account changes. 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.

(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: CAPTCHA, 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. 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.

BSFIs engaged in complex digital products and services, or handling high volumes or high aggregate values of online transactions must adopt stronger authentication mechanisms to ensure the integrity of customer-initiated transactions. These include:

a. **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.
b. **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.
c. **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.
d. **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.
e. **AI and machine learning** – can be integrated into MFA solutions to analyze vast amounts of data (e.g. digital footprints) to identify patterns and anomalies in a more proactive manner.

(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 “kill switch” or a self-service facility that enables account holders to suspend their account and block outgoing financial transactions, and prevent changes to account information when fraud, compromise, or suspicious activities are detected. The request to suspend the account must be properly authenticated and verified to ensure that only legitimate requests are processed.

(ii) A stop payment feature designed to cancel batch electronic fund transfers identified as fraudulent.

(iii) A mechanism to revoke account access or permissions for trusted devices, online merchants, third-party applications, or digital financial services. As the financial ecosystem becomes increasingly interconnected, customers can access their accounts through various channels and link them to merchants or third-party applications for seamless transactions.

While this enhances convenience, it also introduces security risks, as threat actors may exploit vulnerabilities in these connections to gain unauthorized access. To mitigate these risks, BSFIs must empower customers with a facility to manage permissions. This facility should allow users to view, manage, and revoke external access or permissions granted to their financial accounts as needed, thereby strengthening security, and minimizing exposure to potential threats.

(iv) 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.

(v) 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 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. OFI, CSO, 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.)
(xi) Network, hardware, and software information (e.g. device fingerprint, device details, IP address, and/or browser information)

(j) BSFIs must not send clickable links or QR codes via email, instant messaging apps, or SMS, unless the link or QR code is anticipated by the customer, provides only information, and does not redirect to a website or web application that requires the 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 robust risk management systems and controls are in place, proportionate to the complexity of the digital 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.
(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 Annex C of Appendix 79 of the MORB and Appendix Q-66 of the MORNBFI.

(c) BSFIs should enforce and regularly evaluate that third parties or service providers involved in financial transactions strictly adhere to contractual obligations on availability, information security, and cybersecurity, among others. Such third parties or service providers 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 BSP rules and regulations on outsourcing and vendor management.

Failure to perform the above duties and responsibilities may subject the BSFIs, customers or third-party providers for losses arising from fraudulent transactions.

Section X. The following transitory provision shall be incorporated as footnote to Section 148/147-Q/145-S/142-P/126-N as follows:

BSFIs shall comply with the foregoing standards by 30 June 2025.

Section X. Effectivity Clause. This circular shall take effect fifteen (15) calendar days following its publication either in the Official Gazette or any newspaper of general circulation.

FOR THE MONETARY BOARD:

ELI M. REMOLONA, JR.
Governor

__ xxxx 2025