ANTI-FINANCIAL ACCOUNT SCAMMING ACT

REPUBLIC ACT NO. 12010

AN ACT DEFINING AND PENALIZING FINANCIAL ACCOUNT SCAMMING AND OTHER OFFENSES, AND PROVIDING FOR THE ENFORCEMENT MECHANISMS THEREFOR

FOREWORD

The digital age presents both significant opportunities and complex challenges. As we embrace rapid technological advancements in banking and financial services, we are also constrained to confront the growing threat of digital fraud – characterized by its speed, pervasiveness, sophistication, and the anonymity it affords perpetrators.

The enactment of Republic Act No. 12010, also known as the Anti-Financial Account Scamming Act (**"AFASA"**), is a radical step forward in this country's commitment to protecting consumers, deterring fraudsters, and fostering a more inclusive and resilient financial system. The implementing regulations, Bangko Sentral ng Pilipinas (BSP) Circular Nos. 1213, 1214, and 1215, Series of 2025, provide a comprehensive framework for the exercise of the BSP's mandates and translate AFASA's aspirations into actionable rules and policies for BSP-supervised institutions (**"BSIs"**), consumers, and the public. These rules work in tandem to (1) prevent, detect, and delay fraudulent transactions, (2) enhance the ability of fraud victims and BSIs to trace, hold, verify, and recover disputed funds, and (3) provide an expedited procedure for accessing and sharing financial account information for law enforcement purposes.

As fraud schemes continue to evolve to exploit new technologies and system vulnerabilities, the need for effective and anticipatory regulation and collaborative action has never been greater. Guided by global best practices and the particular needs of the Filipino people, the rules equip the BSP and its stakeholders with dynamic tools necessary to build an environment that fosters responsible innovation, strong consumer protection, and a robust and reliable financial system.

AFASA TWG Head

Janice G. Ayson-Zales	Director

AFASA TWG Members

Rochelle D. Tomas	Director
Bridget Rose M. Mesina-Romero	Director
Mary Rose A. Contreras	Director
Alain Bert G. Regis	Acting Director
Abigail M. Asiddao-Alcantara	Deputy Director
Maricris A. Salud	Deputy Director
Paul Khristian J. Baylon	Deputy Director
Fatima Anjanette P. Ferrer-Magtuba	Deputy Director
Carlos Manuel S. Prado	Deputy Director
Tricia T. Defante-Andres	Deputy Director
Leah M. Irao	Deputy Director
Archibald S. Ramos	Legal Officer IV
Joseph Edward L. Matias	Legal Officer IV
Alexander Brian S. Perez	Legal Officer IV
Patricia P. Geraldez-Silva	Senior Complaints Resolution Officer
Richard Armand C. Angeles	Legal Officer IV
Dexter C. Macatangay	Bank Officer V
Antoni Pauline P. Pascual	Bank Officer IV
Henry De Vera	Chief Investigation Officer
Renee Mark Q. Fajardo	Senior Investigation Officer

AFASA TWG Advisers

Elmore O. Capule	Deputy Governor
Charina B. De Vera-Yap	Managing Director

AFASA TWG Secretariat

Cherry Kerr P. Aguilar-Noceda	Bank Officer V
Fidel C. Salo	Bank Officer V
Christian Oliver R. Valdeavilla	Manager
Franklin H. Abella	Cybersecurity Officer
Ervin Jon S. Ventura	Legal Support Officer III
Marco C. Mendoza	Legal Support Officer III
Gene Alejandro M. Asuncion	Legal Support Specialist
Kaleena U. Santillan	Administrative Services Officer III

TABLE OF CONTENTS

REPUBLIC ACT NO. 12010

AN ACT DEFINING AND PENALIZING FINANCIAL ACCOUNT SCAMMING AND OTHER OFFENSES, AND PROVIDING FOR THE ENFORCEMENT MECHANISMS THEREFOR

Section 1. Short Title. - This Act shall be known as the "Anti-Financial Account Scamming Act (AFASA)".

Section 2. Declaration of Policy. - The State recognizes the vital role of banks, non-bank financial institutions, other payment service providers, and the general banking public in promoting and maintaining a stable and efficient financial system. The State also acknowledges that with the increased use of electronic commerce and digital financial services, there is a need to promote awareness on the proper use of Financial Accounts and to protect the public from cybercriminals and criminal syndicates who target Financial Accounts or lure Account Owners into becoming accessories or perpetrators of fraudulent activities. The State shall undertake measures to protect all persons from cybercrime schemes by regulating the use of Financial Accounts and preventing their use in fraudulent activities.

Section 3. Definition of Terms. - As used in this Act:

(a) *Account Owner* refers to the person to whom a Financial Account belongs or under whose name the account was opened or registered;

(b) *Electronic communications* refer to phone calls, short messaging service (SMS), social media platform-enabled messages, electronic mail (email), technology-powered instant messaging, and other messages sent via electronic means;

(c) *Electronic wallet or e-wallet* refers to an electronic instrument or device that can store digital value;

(d) *Financial Account* refers to an account used to avail of products or services offered by Institutions such as:

(1) An interest or non-interest-bearing deposit, trust, investment, or credit card account;

(2) Other transaction account maintained with a bank, non-bank, or financial institution;

(3) E-wallet; and

(4) Any other account used to avail of financial products or services defined under Section 3(c) of Republic Act No. 11765, or the "Financial Products and Services Consumer Protection Act".

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

(f) *Institutions* refer to banks, non-banks, other financial institutions, payments and financial service providers under the jurisdiction of the Bangko Sentral ng Pilipinas (BSP);

(g) *Mass mailer* refers to a service or software used to send electronic communications to an aggregate of fifty (50) or more recipients;

(h) *Multi-Factor Authentication (MFA)* refers to an authentication method that requires two (2) or more verification factors to gain access to a resource; and

(i) *Sensitive identifying information* refers to any information that can be used to access an individual's Financial Accounts such as usernames, passwords, bank account details, credit card, debit card, and e-wallet information among other electronic credentials, and other confidential and personal information.

Section 4. Prohibited Acts. - The following acts shall constitute Financial Account scamming under this Act:

(a) *Money Muling Activities.* - A person performing any of the following acts for the purpose of obtaining, receiving, depositing, transferring, or withdrawing proceeds that are known to be derived from crimes, offenses, or social engineering schemes shall be considered as a money mule:

(1) Using, borrowing or allowing the use of a Financial Account;

(2) Opening a Financial Account under a fictitious name or using the identity or identification documents of another;

(3) Buying or renting a Financial Account;

(4) Selling or lending a Financial Account; or

(5) Recruiting, enlisting, contracting, hiring, utilizing, or inducing any person to perform the acts mentioned in items 1 to 4 of this subsection.

(b) *Social Engineering Schemes.* - A social engineering scheme is committed by a person who obtains sensitive identifying information of another person, through deception or fraud, resulting in unauthorized access and control over the person's Financial Account, by performing any of the following acts:

(1) Misrepresenting oneself as acting on behalf of an Institution, or making false representations to solicit another person's sensitive identifying information; or

(2) Using electronic communications to obtain another person's sensitive identifying information.

(c) *Economic Sabotage.* - The prohibited acts under Section 4(a) and (b) shall be considered as economic sabotage when committed under any of the following circumstances:

(1) By a group of three (3) or more persons conspiring or confederating with one another;

(2) Against three (3) or more persons individually or as a group;

(3) Using a mass mailer; or

(4) Through human trafficking.

Section 5. Other Offenses. - The following shall also constitute as offenses under this Act:

(a) Willfully aiding or abetting in the commission of any of the offenses enumerated under Section 4;

(b) Willfully attempting to commit any of the offenses enumerated under Section 4;

(c) Opening a Financial Account under a fictitious name or using the identity or identification documents of another; or

(d) Buying or selling a Financial Account.

Section 6. Responsibility to Protect Access to Client's Financial Account. - Institutions shall ensure that access to their clients' Financial Accounts is protected by adequate risk management systems and controls such as MFA, FMS, and other Account Owner enrollment and verification processes: *Provided,* That such risk management systems and controls are proportionate and commensurate to the nature, size, and complexity of their operations.

Institutions that are determined by the BSP to be compliant with the requirements of adequate risk management systems and controls

shall not be liable for any loss or damage arising from the offenses under Sections 4 and 5 of this Act.

Without prejudice to other liabilities under existing laws and consistent with BSP rules and regulations, Institutions shall be liable for restitution of funds to the Account Owners for failure to employ adequate risk management systems and controls, or failure to exercise the highest degree of diligence in preventing loss or damage arising from the offenses under Sections 4 and 5. Conviction shall not be a prerequisite to the restitution of funds.

Section 7. Temporary Holding of Funds Subject of a Disputed Transaction. - Institutions shall have the authority to temporarily hold the funds subject of a disputed transaction within the period prescribed by the BSP, which shall not exceed thirty (30) calendar days, unless otherwise extended by a court of competent jurisdiction: *Provided,* That Institutions shall promptly notify the BSP whenever it temporarily holds the funds subject of a disputed transaction.

A transaction shall be considered disputed if the Institution, based on information obtained from another Institution, a complaint from an aggrieved party, or a finding under its own FMS, has reasonable ground to believe that such transaction appears to be:

(a) Unusual;

(b) Without clear economic purpose;

(c) From an unknown or illegal source, or unlawful activity; or

(d) Facilitated through social engineering schemes.

Where such belief arises from a finding under its own FMS, the Institution shall perform acts as may be legally warranted to preserve the integrity of the Financial Account.

No administrative, criminal, or civil liability shall be imposed against an Institution or its directors, trustees, officers, and employees for holding the funds subject of a disputed transaction when done in accordance with BSP rules and regulations.

The BSP shall issue rules and regulations on: the circumstances under which Institutions are required to exercise such authority to avoid probable fraud; the grounds for, procedure, and period of holding funds; the period wherein the Institutions should notify the BSP whenever it holds funds; the verification and validation process; the release of funds subject of a disputed transaction; and other actions that may be undertaken by the Institutions and Account Owners during the period of temporary holding of funds.

Section 8. Coordinated Verification of a Disputed Transaction. - Upon receipt of a complaint, an information from another Institution, or detection through FMS, the Institutions and Account Owners involved shall initiate a coordinated verification process to validate the disputed transaction, regardless of whether the funds remain in the banking system or not. The provisions of Republic Act No. 1405, as amended; Republic Act No. 6426, or the "Foreign Currency Deposit Act of the Philippines", as amended; Republic Act No. 8367, or the "Revised Non-Stock Savings and Loan Association Act of 1997"; and Republic Act No. 10173, or the "Data Privacy Act of 2012" shall not apply during the coordinated verification process of a disputed transaction.

Section 9. Liability for Failure to Temporarily Hold Funds. - An Institution that fails to temporarily hold funds subject of a disputed transaction, as required under this Act and relevant BSP rules and regulations, shall be liable for loss or damage arising from such failure, including the restitution of the disputed funds to the Account Owner.

Section 10. Liability for Improper Holding of Funds. - Without prejudice to liabilities under existing laws, an Institution that holds funds subject of a disputed transaction beyond the allowable period, or improperly holds funds, as provided in this Act and relevant BSP rules and regulations, shall be subjected to administrative action under Republic Act No. 7653, otherwise known as "The New Central Bank Act", as amended.

Section 11. Malicious Reporting. - Any person who, with malice or in bad faith, reports or files completely unwarranted or false information that results in the temporary holding of funds shall be punished under Section 16(e) of this Act.

Section 12. Investigation and Inquiry into Financial Accounts. - The BSP shall have the authority to investigate and inquire into Financial Accounts which may be involved in the commission of a prohibited act or offense under Sections 4 and 5 hereof. The provisions of Republic Act No. 1405, as amended; Republic Act No. 6426, as amended; Republic Act No. 8367; and Republic Act No. 10173 shall not apply to Financial Accounts subject of BSP's investigation.

Any of the information gathered from the investigation or inquiry of a Financial Account by the BSP pursuant to this section may be used for the enforcement of this Act and in the implementation of relevant provisions of Republic Act No. 11765.

The authority to investigate and inquire into Financial Accounts under this section shall be exercised by a duly authorized officer or body from the BSP.

No court below the Court of Appeals shall have jurisdiction to enjoin the BSP from exercising its authority to investigate and inquire into any Financial Account under this Act.

An Institution, or any of its directors, officers, or employees, shall be held free and harmless from any accountability or liability for any act done in compliance with an order from the BSP for an inquiry or investigation of a Financial Account.

Section 13. Cybercrime Warrants and Related Orders. - Without prejudice to the authority of the cybercrime units of the National Bureau of Investigation (NBI) and the Philippine National Police (PNP), the BSP or its duly authorized officer or body shall have the authority to apply for cybercrime warrants and to issue the orders provided in Chapter IV of Republic Act No. 10175, or the "Cybercrime Prevention Act of 2012", with respect to the electronic communications used in any violation of this Act. The BSP may request the assistance of the NBI and the PNP in the investigation of cases and the enforcement and

implementation of cybercrime warrants and related orders for violations of this Act.

Section 14. Sharing of Information of Financial Accounts. - The BSP shall have the authority to issue rules on information-sharing and disclosure with law enforcement and other competent authorities in connection with its inquiry and investigation of Financial Accounts under this Act: *Provided,* That any information on the Financial Account which may be shared by BSP shall be used solely to investigate and prosecute cases involving violations of Sections 4 and 5 of this Act and to implement the relevant provisions of Republic Act No. 11765.

Section 15. Prohibition on the Disclosure of Information of a Financial Account. - Unless otherwise allowed under existing laws, directors, trustees, officers, or employees of an Institution, government officials or employees, or other persons who obtained information on the Financial Account subject of BSP's inquiry or investigation under this Act, shall be prohibited from disclosing such information on the Financial Account for purposes other than those mentioned in Sections 12 and 14 hereof.

Section 16. Penalties. - (a) A person found guilty of the prohibited acts under Section 4(a) shall be penalized with imprisonment of not less than six (6) years but not more than eight (8) years, or a fine of at least One hundred thousand pesos (P100,000.00) but not exceeding Five hundred thousand pesos (P500,000.00), or both, at the discretion of the court. In addition, if the prohibited act falls under Section 4(a), items (1) to (4), the court shall also order the closure of the Financial Account involved in the transaction and forfeiture in accordance with Article 45 of the Revised Penal Code, without prejudice to Section 17 of this Act.

(b) A person found guilty of any of the prohibited acts enumerated under Section 4(b) shall be penalized with imprisonment of not less than ten (10) years but not more than twelve (12) years, or a fine of at least Five hundred thousand pesos (P500,000.00) but not exceeding One million pesos (P1,000,000.00), or both, at the discretion of the court: *Provided,* That the penalty of not less than twelve (12)

years but not more than fourteen (14) years of imprisonment, or a fine of at least One million pesos (P1,000,000.00) but not more exceeding Two million pesos (P2,000,000.00), or both, at the discretion of the court, shall be imposed if the target or victim of the acts enumerated in Section 4(b) is a senior citizen at the time the offense was committed.

(c) A person found guilty of any of the prohibited acts involving economic sabotage enumerated under Section 4(c) shall be penalized with life imprisonment, or a fine of not less than One million pesos (P1,000,000.00) but not exceeding Five million pesos (P5,000,000.00), or both, at the discretion of the court.

(d) A person found guilty of other offenses enumerated in Section 5 shall be penalized with imprisonment of not less than four (4) years but not more than six (6) years, or a fine of at least One hundred thousand pesos (P100,000.00) but not exceeding Two hundred thousand pesos (P200,000.00), or both, at the discretion of the court. In addition, if the prohibited act falls under Section 5(c) or (d), the court shall also order the closure of the Financial Account.

(e) A person found guilty of reporting or filing completely unwarranted or false information that resulted in the temporary holding of funds under Section 11 shall be penalized with imprisonment of not less than one (1) year but not more than five (5) years, or a fine of not less than Fifty thousand pesos (P50,000.00) but not exceeding Two hundred thousand pesos (P200,000.00), or both, at the discretion of the court.

(f) A person found guilty of knowingly or willfully obstructing, impeding, frustrating, or delaying the inquiry and investigation of the BSP as provided under Section 12 shall be penalized with imprisonment of not less than one (1) year but not more than five (5) years, or a fine of not less than Fifty thousand pesos (P50,000.00) but not exceeding Two hundred thousand pesos (P200,000.00), or both, at the discretion of the court.

(g) An official, employee, or agent of an Institution, the government, or any person who obtained information on the Financial Account subject of BSP's inquiry or investigation who shall commit the prohibited act under Section 15 shall be penalized with imprisonment of not less than one (1) year but not more than five (5) years, or a fine of not less than Fifty thousand pesos (P50,000.00) but not exceeding Two hundred thousand pesos (P200,000.00), or both, at the discretion of the court.

(h) When an offender is a juridical person, the fine to be imposed shall be double the amount of the corresponding penalty but shall not exceed Ten million pesos (P10,000,000.00). The liability imposed on the juridical person shall be without prejudice to the criminal liability of the responsible officer who committed the prohibited acts or other offenses under this Act.

(i) A government official or employee who shall be found guilty of the acts or offenses under Sections 4 and 5 shall, in addition to the penalties prescribed under this section, suffer perpetual absolute disqualification from holding any appointive or elective position in the government, or in any agency, entity, or instrumentality thereof.

Section 17. Civil Liability in Case of Conviction. - A conviction for violation of this Act shall carry with it civil liability, which may include restitution for the damage done in favor of the aggrieved party of any unwarranted benefit derived from such violation.

Independent of a criminal case, all properties, tools, instruments and/or any other non-liquid assets used for the commission of the acts prohibited in Sections 4 and 5 of this Act shall be subject to civil forfeiture, upon finding of probable cause, in accordance with rules of procedure to be formulated by the Supreme Court: *Provided,* That in cases of economic sabotage as defined in Section 4(c), the rules shall include a summary procedure for the release of a portion of such assets to the Department of Justice (DOJ) upon *ex-parte* motion, even during the pendency of the proceedings, for operational support and victim

protection, including victims of human trafficking involved in the commission of prohibited acts and other offenses in this Act.

Section 18. Administrative Sanctions. - Without prejudice to the criminal and civil liabilities prescribed under this Act, the administrative sanctions specified in Republic Act No. 7653, as amended, shall be imposed upon the Institution, its directors, officers, trustees, employees, or agents, for violation of this Act or any related rules, regulations, orders or instructions of the BSP.

Section 19. Criminal Liability Under Other Laws. - Prosecution under this Act shall be without prejudice to prosecution for any violation of the Revised Penal Code, as amended, or special laws such as Republic Act No. 8484, or the "Access Devices Regulation Act of 1998", as amended; Republic Act No. 9160, or the "Anti-Money Laundering Act of 2001", as amended; and Republic Act No. 10175.

Section 20. Immunity of Trafficked Persons from Criminal Liability. - Victims of trafficking in persons as defined under Republic Act No. 9208, or the "Anti-Trafficking in Persons Act of 2003", as amended, shall be free from criminal liability for acts committed as a direct result of being trafficked. Conviction under Republic Act No. 9208, as amended, shall not be a prerequisite to this defense, and it shall be sufficient to show clear and convincing evidence of circumstances under prevailing manuals, guidelines, and similar instruments on victim identification issued by the Inter-Agency Council Against Trafficking (IACAT).

Section 21. Jurisdiction. - The Regional Trial Court shall have jurisdiction over any violation of the provisions of this Act. Jurisdiction shall lie if any of the elements was committed within the Philippines or committed with the use of any device, tool, equipment, computer system or infrastructure, wholly or partly situated in the country, or when by such commission, damage is caused to a natural or juridical person who was in the Philippines at the time the offense was committed or whose Financial Account is maintained with an Institution operating in the Philippines.

Section 22. General Principles Relating to International Cooperation. - To the widest extent possible, all relevant instruments on international cooperation in criminal matters and arrangements agreed on the basis of reciprocal legislation and domestic laws, shall be given full force and effect for the purposes of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in the electronic form.

Section 23. Implementing Rules and Regulations. - Within one (1) year from the effectivity of this Act, the BSP, in coordination with the DOJ, the Department of Information and Communications Technology (DICT), the NBI, the PNP, the Cybercrime Investigation and Coordination Center (CICC), and the Anti-Money Laundering Council (AMLC), and upon consultation with relevant stakeholders, shall promulgate the rules and regulations to effectively implement the provisions of this Act.

A cooperative mechanism shall be established among the Institutions, the BSP, concerned government agencies and the private sector, to ensure the effective enforcement of the provisions and the prosecution of cases under this Act.

Section 24. Separability Clause. - If any provision of this Act is declared invalid or unconstitutional, the remainder thereof not otherwise affected shall remain in full force and effect.

Section 25. Repealing Clause. - All laws, presidential decrees, executive orders, letters of instructions, proclamations, or administrative regulations that are inconsistent with the provisions of this Act are hereby repealed, amended, or modified accordingly.

Section 26. Effectivity. - This Act shall take effect after fifteen (15) days following its publication in the *Official Gazette* or in a national newspaper of general circulation.

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

"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. *Card skimming* xxx
f. *Cloud computing* xxx
g. *Compromised state* xxx
h. *Cyber-threat* xxx
i. *Cybersecurity* xxx
j. *Data Breach* xxx
k. *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. *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. *Hacking* xxx

r. *Information security program (ISP)* xxx
s. *Information security strategic plan (ISSP)* xxx
t. *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. *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. *Pharming* xxx
z. *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. *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. *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. *Spear phishing* xxx
hh. *Threat actor* xxx
ii. *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. Failing to do so may erode consumer confidence in electronic channels as safe, secure, 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 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 701/701-Q/401-S/114-P/ 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 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 for electronic banking, electronic payment, electronic money and other electronic products and services.

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

xxx

D. Clearing Switch Operator (CSO)

xxx

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:

(sgd.)
ELI M. REMOLONA, JR.
Governor

CIRCULAR NO. 1214
Series of 2025

Subject : **Rules of Procedure on the Conduct of Inquiry into Financial Accounts and Sharing of Financial Account Information by the Bangko Sentral ng Pilipinas Pursuant to the Anti-Financial Account Scamming Act (AFASA)**

The Monetary Board, in its Resolution No. 522 dated 22 May 2025, approved the following Rules of Procedure on the Conduct of Inquiry into Financial Accounts and Sharing of Financial Account Information by the *Bangko Sentral ng Pilipinas* (**BSP**) pursuant to Sections 12, 13, and 14 of Republic Act No. 12010, otherwise known as the "Anti-Financial Account Scamming Act" (**AFASA**) –

RULE I
GENERAL PROVISIONS

SECTION 1. TITLE. These Rules shall be known as the *"Rules of Procedure on the Conduct of Inquiry into Financial Accounts and Sharing of Financial Account Information by the Bangko Sentral ng Pilipinas Pursuant to the Anti-Financial Account Scamming Act* (**AFASA**).*"*

SECTION 2. CONSTRUCTION. All doubts in the interpretation of the provisions of these Rules shall be construed in favor of the effective implementation of the AFASA.

Unless otherwise stated herein, the provisions of the Rules of Court shall not apply, except suppletorily or by analogy as may be determined by CAPO.

SECTION 3. INAPPLICABILITY OF LAWS ON SECRECY OF DEPOSITS AND DATA PRIVACY. The BSP shall have the authority to investigate and inquire into Financial Accounts which may be involved or utilized in the commission of a Prohibited Act. The provisions of Republic Act No. 1405, as amended, or the "Secrecy of Bank Deposits Law"; Republic Act No. 6426, as amended, or the "Foreign Currency Deposit Act of the Philippines"; Republic Act No. 8367, or the "Revised Non-Stock Savings

and Loan Association Act of 1997"; and Republic Act No. 10173, or the "Data Privacy Act of 2012," shall not apply to any Financial Account subject of BSP's investigation and inquiry.

RULE II
DEFINITION OF TERMS

SECTION 4. DEFINITION OF TERMS. The terms as defined under the AFASA are hereby adopted. For purposes of these Rules, the following terms are hereby defined:

a. *Competent Authority* refers to any of the following:

   i. The Philippine National Police (**PNP**), National Bureau of Investigation (**NBI**), Department of Justice (**DOJ**), Anti-Money Laundering Council (**AMLC**), Cybercrime Investigation and Coordinating Center (**CICC**), and any other government agency duly authorized by law to investigate and/or prosecute the Prohibited Acts; and

   ii. Financial Regulators duly authorized to investigate crimes or offenses related to their respective regulatory functions and adjudicate financial consumer complaints under Section 6(f) of Republic Act No. 11765, or the "Financial Products and Services Consumer Protection Act" (**FCPA**).

b. *Consumer Account Protection Office* (**CAPO**) refers to the duly-constituted office within BSP that is authorized to inquire into Financial Accounts and share Financial Account Information with Competent Authorities within the scope defined under the AFASA.

c. *Day* refers to a "calendar" day.

d. *Financial Account* refers to an account used to avail of products or services offered by Institutions, such as:

   i. An interest or non-interest-bearing deposit, trust, investment, or credit card account;

ii. Other transaction account maintained with a bank, non-bank, or financial institution;
iii. E-wallet; and
iv. Any other account used to avail of financial products or services defined under Section 3(c) of the FCPA.

e. *Financial Account Information* refers to any information related to a Financial Account, such as, but not limited to:

i. Account number;
ii. Account owner's name and other personal information;
iii. Registered mobile number and e-mail address of the account owner;
iv. Documents submitted by the account owner for the purpose of opening and/or maintaining the Financial Account;
v. Type and status of the accounts; or
vi. Transaction records.

f. *Inquiry* refers to the act of examining, looking into, and obtaining information, documents or objects pertaining to a Financial Account for the purpose of determining whether the same was involved or utilized in the commission of a Prohibited Act. An Inquiry may be conducted either onsite or offsite, and may include any of the following:

i. Reviewing reports and documents pertaining to a Financial Account;
ii. Interviewing and obtaining sworn statements of any of the Institution's officers, employees, stockholders, owners, representatives, agents, managers, directors, or officers-in-charge;
iii. Gathering, inspecting, and evaluating all physical and electronic documents, communications, records, and other information related to a Financial Account; or
iv. Performing any other activity in the course of investigating a Financial Account which may be involved or utilized in the commission of a Prohibited Act.

g. *Institutions* refer to banks, non-banks, other financial institutions, payments and financial services providers under the jurisdiction of the BSP.

h. *Portable Document Format* (**PDF**) refers to a file format of an electronic document generated from a word processing or PDF creation program, or through electronic scanning of a physical document, or combination of both methods. In all cases, the contents of the PDF copy must be completely legible.

i. *Prohibited Act* refers to any of the following acts which are punishable under Sections 4 and 5 of the AFASA:

   i. *Money Muling Activities*. A person performing any of the following acts for the purpose of obtaining, receiving, depositing, transferring, or withdrawing proceeds that are known to be derived from crimes, offenses, or social engineering schemes shall be considered as a money mule:

      1. Using, borrowing or allowing the use of a Financial Account;
      2. Opening a Financial Account under a fictitious name or using the identity or identification documents of another;
      3. Buying or renting a Financial Account;
      4. Selling or lending a Financial Account; or
      5. Recruiting, enlisting, contracting, hiring, utilizing, or inducing any person to perform the acts mentioned in items 1 to 4 of this subsection.

   ii. *Social Engineering Schemes*. A Social Engineering Scheme is committed by a person who obtains sensitive identifying information of another person, through deception or fraud, resulting in unauthorized access and control over the person's Financial Account, by performing any of the following acts:

1. Misrepresenting oneself as acting on behalf of an Institution, or making false representations to solicit another person's sensitive identifying information; or
2. Using electronic communications to obtain another person's sensitive identifying information.

iii. *Economic Sabotage*. A Money Muling Activity or Social Engineering Scheme shall be considered as Economic Sabotage when committed under any of the following circumstances:

1. By a group of three (3) or more persons conspiring or confederating with one another;
2. Against three (3) or more persons individually or as a group;
3. Using a mass mailer; or
4. Through human trafficking.

iv. *Other Offenses.* Refers to the following acts:

1. Willfully aiding or abetting in the commission of Money Muling Activity, Social Engineering Scheme, or Economic Sabotage;
2. Willfully attempting to commit Money Muling Activity, Social Engineering Scheme, or Economic Sabotage;
3. Opening a Financial Account under a fictitious name or using the identity or identification documents of another; or
4. Buying or selling a Financial Account.

j. *Sensitive Identifying Information* refers to any information that can be used to access an individual's Financial Accounts such as usernames, passwords, bank account details, credit card, and e-wallet information among other electronic credentials, and other confidential and personal information.

RULE III
INFORMATION SHARING AGREEMENT WITH COMPETENT AUTHORITIES

SECTION 5. EXECUTION OF AN INFORMATION SHARING AGREEMENT. A Competent Authority shall enter into an *Information Sharing Agreement* with BSP, which shall govern the sharing of Financial Account Information obtained by CAPO pursuant to its authority to investigate and inquire into Financial Accounts under the AFASA and these Rules. The CAPO shall only accept a *Request to Inquire into Financial Account* (the "**Request**") from, and disclose Financial Account Information to, a Competent Authority that has an existing *Information Sharing Agreement* with BSP.

SECTION 6. CONTENTS OF AN INFORMATION SHARING AGREEMENT. The *Information Sharing Agreement* between BSP and the Competent Authority shall be in writing, notarized, and shall contain the terms and conditions for the sharing of Financial Account Information, including, but not limited to, the following:

a. Undertaking of the Competent Authority to use the Financial Account Information for the specific purposes indicated in Sections 12 and 14 of the AFASA;

b. Position or designation of the officers of the Competent Authority who are authorized to request and receive Financial Account Information from BSP;

c. Dedicated official electronic mail (e-mail) accounts to be used in the electronic transmission of *Requests* and correspondence between BSP and the Competent Authority, as well as the official address of the Competent Authority where physical copies of the orders, notices, correspondences, and other relevant documents will be delivered;

d. Security measures to protect Financial Account Information obtained from BSP, including the Competent Authority's policies on:

   i. Disclosure and confidentiality;
   ii. Encryption and data protection;
   iii. Retention and disposal of records;
   iv. Management of security incidents and breaches;
   v. Access controls and authorization;
   vi. Audit trails;
   vii. Data integrity and validation;
   viii. Data transfer and transmission security; and
   ix. Other administrative, technical, and physical safeguards; and

e. Duration, periodic review, and renewal of the *Information Sharing Agreement.*

SECTION 7. USE OF FINANCIAL ACCOUNT INFORMATION SHARED BY CAPO. Any Financial Account Information shared by CAPO to a Competent Authority pursuant to these Rules shall be used solely to investigate and prosecute criminal cases involving the commission of a Prohibited Act, or to adjudicate a financial consumer complaint under Section 6(f) of the FCPA.

The Competent Authority shall be fully responsible for maintaining the confidentiality and security of any information shared by CAPO pursuant to these Rules.

RULE IV
REQUEST FOR INQUIRY INTO FINANCIAL ACCOUNT

SECTION 8. FILING OF A REQUEST. An Inquiry into a Financial Account by CAPO shall be initiated upon the filing of a *Request* by a Competent Authority with CAPO. The *Request* shall be filed primarily through electronic transmission using the Competent Authority's dedicated e-mail account to the official e-mail address of CAPO, attaching therewith a PDF copy of the *Request* and all its supporting documents. The CAPO shall acknowledge receipt of the *Request* through e-mail. The date indicated in the acknowledgment e-mail of CAPO shall constitute the effective date of receipt of the *Request*.

The Competent Authority shall implement appropriate security measures in the transmission of the *Request* and supporting documents to CAPO. The Competent Authority shall also ensure that access to the information contained in the *Request* is restricted to authorized personnel only, and that all documents, records, and information are transmitted through secure channels only.

SECTION 9. CONTENTS OF THE REQUEST. The *Request* must be in writing, under oath, and shall contain, among others, the following information:

a. Full name, position, office/department/unit, office address, and contact details of the authorized officer of the Competent Authority;
b. Purpose and justification for an inquiry into a Financial Account;

c. Description of the Financial Account suspected to be involved or utilized in the commission of a Prohibited Act;

d. Details of the Prohibited Act that was committed and how the Financial Account subject of the *Request* has been involved or utilized in its commission;

e. Scope of the transactions involving the Financial Account which are relevant to the investigation of a Prohibited Act;

f. A statement as to whether the suspected Prohibited Act was reported to the Institution concerned by a victim or private complainant, and the actions taken by such Institution; and

g. Other relevant and material information, which may include the following:

    i. Date, time, and place of the commission of the Prohibited Act;
    ii. Name, age, address, and contact information of any private complainant or victim;
    iii. Available information on any suspect or person of interest, which may include the person's name, alias,

age, and last known address; and

iv. Name, age, address, and contact information of any known witness.

SECTION 10. ATTACHMENTS TO THE REQUEST. The *Request* shall be accompanied by documents and pieces of evidence in support of the Competent Authority's finding that the Financial Account subject of the *Request* was involved or utilized in the commission of a Prohibited Act. These may include affidavits of the investigating officers, private complainants, victims, or witnesses; forensic analysis reports; business records; transaction logs and records; photographs; and video recordings.

RULE V
INQUIRY ORDER

SECTION 11. FORM AND CONTENTS OF THE INQUIRY ORDER. The *Inquiry Order* shall:

a. State the factual and legal bases for the conduct of Inquiry;

b. Describe with particularity the Financial Account subject of the Inquiry and the Prohibited Act that was purportedly committed using the Financial Account;

c. Direct the Institution to:

   i. Disclose relevant Financial Account Information to CAPO;
   ii. Provide CAPO full access to all physical and electronic records related to the Financial Account subject of the Inquiry within the duration of the Inquiry; and
   iii. Allow CAPO to conduct the activities mentioned in Section 4(f) of these Rules, and comply with any instruction by CAPO in connection with its Inquiry.

d. Forbid the Institution or any of its officers, employees, stockholders, owners, representatives, agents, managers, directors, or officers-in-charge from disclosing, divulging, directly or indirectly, or in any manner, to the owners or

holders of Financial Account subject of the Inquiry, or to any other person, the fact that said Financial Account is being inquired into, with a warning that violation thereof is punishable under Section 16(f) of the AFASA.

SECTION 12. ISSUANCE OF AN INQUIRY ORDER. Within reasonable time from receipt of the *Request*, CAPO shall issue an *Inquiry Order* to the Institution concerned, copy furnished the requesting Competent Authority, upon its determination that, based on the information and evidence provided in the *Request* and supporting documents, there exists sufficient ground to establish a well-founded belief that a Prohibited Act has been committed and that the Financial Account subject of the *Request* may be involved or utilized in the commission of the Prohibited Act.

The CAPO shall serve the *Inquiry Order* to the Institution concerned electronically by transmitting a PDF copy thereof to all of the registered e-mail accounts of the Institution. The date indicated in the electronic record of delivery of the *Inquiry Order* shall be the effective date of receipt by the Institution concerned.

SECTION 13. CORRECTION OR AMENDMENT OF REQUEST. Upon determination of CAPO that the *Request* fails to establish the ground specified in Section 12 of these Rules, or is non-compliant with these Rules or an existing *Information Sharing Agreement*, it shall issue a *Notice to Amend* to the Competent Authority stating its findings on the deficiencies of the *Request*. The date indicated in the electronic record of delivery of the notice shall be the effective date of receipt by the Competent Authority.

The Competent Authority may file a corrected or amended *Request* with CAPO within fifteen (15) days from receipt of the *Notice to Amend*, following the same procedures in Section 8 of these Rules.

SECTION 14. DENIAL OF REQUEST. If the Competent Authority fails to correct or amend the *Request* within the prescribed period, or if CAPO determines that the corrected or amended *Request* still fails to establish the ground mentioned in Section 12 of these Rules, or remains non-compliant with these Rules or an existing *Information Sharing Agreement,* it shall issue a *Notice of Denial* informing the Competent Authority of the denial of its *Request* with prejudice, and

specifying the reasons for such denial.

The Competent Authority may file a motion for reconsideration of CAPO's denial of *Request* within five (5) days from receipt of the *Notice of Denial*. A second motion for reconsideration shall not be allowed.

A denial of a motion for reconsideration is final and is not appealable to the Governor or the Monetary Board.

RULE VI
DISCLOSURE OF FINANCIAL ACCOUNT INFORMATION

SECTION 15. DUTIES OF AN INSTITUTION. Upon receipt of the *Inquiry Order*, the Institution concerned shall immediately comply with CAPO's directives. Within ten (10) days from receipt of the *Inquiry Order*, the Institution concerned shall submit to CAPO a *Return on the Inquiry Order* (the "**Return**") providing therein all the Financial Account Information required in the *Inquiry Order*, as well as other relevant supporting documents. A PDF copy of the *Return* and its supporting documents shall be submitted electronically by the Institution concerned to the official e-mail account of CAPO.

The Institution concerned shall implement appropriate measures to safeguard all information and documents shared with CAPO. The Institution concerned shall also ensure that access to any information shared with CAPO is restricted to authorized personnel only, and that all documents, records, and information are transmitted through secure channels only.

SECTION 16. DISCLOSURE OF THE RESULTS OF INQUIRY. CAPO shall furnish the Competent Authority with its *Response to the Request for Inquiry into Financial Account* containing the relevant Financial Account Information and other related documents gathered, by sending an e-mail to the Competent Authority's dedicated e-mail account within ten (10) days from its receipt of the *Return* and all the necessary information from the Institution concerned, unless otherwise extended by CAPO for meritorious reasons.

SECTION 17. DISCLOSURE OF PREVIOUSLY SHARED FINANCIAL ACCOUNT INFORMATION. If CAPO has determined that the subject of the *Request* pertains or is identical to any Financial Account Information previously shared with another Competent Authority, it may disclose the requested information in accordance with the procedures prescribed in the immediately preceding section without conducting a new or separate Inquiry; *Provided,* that such *Request* must establish the ground mentioned in the first paragraph of Section 12 of these Rules and must not have any of the defects mentioned in the first paragraph of Section 13 of these Rules. Provided, further, that the Financial Account Information to be disclosed by CAPO shall be limited strictly to the details specified in the new *Request*.

SECTION 18. SAFE HARBOR CLAUSE. Any Institution, or any of its officers, employees, stockholders, owners, representatives, agents, managers, directors, or officers-in-charge shall be held free and harmless from any accountability or liability for any act done in compliance with an *Inquiry Order* of CAPO.

RULE VII
ELECTRONIC TRANSMISSION OF CORRESPONDENCE

SECTION 19. REGISTRATION OF E-MAIL ACCOUNTS. Institutions must register with BSP the e-mail accounts that they will use to communicate with CAPO. The e-mail accounts must be authorized by the President of the Institution or an officer of equivalent rank. An Institution can officially register a maximum of three (3) e-mail accounts. Each e-mail account shall be registered to a single officer only, one of whom must be the President, Chief Compliance Officer, Head of the Legal Department of the Institution, or an officer of equivalent rank. In no case shall there be two (2) or more registered officers for the same e-mail address.

Within thirty (30) days from the effectivity of these Rules, Institutions shall register their e-mail accounts using the prescribed *Registration Form* which can be downloaded from the BSP website. The scanned copy of the duly-accomplished *Registration Form* shall be transmitted to the official e-mail account of CAPO.

SECTION 20. USE OF REGISTERED E-MAIL ACCOUNT. All *Inquiry Orders* and other notices of CAPO shall be sent exclusively to the registered e-mail accounts of an Institution. The CAPO shall only acknowledge and accept submissions from a registered e-mail account of an Institution. An electronic transmittal from an unregistered e-mail account shall be rejected and shall not be considered as an official submission of an Institution in accordance with AFASA.

SECTION 21. CHANGES IN THE REGISTERED E-MAIL ACCOUNTS. In the event that an authorized officer with access to a registered e-mail account is separated from service or is otherwise no longer authorized to act on behalf of an Institution, or, in case a registered e-mail account has been compromised, the Institution concerned shall immediately:

a. Revoke the separated or unauthorized officer's access to the registered e-mail account and all data contained therein;

b. Disable access to the compromised e-mail account;

c. Notify CAPO within three (3) days from the separation, or revocation of access, of the concerned officer. In case of a compromised e-mail account, such notification must be made within twenty-four (24) hours upon discovery of the compromise or security breach; and

d. Register a replacement e-mail account following the procedures under Section 19 of these Rules.

SECTION 22. PRESUMPTION OF RECEIPT. Any e-mail sent by CAPO to an Institution's registered e-mail account shall be presumed to have been duly received by the Institution. It shall be the responsibility of the Institution to ensure the availability, functionality, and capacity of its registered e-mail accounts to receive all official communications from CAPO, including *Inquiry Orders*, notices, correspondence, and other relevant documents.

SECTION 23. USE OF ALTERNATIVE MODES OF TRANSMISSION. For meritorious reasons, BSP may authorize and resort to alternative modes of transmission of *Requests, Inquiry Orders*, notices, correspondence, documents and other communication under these

Rules, subject to strict adherence to appropriate security measures to ensure the confidentiality, integrity, and availability of transmission.

RULE VIII
CYBERCRIME WARRANTS AND PRESERVATION ORDER

SECTION 24. APPLICATION FOR CYBERWARRANTS AND PRESERVATION ORDER. Without prejudice to the authority of the cybercrime units of NBI and PNP, CAPO shall have the authority to apply for cybercrime warrants and/or to issue preservation orders as provided in Chapter IV of Republic Act No. 10175, or the "Cybercrime Prevention Act of 2012," with respect to the electronic communications involved in the commission of a Prohibited Act.

SECTION 25. REQUEST FOR ASSISTANCE WITH LAW ENFORCEMENT AUTHORITIES. The CAPO may request the assistance of NBI and PNP in the enforcement and implementation of cybercrime warrants and preservation orders in relation to its investigation and inquiry.

RULE IX
UNAUTHORIZED DISCLOSURE AND NON-COMPLIANCE WITH CAPO'S INQUIRY ORDER

SECTION 26. UNAUTHORIZED DISCLOSURE OF FINANCIAL ACCOUNT INFORMATION. Unless otherwise allowed under existing laws, any person who obtained any information on the Financial Account subject of CAPO's investigation or inquiry under these Rules shall be prohibited from disclosing such information for purposes other than those mentioned in Sections 12 and 14 of the AFASA.

Any person who shall disclose any information mentioned in the immediately preceding paragraph for purposes other than those mentioned under Sections 12 and 14 of the AFASA shall be subject to criminal and administrative liabilities under Section 16(g) of the AFASA, Sections 36 and 37 of Republic Act No. 7653, as amended, other applicable laws, and BSP rules and regulations.

SECTION 27. FAILURE TO COMPLY WITH CAPO'S INQUIRY ORDER. Any person who knowingly or willfully obstructs, refuses, impedes, or delays the investigation and inquiry of CAPO under these Rules shall be subject to criminal and administrative liabilities under Section 16(f) of

the AFASA, Republic Act No. 7653, as amended, other existing laws, and BSP rules and regulations.

RULE X
FINAL PROVISIONS

SECTION 28. INVESTIGATIVE AUTHORITY OF BSP. The BSP, based on meritorious reasons, may *motu proprio* initiate or conduct investigation of a Financial Account which may be involved or utilized in the commission of a Prohibited Act. In the conduct of such investigation, CAPO shall have the authority to inquire into a Financial Account and share Financial Account Information in accordance with these Rules.

SECTION 29. TRANSITORY CLAUSE. These Rules shall apply to all *Requests* filed after its effectivity, provided that the Prohibited Act subject of a *Request* was committed after the effectivity of the AFASA.

SECTION 30. SEPARABILITY CLAUSE. If any part of these Rules is declared unconstitutional or invalid, the remainder thereof not otherwise affected shall remain valid.

SECTION 31. REPEALING CLAUSE. All existing rules, regulations, orders, or circulars or any part thereof which are inconsistent with these Rules are hereby repealed, amended, or modified accordingly.

SECTION 32. EFFECTIVITY CLAUSE. These Rules shall take effect fifteen (15) days following its publication in any newspaper of general circulation.

FOR THE MONETARY BOARD:

(sgd.)
ELI M. REMOLONA, JR.
Governor

CIRCULAR NO. 1215
Series of 2025

Subject : **Regulations on the Temporary Holding of Funds Subject of Disputed Transactions and Coordinated Verification Process**

The Monetary Board, in its Resolution No. 523 dated 22 May 2025, approved the adoption of the Regulations on the Temporary Holding of Funds Subject of Disputed Transactions and Coordinated Verification Process to implement Sections 7 to 11 of Republic Act (R.A.) No. 12010 or the "Anti-Financial Account Scamming Act (AFASA)," and accordingly approved the constitution of new provisions and/or amendments to the relevant provisions of the Manual of Regulations for Banks (MORB), the Manual of Regulations for Non-Bank Financial Institutions (MORNBFI), and the Manual of Regulations for Payment Systems (MORPS).

Section 1. *Temporary Holding of Funds Subject of Disputed Transactions and Coordinated Verification Process.* Section 1006/1006-Q/1105, and Appendices 160/Q-104/1105-1 (*Annex A of this Circular*), 161/Q-105/1105-2 (*Annex B of this Circular*), and 162/Q-106/1105-3 (*Annex C of this Circular*), of the MORB/MORNBFI/MORPS shall be created to read as follows:

1006/1006-Q/1105 TEMPORARY HOLDING OF FUNDS SUBJECT OF DISPUTED TRANSACTIONS AND COORDINATED VERIFICATION PROCESS

Policy Statement. The State recognizes the vital role of banks, non-bank financial institutions, other payment service providers, and the general banking public in promoting and maintaining a stable and efficient financial system. The State also acknowledges that with the increased use of electronic commerce and digital financial services, there is a need to promote awareness on the proper use of financial accounts and to protect the public from cybercriminals and criminal syndicates who target financial accounts or lure account

owners into becoming accessories or perpetrators of fraudulent activities. The State shall undertake measures to protect all persons from cybercrime schemes by regulating the use of financial accounts and preventing their use in fraudulent activities.

Scope and Applicability. This Section applies to all *Bangko Sentral*-Supervised Institutions (BSIs) that shall pursue the coordinated verification of disputed transactions as defined under this Section, regardless of whether the funds remain in the financial system or not.

Temporary holding of disputed funds as defined under this Section shall apply to electronic transfer of funds from one financial account to another financial account.

This Section shall not apply to erroneous transactions. These regulations shall likewise not apply to credit card transactions, except insofar as credit cards are used to perform electronic fund transfers through Automated Clearing House (ACH).

Obligations of BSIs with respect to erroneous transactions shall be covered by Section 1003/1003-Q of the MORB/MORNBFI (*Consumer Protection Standards of Conduct*).

The provisions on unauthorized transactions and liability for losses arising from unauthorized transactions under Section 1003/1003-Q of the MORB/MORNBFI (*Consumer Protection Standards of Conduct*) are hereby supplemented.

Further, this Section shall not restrict or limit the application of anti-money laundering laws, rules, and regulations.

Definition of Terms. For purposes of this Section, the following definitions shall apply:

a. *Account Owner* – refers to the person, natural or juridical, to whom a financial account belongs or under whose name the account was opened or registered.

b. *Automated Clearing House* (ACH) – refers to a multilateral agreement among ACH participants governing the clearing and settlement of payment orders for a specific payment stream.

c. *ACH Participant* – refers to a financial institution duly licensed by the *Bangko Sentral* that is a Payment System Management Body member, and undertakes clearing in, and is a signatory to, at least one ACH.

d. *Bangko Sentral-Supervised Institution* (BSI) – refers to a person, natural or juridical, that provides financial products or services under the jurisdiction of the *Bangko Sentral*, as provided in existing laws, rules and regulations. This covers banks, non-banks, payments and other financial service providers, including ACH participants and CSOs, under the jurisdiction of the *Bangko Sentral*. Further, for purposes of this Section, BSIs may refer to originating financial institutions (OFIs), receiving financial institutions (RFIs), or subsequent receiving financial institutions (Subsequent-RFIs) as defined herein.

e. *Beneficiary Account* – refers to a financial account where disputed funds have been credited, whether total or partial, and regardless of the fact that the funds may have been subsequently transferred or exfiltrated to a different financial account, within the same or different BSI, or withdrawn from the financial system.

f. *Beneficiary Account Owner* – refers to the owner of the beneficiary account based on the BSI's records.

g. *Clearing Switch Operator* (CSO) – refers to the party designated which provides clearing switch services by acting as the operator of a payment system to be used by the ACH participants in accordance with the guidelines and principles set forth in related ACH documents.

h. *Coordinated Verification Process* – refers to a systematic sharing of information and coordination among BSIs, including ACH participants and CSOs, and account owners to track and determine the legitimacy of a disputed transaction.

i. *Day* – refers to twenty-four (24) hours. In computing a period, the first day shall be excluded, and the last day included.

j. *Disputed Funds* – refer (1) to the funds or equivalent amounts subject of a disputed transaction, or (2) to the funds or equivalent amounts, whether total or partial, that originated from a disputed transaction and moved through various financial accounts within the same or different BSIs.

k. *Disputed Transaction* – refers to a financial transaction that occurs after the effectivity of the AFASA,[1] where a BSI has reasonable grounds to believe, based on an information obtained from another BSI, a complaint from an aggrieved party, or a finding under its own FMS, that such transaction appears to be any of the following:

(1) *Unusual.* A transaction is considered unusual when it shows patterns that are inconsistent

[1] 13 August 2024.

with the account owner's usual behavior, is not commensurate with the known business or financial capacity of the account owner, or deviates from the account owner's profile. It also covers transactions that are inconsistent in amount, origin, destination, or type with an account owner's known legitimate business or activities or are significantly larger than the typical transactions of an account owner.

(2) *Without clear economic purpose.* This covers transactions that have no underlying legal or trade obligation, purpose, or economic justification. It also includes transactions that appear to be out of the normal course for industry practice, do not appear to be economically viable for the account owner, are unnecessarily complex for their stated purpose, are without business explanation for their size, or are not commensurate with the business size and without reasonable justification.

(3) *From an unknown or illegal source, or unlawful activity.* A source is unknown if the clear and legitimate source cannot be established or does not match the BSI's information on the account owner's profile. This includes situations where there is insufficient or no documentation to support the origin of funds. A transaction is considered to be from an illegal source when it arises from, or uses the proceeds of, an unlawful activity. Unlawful activity refers to any act or omission, or series or combination thereof, that violates a provision of law or constitutes a criminal offense. Prior conviction is not necessary to consider an act or activity as unlawful or criminal.

(4) *Facilitated through social engineering schemes.* A transaction is considered facilitated through

social engineering schemes when sensitive identifying information of another person is obtained through deception or fraud resulting in unauthorized access and control over a financial account. The scheme may be performed by any of the following acts: misrepresenting oneself as acting on behalf of a BSI; making false representations to solicit another person's sensitive identifying information; or using electronic communications to obtain another person's sensitive identifying information.

l. *Disputed Transaction Chain* – refers to a series or sequence of linked transactions involving funds that originated from a disputed transaction and moved through various financial accounts with RFIs and/or subsequent-RFIs to a final destination, including cash out or cash withdrawal.

m. *Domestic Remittance* – refers to a transfer of funds between a sender/remitter and a beneficiary who are both within the Philippines and that is not covered by electronic payment transactions as defined under the National Retail Payment System Framework.

n. *Electronic Fund Transfer* (EFT) – refers to transfers of funds between two financial accounts in the same or different BSIs which are initiated and received using electronic devices and channels to transmit payment instructions. This is synonymous to electronic payments and excludes domestic remittance transactions under existing *Bangko Sentral* regulations.

o. *Erroneous Transaction* – refers to an incorrect electronic fund transfer or domestic remittance as a result of any of the following circumstances: sending to an incorrect beneficiary account due to the

erroneous encoding of account number by the sender; and sending to a beneficiary account an incorrect amount due to erroneous encoding by the sender.

p. *Extended Holding* – refers to the holding of disputed funds for not more than twenty-five (25) calendar days after the lapse of the initial holding period, in accordance with this Section.

q. *Extended Holding Request* – refers to a request initiated by the OFI to extend the initial holding of disputed funds for an additional period of not more than twenty-five (25) calendar days.

r. *Financial Account* – refers to an account used to avail of products or services offered by BSIs, such as interest or non-interest bearing deposit, trust, investment, or credit card account; other transaction account maintained with a bank, non-bank, or financial institution; e-wallet; and any other account used to avail of financial products or services defined under Section 3(c) of R.A. No. 11765. The term is synonymous with transaction account, as used and defined under the MORPS.

s. *Financial Consumer Protection Assistance Mechanism* (FCPAM) – refers to the first-level recourse mechanism for financial consumers who are dissatisfied with a financial product or service of a BSI.

t. *Fraud Management Systems* (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.

u. *FMS Finding* – refers to an FMS notification or alert flagging a transaction as a disputed transaction.

v. *Industry Protocol* – refers to the protocols, conventions, or mechanisms that BSIs shall develop and adopt to effectively undertake temporary holding of disputed funds and coordinated verification, as well as operationalize the provisions of this Section. The protocols shall, at a minimum, meet the expectations set forth under this Section and ensure their effective application.

w. *Initial Holding* – refers to the holding of disputed funds for not more than five (5) calendar days, in accordance with this Section.

x. *Initial Holding Request* – A request initiated by an OFI to initially hold disputed funds for a period of not more than five (5) calendar days.

y. *Originating Financial Institution* (OFI) – refers to a BSI that transmits funds subject of a disputed transaction from one financial account to another financial account within the same or different BSI. The OFI holds the source account of the fund transfer.

z. *Receiving Financial Institution* (RFI) – refers to a BSI that receives or accepts funds subject of a disputed transaction from an OFI. The RFI holds the beneficiary account of the fund transfer.

aa. *Sensitive Identifying Information* – refers to any information that can be used to access an individual's financial account, such as usernames, passwords, bank account details, credit card, debit card, and e-wallet information among other electronic credentials, and other confidential and personal information.

bb. *Source Account* – refers to the financial account where the disputed funds originated.

cc. *Source Account Owner* – refers to the owner of the source account based on the OFI's records.

dd. *Subsequent Receiving Financial Institution* (Subsequent-RFI) – refers to any BSI, other than the OFI and RFI, that receives or accepts funds in the disputed transaction chain. The subsequent-RFI holds the beneficiary account of the subsequent fund transfer.

ee. *Temporary Holding of Disputed Funds* – refers to the authority and responsibility of BSIs to hold disputed funds for a period of not more than thirty (30) calendar days, consisting of the initial and extended holding periods, in accordance with this Section.

Financial Account Protection and Security. BSIs must actively and regularly engage with their client account owners on proactive measures to safeguard their personal and financial information, and ensure the security and integrity of their financial accounts. BSIs must provide regular updates on security best practices, alerts on potential threats, and guidance on how to respond to suspicious activities, including information on proper reporting procedure and channels.

a. BSIs' communications with their account owners may include the following:

(1) Account owners shall take reasonable steps to protect their sensitive identifying information, including usernames, user IDs, passwords, personal identification numbers (PINs), one-time passwords/PINs, and other account credentials or authentication factors. These include using strong and unique passwords, refraining from sharing credentials, using secure devices and secure connections, and exercising caution to avoid falling victim to social engineering

schemes. Account owners are strongly encouraged to regularly update their account credentials, including passwords and PINs, and to do so immediately if there is any suspicion of compromise of their financial account.

(2) Account owners shall immediately report any disputed transaction to their BSIs to facilitate the investigation and perform necessary steps to protect the financial account.

(3) Account owners shall cooperate with BSIs in the investigation and verification of disputed transactions. This includes providing any requested information or documentation necessary to support the investigation and mitigate further risk.

(4) Account owners shall comply with the security practices recommended by BSIs, including activating available features, such as transaction limits, real-time alerts, and multi-factor authentication, to enhance the security of their accounts.

(5) Account owners shall promptly notify BSIs of any changes to their account information, such as contact details, security preferences, or other relevant details, to ensure that account records remain accurate and up to date.

(6) Account owners shall regularly read and monitor notifications from BSIs. This includes reviewing, in a reasonable and prudent manner, statements of account, BSI alerts, transaction records, and any communication regarding account security to promptly identify potential issues or unauthorized activities.

b. In addition to their obligations under laws and *Bangko Sentral* regulations, BSIs shall safeguard the personal and financial information of account owners, and ensure the security and integrity of the account owners' financial accounts through the following:

(1) Conduct regular monitoring and performance assessment of outsourcing arrangements providing direct or indirect access to personal and financial information; and

(2) Identify the types of customers who are more vulnerable to social engineering schemes and who may need a more robust engagement.

Industry Protocol for Temporary Holding of Disputed Funds and Coordinated Verification of Disputed Transactions. BSIs shall collaborate and establish an integrated and holistic industry protocol for the temporary holding of disputed funds and coordinated verification of disputed transactions in accordance with law and the rules and regulations issued by the *Bangko Sentral*.

BSIs shall subscribe and adhere to the industry protocol to ensure timely, efficient, and effective temporary holding of disputed funds and coordinated verification of disputed transactions. The industry protocol shall:

a. Contain clear and specific roles and responsibilities of BSIs in the temporary holding of funds and the coordinated verification process, provided that the minimum requirements set forth in this Section are complied with.

b. Enable timely and streamlined systems and procedures for the temporary holding of funds and the accurate and efficient coordinated verification of disputed transactions, including the maintenance of time logs for the entire process.

c. Implement mechanisms and safeguards to prevent abuse and malicious use of the temporary holding and coordinated verification process.

d. Require prompt notifications to source and beneficiary account owners whose financial accounts are affected by the temporary holding of funds and the coordinated verification process.

e. Identify the minimum documents that are required to initiate, continue, or conclude temporary holding and coordinated verification process among BSIs, and the exceptional instances when these documents may be dispensed with, taking into account the amount of disputed funds, the personal circumstances of the account owners, and other relevant considerations.

f. Institutionalize a secure, real-time or near-real-time, automated system for tracing disputed transactions, with capability to generate and record a visible disputed transaction chain, trigger the temporary holding of disputed funds, and induce timely alerts for involved BSIs.

g. Implement strong measures to safeguard the confidentiality and integrity of information disclosed and shared during coordinated verification and to ensure that use and access to the same is limited to authorized persons and for authorized purposes under this Section.

h. Incorporate a clearly defined mechanism for settling disputes and determining liability for losses among BSIs that may arise from the temporary holding, coordinated verification, and release of disputed funds, and other rules on shared accountability.

i. Include a regular communication plan to inform account owners about the basic responsibilities of parties, the timelines applicable to the temporary holding of disputed funds and the coordinated verification process, among other key messages, to manage expectations of account owners and the general public.

j. Include provisions requiring BSIs to advise their account owners that cooperation in the coordinated verification process is part of their responsibilities under the AFASA, and that the prohibition on waiver of consumer rights under R.A. No. 11765 remains in force.

k. Contain other rules, procedures, and systems necessary to seamlessly conduct an industry-wide temporary holding of funds and coordinated verification process, as well as to operationalize the provisions of this Section.

Prior to its implementation, the industry protocol shall be reviewed by the *Bangko Sentral* to ensure compliance with existing laws, rules and regulations.[2]

Responsibility of BSIs to Temporarily Hold Disputed Funds and Conduct Coordinated Verification. BSIs shall have the authority to temporarily hold disputed funds for a period of not more than thirty (30) calendar days, inclusive of the initial and extended holding periods defined in this Section. The period to hold disputed funds under this Section may be further extended only by a court of competent jurisdiction.

Once the disputed funds in the beneficiary accounts have been held, the equivalent amount shall be considered credited but cannot be withdrawn during the holding period.

[2] The industry protocol must be fully operational within one (1) year from the effectivity of this Circular.

Simultaneously with the temporary holding of disputed funds, BSIs and account owners shall initiate a coordinated verification process to validate a disputed transaction.

For this purpose, all BSIs shall establish and implement their own policies, systems, and procedures for verification of disputed transactions, provided that the same are compliant with the requirements set forth in this Section and conform with the agreed industry protocol. Mechanisms must also be in place to prevent the malicious and abusive use of the temporary holding process.

In accordance with the abovementioned policies, systems, and procedures, involved account owners shall cooperate with BSIs in the investigation and verification of disputed transactions by timely providing requested information and documentation necessary to support the investigation, prove the legitimacy of the transaction, and mitigate further risk.

Initiating the Temporary Holding of Disputed Funds and Coordinated Verification Process. The temporary holding of disputed funds and coordinated verification process are initiated through any of the following triggers:

a. Complaint-initiated holding – a complaint filed by the source account owner, through the 24/7 fraud reporting channel of the OFI's FCPAM, which the OFI shall handle in accordance with the procedures hereunder.

b. FMS-initiated holding – an OFI or RFI's FMS finding.

    (1) For FMS findings involving outgoing transactions, the OFI which flagged the disputed transaction shall proceed in accordance with the procedures hereunder.

(2) For FMS findings involving incoming transactions, the RFI which flagged the disputed transaction shall proceed in accordance with *Appendix 160/Q-104/1105-1*.

c. Request-initiated holding – an initial holding request from an OFI to an RFI or subsequent-RFI.

(1) For initial holding requests based on complaints or FMS findings involving outgoing transactions, the OFI shall proceed in accordance with the procedures hereunder.

(2) For initial holding requests based on the OFI's fraud investigation and/or risk management policies and procedures that are not covered by any complaint or FMS findings, the OFI shall proceed in accordance with *Appendix 161/Q-105/1105-2*.

BSIs shall keep logs of the actual date and time of receipt of any of the foregoing triggers. These logs shall be used as basis to determine timely compliance by BSIs of their obligations under this Section and liabilities for failure to temporarily hold disputed funds or improper holding of disputed funds, among others.

Procedure for Initial Holding of Disputed Funds. Immediately from receipt of a complaint or FMS finding involving an outgoing transaction, the OFI shall, in accordance with the turnaround time prescribed under the industry protocol, simultaneously:

a. Verify the information received to enable it to identify the disputed transaction and the disputed funds to be subjected to initial holding and coordinated verification process. At the minimum, the BSI shall confirm the unique transaction reference number or transaction identifier, the source account owner and number, the amount of

disputed funds, the mode of transfer or payment transaction, the date and time of the disputed transaction, the RFIs and/or subsequent-RFIs involved, and the beneficiary account owner and number, if known.

For complaint-initiated holding, the OFI shall additionally verify the identity of the person making the complaint and confirm that such person is the source account owner or the latter's authorized representative, in accordance with the OFI's standard operating procedures and the agreed industry protocol.

b. Prepare a disputed transaction report documenting the minimum information necessary to identify the disputed transaction, the disputed funds, and the reasons why the transaction appears to be a disputed transaction.

c. When applicable, perform actions necessary to preserve the integrity of the source account, such as disabling access and/or funds transfer functionality to prevent further disputed transactions.

d. If the disputed funds were transferred to a beneficiary account owner within the same BSI, initially hold the disputed funds for not more than five (5) calendar days.

e. If the disputed funds have been wholly or partially transferred to a different BSI, transmit, using the automated system for tracing of disputed transactions, an initial holding request to all RFIs and subsequent-RFIs identified in the disputed transaction chain to hold the disputed funds for not more than five (5) calendar days from receipt thereof.

f. Upon holding of the disputed funds, if applicable, notify its own beneficiary account owner about the initial holding, together with information on:

(1) The unique transaction reference number or transaction identifier, the amount of disputed funds, the mode of transfer or payment transaction, the date and time of the disputed transaction;

(2) The general reasons for the initial holding of disputed funds;

(3) Consumer rights and how the beneficiary account owner may challenge or request the lifting of the initial holding or substantiate the legitimacy of the disputed transaction; and

(4) The possible extension of the initial holding and the possible consequences for failing to participate in the coordinated verification process or to substantiate the legitimacy of the disputed transaction, such as the debiting of the disputed funds from the beneficiary account and the release thereof to the source account owner.

g. Inform the source account owner of the initial actions taken on the disputed transaction and:

(1) For complaint-initiated holding, the OFI shall generate an acknowledgment of the complaint and provide the source account owner with a case reference number.

(2) For FMS-initiated holding involving outgoing transactions, the OFI shall communicate with the source account owner to verify and investigate whether the latter performed and authorized the disputed transaction. The

OFI shall also provide the source account owner with a case reference number.

In both instances, the source account owner shall be informed that any person who, with malice or in bad faith, reports or files completely unwarranted or false information that results in the temporary holding of funds may be held criminally liable for malicious reporting under Section 11, in relation to Section 16(e), of the AFASA.

h. Participate in the coordinated verification process by tracing and verifying the accuracy, authenticity, and legitimacy of the disputed transaction, and coordinating with the involved BSIs and account owners.

Immediately from receipt of an initial holding request, the RFI or subsequent-RFI shall, in accordance with the turnaround time prescribed under the industry protocol, comply with subparagraph (a) above as to the beneficiary account owner, and subparagraphs (b), (d), (f), and (h) above.

In view of the urgent need to prevent the transfer and/or exfiltration of disputed funds through the financial system, a BSI shall, for purposes of initial holding, have the right to rely on the allegations of the person making the complaint, the FMS finding, or initial holding request as to the circumstances giving rise to the disputed transaction.

Response to Initial Holding Request. Immediately from receipt of the initial holding request and in accordance with the turnaround time prescribed under the industry protocol, the RFI and/or subsequent-RFI shall provide the OFI with information on whether the disputed funds are partially or fully intact, including:

a. Whether the RFI or subsequent-RFI was able to carry out the initial holding of disputed funds in accordance with this Section and the amounts successfully held, if any.

b. Whether the disputed funds sent to the beneficiary account owner have been withdrawn in a manner that prevents the further tracing and holding of disputed funds.

c. Whether the disputed funds sent to the beneficiary account owner have been transferred to a subsequent-RFI.

d. Other relevant information and documents, as may be available.

The OFI shall be responsible for consolidating the information from the responses received from the RFIs and subsequent-RFIs and coordinating future directives for the extended holding of disputed funds, if applicable.

Notice to Source Account Owner of Initial Holding of Disputed Funds. Promptly, and in accordance with the turnaround time prescribed under the industry protocol, the OFI shall provide the source account owner with an update on the complaint, together with information on whether disputed funds were successfully held for not more than five (5) calendar days and the subsequent steps to be taken to extend the initial holding period and, if warranted, to recover the disputed funds.

The OFI shall likewise provide the source account owner with information on other available legal remedies, such as the filing of a complaint with appropriate law enforcement agencies authorized to request information from the *Bangko Sentral* pursuant to the AFASA.

The OFI shall inform the source account owner that the OFI has commenced the coordinated verification process under this Section, which includes the coordination with the RFIs, subsequent-RFIs, CSOs, and account owners, as

appropriate, and the investigation and validation of the disputed transaction.

The notice shall also contain a statement that any person who, with malice or in bad faith, reports or files completely unwarranted or false information that results in the temporary holding of funds may be held criminally liable for malicious reporting under Section 11, in relation to Section 16(e), of the AFASA.

Assessing the Propriety of Extended Holding of Disputed Funds. The initial holding of disputed funds may be extended by not more than twenty-five (25) calendar days from the lapse of the initial holding period, if the nature of the transaction, together with other readily available information on its account owners (e.g., their customer and risk profiles and/or behavioral patterns), gives reasonable grounds to believe that the funds held are likely to be disputed funds, and additional time is needed to complete the coordinated verification process.

In assessing the propriety of extended holding:

a. The OFI shall consider the supporting documents provided by the source account owner and other readily available information on its account owners.

   The source account owner shall submit supporting documents (i.e., sworn complaint, affidavit, police report, or any other supporting document) within the initial holding period, except as may be otherwise provided in the industry protocol. The supporting documents shall detail the circumstances that gave rise to the transaction and the reasons why the source account owner believes that the transaction is probably a disputed transaction.

b. RFI or subsequent-RFI shall consider the extended holding request by the OFI and other readily available information on its account owners.

The OFI shall submit an extended holding request within the initial holding period and in accordance with the industry protocol. The extended holding request shall contain the detailed reasons why the OFI reasonably believes that the transaction is likely to be a disputed transaction.

The extended holding request may be accompanied by supporting documents from the source account owner, relevant FMS findings, investigation reports, or other similar information.

For purposes of extended holding, an OFI, an RFI, or a subsequent-RFI that relies in good faith on the information and documents submitted, as well as other readily available information, when determining the attendant circumstances giving rise to the disputed transaction, shall not be held liable for improper holding of disputed funds.

An RFI or a subsequent-RFI may not extend the holding period without prior submission by the OFI of an extended holding request. However, despite receipt of an extended holding request from the OFI, an RFI or subsequent-RFI is not precluded from making its own independent assessment on the propriety of extending the temporary holding based on other readily available information regarding the account owners.

Procedure for Extended Holding of Disputed Funds. If the OFI finds that extended holding is warranted under this Section, it shall perform the following before the lapse of the initial holding period:

a. Extend the initial holding period by an additional period of not more than twenty-five (25) calendar days if the disputed funds were subjected to temporary holding within its system.

b. Transmit an extended holding request to all RFIs and subsequent-RFIs previously requested to initially hold disputed funds, if applicable.

c. Notify its own beneficiary account owner about the extended holding, together with information on:

(1) The unique transaction reference number or transaction identifier, the amount of disputed funds, the mode of transfer or payment transaction, the date and time of the disputed transaction;

(2) The general reasons for the extended holding of disputed funds;

(3) Consumer rights and how the beneficiary account owner may challenge or request the lifting of the extended holding of disputed funds or substantiate the legitimacy of the disputed transaction; and

(4) The possible consequences of failing to participate in the coordinated verification process and to substantiate the legitimacy of the transaction, such as the debiting of disputed funds from the beneficiary account and the release thereof to the source account owner.

d. Acknowledge receipt of the sworn complaint, affidavit, police report, or other supporting documents submitted, and inform the source account owner that the BSIs involved shall engage in the coordinated verification process in accordance with this Section.

If the RFI or subsequent-RFI finds that extended holding is warranted under this Section, it shall, upon receipt of an extended holding request from the OFI and within the initial holding period, comply with subparagraphs (a) and (c) above.

Response to Extended Holding Request. Immediately from receipt of the extended holding request, and in accordance with the turnaround time prescribed under the industry protocol, the RFI and subsequent-RFI shall provide the OFI with information on the action taken on the extended holding request, and the reasons and justifications for the same, if available.

Notice to Source Account Owner of Extended Holding of Disputed Funds. Upon receipt of the response to the extended holding request, the OFI shall provide the source account owner with information on whether the initial holding of disputed funds was extended and other relevant updates on the status of its investigation and verification.

Remedies of Beneficiary Account Owner. Beneficiary account owners whose funds are subjected to temporary holding may, at any time, challenge the same or request the lifting thereof from their BSIs by providing information, documents, or evidence to substantiate the legitimacy of the disputed transaction, such as, but not limited to, affidavits, sworn statements, police reports, other supporting documents, or evidence on the purpose of the transaction, the relationship of the parties, or the source of funds.

If substantiated, the BSI shall, after evaluation, immediately lift the temporary holding of disputed funds and release the same to the beneficiary account owner, even prior to the lapse of the applicable holding period.

Immediately upon receipt of the lifting request and in accordance with the turnaround time prescribed under the industry protocol, the appropriate BSI must inform its beneficiary account owner of its decision to lift the temporary holding of disputed funds or to continue with the same pending further investigation.

Coordinated Verification Process. All BSIs identified or involved in a disputed transaction chain shall participate in the coordinated verification process, regardless of whether the funds remain in their systems or not.

Once the coordinated verification process is initiated in accordance with this Section, BSIs shall:

a. Trace, verify, and validate the accuracy, authenticity, and legitimacy of a disputed transaction, which may include:

(1) Sharing information with involved BSIs, such as the names of the account owners involved, their address and contact details, the date and time of the transaction, the amount involved, the unique transaction reference numbers, the relevant bank or financial account information and transaction details, and the reasons why the transaction is likely to be legitimate or not;

(2) Sharing and reviewing supporting documents, such as the source account owner's sworn complaint, affidavit, police report, relevant FMS findings, investigation reports, or other similar information;

(3) Timely communicating with other relevant entities, such as authorized or accredited agents and third-party service providers, among others, to obtain additional information necessary and critical to effectively implement the coordinated verification process;

(4) Timely communicating with account owners to obtain additional information or documentation on the purpose of the transaction, the relationship of the parties, the source of funds, or other proofs of the legitimacy or illegitimacy of the disputed transaction;

(5) Investigating customer accounts for known fraud indicators and unusual patterns;

(6) Analyzing transaction patterns and recent account activity for red flags in accordance with common fraud parameters and other indicators;

(7) Verifying the information gathered by cross-checking it against other independent or reliable data sources;

(8) Evaluating the veracity of the claims by considering the nature of the transaction vis-a-vis the account owners' risk profile, behavior, claims, or allegations; and

(9) Other means as may be established by a BSI's policies, systems, and/or the agreed industry protocol.

b. Provide appropriate and timely notification and information to their own account owners whose financial accounts are affected by the coordinated verification process. The timing and manner of sharing information with account owners shall be clearly defined in the industry protocol and the BSI's disclosure and transparency policies and procedures that form part of its Consumer Protection Risk Management System, as defined in

Section 1002/1002-Q of the MORB/MORNBFI (*Duties of BSIs and Authorized Third Parties*).

c. Swiftly and efficiently complete the coordinated verification process from the receipt of a complaint, FMS finding, or initial holding request:

   (1) If funds were successfully held: Within the thirty (30) - calendar day temporary holding period, unless said period is extended by a court of competent jurisdiction.

   (2) If no funds were held: Within thirty (30) calendar days. For meritorious reasons as determined by the OFI in accordance with its risk management policies, the coordinated verification process may be extended, provided that the total period does not exceed sixty (60) calendar days.

d. Release the disputed funds in accordance with this Section.

e. Upon the request of source account owners, provide them with transaction reference numbers or transaction identifiers, information on RFIs or subsequent-RFIs involved, and dates and times of transactions.

Responsibilities of CSOs. All CSOs involved in fund transfers related to a disputed transaction shall actively participate in the coordinated verification process by sharing the necessary information for tracing, holding, and verifying the accuracy, authenticity, and legitimacy of the transaction.

Responsibilities of Other Entities Involved in the Disputed Transaction. All BSIs involved in a disputed transaction shall coordinate with their authorized agents and third-party service providers to ensure timely information

gathering and effective implementation of the coordinated verification process.

Non-Applicability of Secrecy of Bank Deposits and Data Privacy Laws during Coordinated Verification Process. The provisions of R.A. No. 1405, as amended; R.A. No. 6426, or the "Foreign Currency Deposit Act of the Philippines", as amended; R.A. No. 8367, or the "Revised Non-Stock Savings and Loan Association Act of 1997"; and R.A. No. 10173, or the "Data Privacy Act of 2012" shall not apply during the coordinated verification process of a disputed transaction. Notwithstanding the foregoing, information shared during the coordinated verification process shall be handled securely with appropriate safeguards to ensure that disclosure is confined to the scope of said process.

Release of Disputed Funds. Immediately upon the lapse of the initial or extended holding of disputed funds, or at any time upon confirmation of the legitimacy of the disputed transaction as substantiated by the beneficiary account owner or through other means, appropriate BSIs shall lift the temporary holding of disputed funds and release the same to the beneficiary account owner, unless:

a. The period for holding the disputed funds is extended by a court of competent jurisdiction;

b. The beneficiary account owner executes a written waiver of any claim over the disputed funds; or

c. The totality of the information obtained during the coordinated verification process gives rise to a reasonable conclusion that:

    (1) The disputed funds are derived from or are related to money muling, unlawful activities, or illegal sources;

(2) The transaction has no underlying economic purpose;

(3) The disputed funds are derived from social engineering schemes; or

(4) Other grounds similar or analogous to the foregoing.

In cases falling under subparagraphs (b) and (c) above, the BSI holding the disputed funds shall deduct the equivalent amount from the beneficiary account owner and return the same to the BSI of the source account owner immediately upon receipt of the written waiver or completion of the coordinated verification process, as applicable. BSIs involved shall, without undue delay, notify the beneficiary account owner and the source account owner of the release of the funds and the reasons therefor.

The decision of the BSI to release the disputed funds to the beneficiary account owner or source account owner shall be without prejudice to any other legal remedy available to the aggrieved party.

Report to Bangko Sentral on the Temporary Holding of Disputed Funds. All BSIs shall provide the *Bangko Sentral* with a report on the temporary holding of disputed funds. The content and coverage of the report, as well as the timeline, frequency, and manner of reporting, shall be in accordance with *Appendix 162/Q-106/1105-3*.

Execution of Annual Notarized Certification. Within thirty (30) calendar days from end of year, the BSI initiating or effecting the temporary holding of disputed funds shall execute and submit to the appropriate *Bangko Sentral* department a notarized certification that it is compliant with the related requirements of adequate risk management systems and controls as prescribed by the *Bangko Sentral* at the time that it initiated or effected the holding of the funds. This certification

shall be considered as a Category B report in accordance with Sections 171 and 173/171-Q and 172-Q. For stand-alone operators of payment systems, non-submission, erroneous submission, and delayed submission shall be subject to applicable penalties under the MORPS.

Liability for Failure to Temporarily Hold Funds. A BSI that fails to temporarily hold funds subject of a disputed transaction, as required under the AFASA and this Section, shall be liable for loss or damage arising from such failure, including the restitution of the disputed funds to the account owner.

Liability for Improper Holding of Funds. Without prejudice to liabilities under existing laws, a BSI that holds funds subject of a disputed transaction beyond the allowable period, or improperly holds funds, as provided under the AFASA and this Section, shall be subjected to administrative action under R.A. No. 7653, as amended, other related laws, and *Bangko Sentral* rules, regulations, orders, or instructions.

A fund shall be considered improperly held if the BSI holding the disputed funds fails to comply with the procedures and requirements prescribed under this Section.

Malicious Reporting of Disputed Transactions. All BSIs shall minimize exposure to malicious reporting of disputed transactions by, among others, incorporating in their FCPAM forms, systems, and procedures a notification or provision that any person who, with malice or in bad faith, reports or files completely unwarranted or false information that results in the temporary holding of funds shall be liable under Section 11, in relation to Section 16(e), of the AFASA.

Role of the Bangko Sentral Consumer Assistance Mechanism (CAM) and BSP Online Buddy (BOB) in Handling Complaints or Reports on Disputed Transactions. The BSI's FCPAM shall continue to serve as the first-level recourse for account owners with disputed transaction complaints.

The *Bangko Sentral* CAM/BOB remains as the second-level recourse for account owners who have filed disputed transaction complaints with BSIs and are dissatisfied with the BSI's actions on their complaints. Disputed transaction complaints escalated by account owners to the *Bangko Sentral* CAM/BOB shall be processed in accordance with the rules of procedure under Rule III of Circular No. 1169, Series of 2023.

Retention of BSI Records on Disputed Transactions. BSIs shall ensure that all digital and physical information, data, and records related to a disputed transaction shall be maintained in accordance with existing laws, rules and regulations on record management, retention, and disposal.

Safe Harbor Provision. No administrative, criminal, or civil liability shall be imposed against a BSI or its directors, trustees, officers, and employees for holding funds subject of a disputed transaction when done in accordance with this Section.

Enforcement Actions. The *Bangko Sentral* reserves the right to deploy its range of supervisory tools to promote adherence to the requirements set forth in this Section and bring about timely corrective actions and compliance with *Bangko Sentral* directives.

Section 2. *Applicability to Other Non-Bank Financial Institutions (NBFIs)*. Except with respect to credit card transactions that are not covered by this Circular, the provisions under Section 1 hereof on the amendments to MORNBFI (Q-Regulations) shall likewise apply to non-stock savings and loan associations, pawnshops, trust corporations, and other NBFIs, insofar as these are applicable to their operations. This is in accordance with Part Seven of the S-Regulations, Part Six of the P-Regulations, Section 101-T of the T-Regulations, Part Seven of the N-Regulations, and Section 301-M of the M-Regulations, each of which makes a cross-reference to Part Ten of the Q-Regulations, where Section 1006-Q will be incorporated.

Section 3. *Amendments to List of Reports Required from BSIs*. The following entries shall be inserted in Appendix 7 of the MORB and Appendices Q-3, S-2, P-7, T-4, N-1, and M-6 of the MORNBFI:

(a) Appendix 7 of the MORB (for all types of banks):

Category	Form No.	MOR Ref.	Report Title	Frequency	Submission Deadline	Submission Procedure/ E-mail Address
B		Section 1006 (*Report to Bangko Sentral on the Temporary Holding of Disputed Funds*)	Report on Temporarily Held Funds (THF)	Monthly	Every 15th of the month, covering data from the previous reference month	See Appendix 162/ AFASAReport @bsp.gov.ph
B		Section 1006 (*Execution of Annual Notarized Certification*)	Annual Notarized Certification (Temporary Holding)	Annually	Within thirty (30) calendar days from end of year	Specific guidelines to be issued by BSP

(b) Appendix Q-3 of the MORNBFI:

Category	Form No.	MOR Ref.	Report Title	Frequency	Submission Deadline	Submission Procedure
B		Section 1006-Q (*Report to Bangko Sentral on the Temporary Holding of Disputed Funds*)	Report on Temporarily Held Funds (THF)	Monthly	Every 15th of the month, covering data from the previous reference month	See Appendix Q-106/ AFASAReport @bsp.gov.ph
B		Section 1006-Q (*Execution of Annual Notarized Certification*)	Annual Notarized Certification (Temporary Holding)	Annually	Within thirty (30) calendar days from end of year	Specific guidelines to be issued by BSP

(c) Appendices S-2/P-7/T-4/N-1/M-6 of the MORNBFI:

Category	Form No.	MOR Ref.	Report Title	Frequency	Submission Deadline	Submission Procedure
B		Section 1006-Q (*Report to Bangko Sentral on the*	Report on Temporarily Held Funds (THF)	Monthly	Every 15th of the month, covering data from	See Appendix Q-106/ AFASAReport @bsp.gov.ph

		Temporary Holding of Disputed Funds), in relation to Part Seven of the S-Regulations/ Part Six of the P-Regulations/ Section 101-T of the T-Regulations/ Part Seven of the N-Regulations/ Section 301-M of the M-Regulations			the previous reference month	
B		Section 1006-Q (*Execution of Annual Notarized Certification*), in relation to Part Seven of the S-Regulations/ Part Six of the P-Regulations/ Section 101-T of the T-Regulations/ Part Seven of the N-Regulations/ Section 301-M of the M-Regulations	Annual Notarized Certification (Temporary Holding)	Annually	Within thirty (30) calendar days from end of year	Specific guidelines to be issued by BSP

Section 4. *Transitory Provisions.* The following transitory provisions shall be incorporated as footnotes to:

(a) Section 1006/1006-Q/1105 of the MORB/MORNBFI/MORPs:

BSIs shall be given one (1) year from the effectivity of this Circular to develop and fully adopt the industry protocol necessary to operationalize this Section.

Pending full adoption of the industry protocol, BSIs shall employ reasonable efforts to comply with their obligations to trace and hold disputed funds, and engage in coordinated verification of disputed transactions, under R.A. No. 12010 or the Anti-Financial Account Scamming Act (AFASA).

BSIs shall be given six (6) months from the effectivity of this Circular to adopt such interim arrangements, mechanisms, or protocols that shall be implemented until full adoption of the industry protocol, provided that the temporary holding of disputed funds during this transitory period shall conform with the initial and extended holding periods as defined in the regulations under this Section.

(b) Appendix 162/Q-106/1105-3 of the MORB/MORNBFI/MORPs:

The *Guidelines on the Submission of Report on Temporary Holding of Disputed Funds* (Guidelines) shall take effect one (1) year from the effectivity of this Circular.

The BSIs' first report shall be submitted to the *Bangko Sentral* on the 15th day of the second month following the effectivity of the Guidelines.

The *Bangko Sentral* reserves the right to require a BSI to submit such report even prior to the effectivity of the Guidelines.

Section 5. *Effectivity Clause.* This Circular shall take effect fifteen (15) calendar days after its publication in the Official Gazette or in a newspaper of general circulation.

APPENDIX 160/Q-104/1105-1
(Annex A of Circular)

Incoming Disputed Transactions Flagged by Receiving Financial Institution's Fraud Management System
(Appendix to Section 1006/1006-Q/1105 on Initiating the Temporary Holding of Disputed Funds and Coordinated Verification Process)

FMS-Initiated Holding Involving Incoming Transactions. An RFI may temporarily hold disputed funds and initiate coordinated verification of disputed transactions under Section 1006/1006-Q/1105 when its FMS detects an incoming transaction that appears to be a disputed transaction.

Procedure for Initial Holding of Disputed Funds. Immediately from receipt of an FMS finding involving incoming disputed transactions, an RFI shall, in accordance with the turnaround time prescribed under the industry protocol, simultaneously:

a. Verify the information received to enable it to identify the disputed transactions and the disputed funds to be subjected to initial holding and the coordinated verification process. At the minimum, the RFI shall confirm the unique transaction reference number or transaction identifier, the beneficiary account owner and number, the amount of disputed funds, the mode of transfer or payment transaction, the date and time of the disputed transaction, the OFI involved, and the source account owner and number, if known.

b. Prepare a disputed transaction report, documenting the minimum information necessary to identify the disputed transaction, the disputed funds, and the reasons why the transaction appears to be a disputed transaction.

In view of the urgent need to prevent the transfer and/or exfiltration of disputed funds through the financial system, the RFI shall, for purposes of initial holding, have the right to rely on the FMS finding as to the attendant circumstances giving rise to the disputed transaction.

c. Initially hold the disputed funds transferred to the beneficiary account owner for not more than five (5) calendar days.

d. Notify the beneficiary account owner about the initial holding, together with information on:

   (1) The unique transaction reference number or transaction identifier, the amount of disputed funds, the mode of transfer or payment transaction, the date and time of the disputed transaction;

   (2) Consumer rights and how the beneficiary account owner may challenge or request the lifting of the initial holding or substantiate the legitimacy of the disputed transaction; and

   (3) Information on the possible extension of the initial holding and the possible consequences for failing to participate in the coordinated verification process or to substantiate the legitimacy of the disputed transaction, such as the debiting of the disputed funds from the beneficiary account owner and the release thereof to the source account owner.

e. Immediately notify the OFI that the RFI's FMS flagged circumstances that give reasonable grounds to believe that the transaction originating from the OFI may be a disputed transaction, and provide:

(1) Information sufficient for the OFI to identify the disputed transaction and to verify the same with its source account owner;

(2) Information on whether the disputed funds were successfully held, or were withdrawn, or transferred to a subsequent-RFI;

(3) Information on the subsequent steps to be taken to extend the initial holding period and, if warranted, to recover the disputed funds; and

(4) Other relevant information and documents, as may be available.

f. Participate in the coordinated verification process by tracing and verifying the accuracy, authenticity, and legitimacy of the disputed transaction, and coordinating with the involved BSIs and account owners in accordance with Section 1006/1006-Q/1105.

Other Procedures. The extended holding, coordinated verification, and release of disputed funds shall proceed in accordance with Section 1006/1006-Q/1105.

APPENDIX 161/Q-105/1105-2
(Annex B of Circular)

Disputed Transactions Based on Other Information from Originating Financial Institution
(Appendix to Section 1006/1006-Q/1105 on Initiating the Temporary Holding of Disputed Funds and Coordinated Verification Process)

Request-Initiated Holding. In accordance with the policies and procedures set forth in its fraud detection and risk management framework, an OFI may request the temporary holding of disputed funds and the coordinated verification of transactions under Section 1006/1006-Q/1105, not based on complaint or FMS finding, when it has reasonable ground to believe based on its personal knowledge and/or authentic records that such transaction appears to be a disputed transaction.

Procedure for the OFI on the Initial Holding of Disputed Funds. An OFI requesting the initial holding of disputed funds shall, in accordance with the turnaround time and procedures prescribed under the industry protocol:

a. Identify the disputed transaction and the disputed funds to be subjected to initial holding and coordinated verification. At the minimum, the OFI shall confirm the unique transaction reference number or transaction identifier, the amount of disputed funds, the mode of transfer or payment transaction, the date and time of the disputed transaction, the RFIs and/or subsequent-RFIs involved, and the affected account owners and numbers.

b. Prepare a disputed transaction report documenting the information necessary to identify the disputed transaction, the disputed funds, and the reasons why the transaction, based on its personal

knowledge and/or authentic records, appears to be a disputed transaction.

c. When applicable, perform actions necessary to preserve the integrity of the source account, such as disabling access and/or transfer functionality to prevent further disputed transactions.

d. Transmit, using the automated system for tracing of disputed transactions or through other means as provided in the industry protocol, an initial holding request to all RFIs and subsequent-RFIs identified in the disputed transaction chain to initially hold the disputed funds for not more than five (5) calendar days from receipt thereof.

e. Where relevant, immediately verify the disputed transactions with the source account owner in accordance with Section 1006/1006-Q/1105.

f. Participate in the coordinated verification process by tracing and verifying the accuracy, authenticity, and legitimacy of the disputed transaction, and coordinating with the involved BSIs and account owners in accordance with Section 1006/1006-Q/1105.

Procedure for the RFI or Subsequent-RFI on the Initial Holding of Disputed Funds. Immediately from receipt of an initial holding request, the RFI or subsequent-RFI shall, in accordance with the turnaround time prescribed under the industry protocol, simultaneously:

a. Verify the information received to enable it to identify the disputed transaction and the disputed funds to be subjected to initial holding and coordinated verification process.

b. Prepare a disputed transaction report documenting the minimum information necessary to identify the disputed transaction, the disputed funds, and the

reasons why the transaction appears to be a disputed transaction.

In view of the urgent need to prevent the transfer and/or exfiltration of disputed funds through the financial system, the RFI or subsequent-RFI shall, for purposes of initial holding, have the right to rely on the initial holding request as to the attendant circumstances giving rise to the disputed transaction.

c. Initially hold the disputed funds for not more than five (5) calendar days.

d. Upon holding of the disputed funds, notify its own beneficiary account owner in accordance with Section 1006/1006-Q/1105.

e. Respond to the initial holding request in accordance with Section 1006/1006-Q/1105 and the turnaround time prescribed under the industry protocol.

f. Participate in the coordinated verification process by tracing and verifying the accuracy, authenticity, and legitimacy of the disputed transaction, and coordinating with the involved BSIs and account owners.

Other Procedures. The extended holding, coordinated verification, and release of disputed funds shall proceed in accordance with Section 1006/1006-Q/1105.

APPENDIX 162/Q-106/1105-3
(Annex C of Circular)

Guidelines on the Submission of Report on Temporary Holding of Disputed Funds

(Appendix to Section 1006/1006-Q/1105 on Report to Bangko Sentral on the Temporary Holding of Disputed Funds)

Scope. These Guidelines shall apply to all *Bangko Sentral*-Supervised Institutions (BSIs) that temporarily hold funds subject of disputed transactions, in accordance with Section 7 of R.A. No. 12010, or the Anti-Financial Account Scamming Act (AFASA), and its implementing rules and regulations.

Report Content. A BSI shall promptly notify the *Bangko Sentral* whenever it temporarily holds funds that are the subject of a disputed transaction.

The report shall be called **Report on Temporarily-Held Funds (THF).** The required information, definitions, formats, values, and field requirements are provided below. These details are arranged according to their order on the **Data Entry Template (DET)**. All information tagged as "Conditional" may be left blank only if the information is unavailable in the reporting BSI.

Field Name	Definition	Format	Value	Field Requirement
Reporting BSI	The Bank Code of the BSP Supervised Institution (BSI) who is submitting the Report	Numeric	Assigned BSI per Reporting Entity	Mandatory
Branch of Account	The Branch Code of the specific Branch of the Reporting BSI where the account subjected to holding of funds is maintained	Numeric	>=0, Positive integers	Mandatory

Field Name	Definition	Format	Value	Field Requirement
Reference No.	Unique Reference Number per Case (Should be unique per case) Convention: THF_YYYYMMDD_Bank Code_0000001	Text	Text	Mandatory
Trigger to Hold Funds	The main trigger for the Reporting BSI to initiate holding of funds Choose only One from these options: • Complaint filed by Source Account Owner • BSI's own Fraud Management System (Outgoing Transactions) – flagged by Originating Financial Institution • BSI's own Fraud Management System (Incoming Transactions) – flagged by Receiving Financial Institution • Information from another BSP Supervised Institution (Based on Complaint or FMS Finding) – Initial Holding Request based on complaint or FMS	Text	Text	Mandatory

Field Name	Definition	Format	Value	Field Requirement
	• Information from another BSP Supervised Institution (Based on Other Grounds) – Initial Holding Request not based on complaint or FMS			
Status of Held Funds at the Time of Reporting	The Status of the temporarily held funds at the time of reporting: Choose only One from these options: • Ongoing - Funds remain on hold • Released to Source Account Owner - Amount on hold was released to the Source Account Owner • Released to Beneficiary Account Owner - Amount on hold was released to the Beneficiary Account Owner	Text	Text	Mandatory
Date of Receipt/ Transmission of Trigger to Hold Funds	Date when the trigger to initiate the holding of funds was received by, or transmitted to, the Reporting BSI "Date of Receipt/ Transmission" can be any of the following, whichever Trigger to Hold Funds came first: • Date of receipt of information or Initial Holding Request from another BSI • Date of transmission of finding/	Numeric	Date Convention: YYYYMMDD	Mandatory

Field Name	Definition	Format	Value	Field Requirement
	notification/ alert through BSI's own FMS • Date of receipt of complaint from Source Account Owner			
Time of Receipt/ Transmission of Trigger to Hold Funds	Exact Time when the trigger to initiate the holding of funds was received by, or transmitted to, the Reporting BSI "Time of Receipt/ Transmission" can be any of the following whichever Trigger to Hold Funds came first: • Time of receipt of information or Initial Holding Request from another BSI • Time of transmission of finding/ notification/ alert through BSI's own FMS • Time of receipt of complaint from Source Account Owner	Numeric	Time Convention: HH:MM:SS	Mandatory
Date of Initiation of Hold	Date when the Reporting BSI initiated the holding of funds	Numeric	Date Convention: YYYYMMDD	Mandatory
Time of Initiation of Hold	Exact Time when the Reporting BSI initiated the holding of funds	Numeric	Time Convention: HH:MM:SS	Mandatory
Date of Release of Held Funds	Date when the Reporting BSI released the held funds to the Source/Beneficiary Account Owner	Numeric	Date Convention: YYYYMMDD	Conditional
Time of Release of Held Funds	Exact Time when the Reporting BSI released the held funds to the Source/Beneficiary Account Owner	Numeric	Time Convention: HH:MM:SS	Conditional
Amount on Hold in	Amount that is temporarily on hold in Original Currency	Numeric	>=0, Positive integers	Mandatory

<table>
<tr><th>Field Name</th><th>Definition</th><th>Format</th><th>Value</th><th>Field Requirement</th></tr>
<tr><td>Original Currency</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Original Currency of Amount on Hold</td><td>Original Currency of the amount that is temporarily on hold

Choose Currency Code from the list below:

<table><tr><th>Currency Code</th><th>Currency Unit</th></tr><tr><td>PHP</td><td>Philippine Peso</td></tr><tr><td>USD</td><td>U.S. Dollar</td></tr><tr><td>JPY</td><td>Japanese Yen</td></tr><tr><td>GBP</td><td>British Pound</td></tr><tr><td>HKD</td><td>Hongkong Dollar</td></tr><tr><td>CHF</td><td>Swiss Franc</td></tr><tr><td>CAD</td><td>Canadian Dollar</td></tr><tr><td>SGD</td><td>Singapore Dollar</td></tr><tr><td>AUD</td><td>Australian Dollar</td></tr><tr><td>BHD</td><td>Bahraini Dinar</td></tr><tr><td>KWD</td><td>Kuwaiti Dinar</td></tr><tr><td>SAR</td><td>Saudi Arabian Riyal</td></tr><tr><td>BND</td><td>Bruneian Dollar</td></tr><tr><td>IDR</td><td>Indonesian Rupiah</td></tr><tr><td>THB</td><td>Thai Baht</td></tr><tr><td>AED</td><td>Emirati Dirham</td></tr><tr><td>EUR</td><td>Euro</td></tr><tr><td>KRW</td><td>South Korean Won</td></tr><tr><td>CNY</td><td>Chinese Yuan</td></tr></table>
If the Original Currency is not included in the defined Currency Codes, input CCC; [original currency unit in full].</td><td>Text</td><td>Text</td><td>Mandatory</td></tr>
</table>

Field Name	Definition	Format	Value	Field Requirement
Amount on Hold in PHP	Amount that is temporarily on hold in PHP equivalent at the time of reporting, based on BSP Reference Exchange Rates Bulletin published in BSP website	Numeric	>=0, Positive integers	Mandatory
Account Number Subject to Hold	Account Number subject to the temporary hold of funds	Text	Text	Mandatory
Last Name of Account Owner Subject to Hold	Last Name of Account Owner subject to the temporary hold of funds For Corporate Accounts, use registered Corporate Account Name recorded in the BSI	Text	Text	Mandatory
First Name of Account Owner Subject to Hold	First Name of Account Owner subject to the temporary hold of funds For Joint Accounts, Names should be separated by commas May be left blank only if the Account Subject to Hold is a Corporate Account	Text	Text	Conditional
Middle Name of Account Owner Subject to Hold	Middle Name of Account Owner subject to the temporary hold of funds For Joint Accounts, Names should be separated by commas Mandatory if information is available in the Reporting BSI	Text	Text	Conditional
Address of Account Owner Subject to Hold	Address of Account Owner subject to the temporary hold of funds Format: House Number, Street/Block, Barangay, Town, City/Municipality For Joint Accounts with different addresses, addresses should be separated by commas	Text	Text	Mandatory

<table>
<tr><th>Field Name</th><th>Definition</th><th>Format</th><th>Value</th><th>Field Requirement</th></tr>
<tr><td>Contact Number of Account Owner Subject to Hold</td><td>Contact Number of Account Owner subject to the temporary hold of funds

For Joint Accounts and those that have multiple contact numbers, contact numbers should be separated by commas

Mandatory if information is available in the Reporting BSI</td><td>Text</td><td>Text</td><td>Conditional</td></tr>
<tr><td>Email Address of Account Owner Subject to Hold</td><td>Email Address of Account Owner subject to the temporary hold of funds

For Joint Accounts and those that have multiple e-mail addresses, e-mail addresses should be separated by commas

Mandatory if information is available in the Reporting BSI</td><td>Text</td><td>Text</td><td>Conditional</td></tr>
<tr><td>Name of Originating Financial Institution</td><td>Complete Legal/Registered Name of the Originating Financial Institution (Do Not Abbreviate)

Mandatory if “Trigger to Hold Funds” field shows:
• “Information from another Bangko Sentral Supervised Institution (BSI)” or
• “Complaint filed by Source Account Owner”</td><td>Text</td><td>Text</td><td>Conditional</td></tr>
<tr><td>Amount Under Dispute in Original Currency</td><td>Full amount of funds under dispute in its Original Currency</td><td>Numeric</td><td>>=0, Positive integers</td><td>Mandatory</td></tr>
<tr><td>Original Currency of Amount Under Dispute</td><td>Original Currency of the amount under dispute

Choose Currency Code from the list below:<table><tr><td>Currency Code</td><td>Currency Unit</td></tr><tr><td>PHP</td><td>Philippine Peso</td></tr></table></td><td>Text</td><td>Text</td><td>Mandatory</td></tr>
</table>

Field Name	Definition	Format	Value	Field Requirement
	<table><tr><td>USD</td><td>U.S. Dollar</td></tr><tr><td>JPY</td><td>Japanese Yen</td></tr><tr><td>GBP</td><td>British Pound</td></tr><tr><td>HKD</td><td>Hongkong Dollar</td></tr><tr><td>CHF</td><td>Swiss Franc</td></tr><tr><td>CAD</td><td>Canadian Dollar</td></tr><tr><td>SGD</td><td>Singapore Dollar</td></tr><tr><td>AUD</td><td>Australian Dollar</td></tr><tr><td>BHD</td><td>Bahraini Dinar</td></tr><tr><td>KWD</td><td>Kuwaiti Dinar</td></tr><tr><td>SAR</td><td>Saudi Arabian Riyal</td></tr><tr><td>BND</td><td>Bruneian Dollar</td></tr><tr><td>IDR</td><td>Indonesian Rupiah</td></tr><tr><td>THB</td><td>Thai Baht</td></tr><tr><td>AED</td><td>Emirati Dirham</td></tr><tr><td>EUR</td><td>Euro</td></tr><tr><td>KRW</td><td>South Korean Won</td></tr><tr><td>CNY</td><td>Chinese Yuan</td></tr></table> If the Original Currency is not included in the defined Currency Codes, input **CCC; [original currency unit in full]**.			
Account Number of Source Account	Account Number from which the disputed funds originated Mandatory if "Trigger to Hold Funds" field shows: • "Information from another Bangko Sentral Supervised Institution (BSI)" or • "Complaint filed by Source Account Owner"	Text	Text	Conditional

Field Name	Definition	Format	Value	Field Requirement
Last Name of Account Owner of the Source Account	Last Name of Account Owner from which the disputed funds originated For Corporate Accounts, use registered Corporate Account Name recorded in the BSI Mandatory if "Trigger to Hold Funds" field shows: • "Information from another Bangko Sentral Supervised Institution (BSI)" or • "Complaint filed by Source Account Owner"	Text	Text	Conditional
First Name of Account Owner of the Source Account	First Name of Account Owner from which the disputed funds originated For Joint Accounts, Names should be separated by commas Mandatory if "Trigger to Hold Funds" field shows: • "Information from another Bangko Sentral Supervised Institution (BSI)" or • "Complaint filed by Source Account Owner" May be left blank only if the Account is a Corporate Account	Text	Text	Conditional
Middle Name of Account Owner of the Source Account	Middle Name of Account Owner from which the disputed funds originated For Joint Accounts, Names should be separated by commas Mandatory if "Trigger to Hold Funds" field shows: • "Information from another Bangko Sentral Supervised Institution (BSI)" or • "Complaint filed by Source Account Owner"	Text	Text	Conditional

Field Name	Definition	Format	Value	Field Requirement
	Mandatory if information is available in the Reporting BSI			

Reporting Frequency. The BSI shall submit the THF Report **every 15th of the month**, covering the data from the **previous reference month**.

A BSI is not required to submit a THF Report if no funds were held during the reference month. Non-submission shall be deemed as the BSI's formal declaration that it held no funds.

Reporting Template. The BSI shall use the prescribed **DET** and **Control Prooflist** (CP) when reporting to the *Bangko Sentral*. The prescribed DET, CP, and User Guide can be downloaded from www._____.

Submission Procedures. The DET shall be certified correct through the CP and shall be signed by the BSI's President/Chief Executive Officer and Chief Compliance Officer or officers of equivalent rank, duly designated by the BSI's Board of Directors.

The DET and CP files shall be electronically transmitted on or before the prescribed deadline to AFASAReport@bsp.gov.ph using the subject line [THFR]_[BSI NAME]_[DATE OF REPORT format: YYYYMMDD]_[Series format: XXXX].

For example:

To: AFASAReport@bsp.gov.ph
Subject: THFR_ABC BANK_20250106_0001

The **DET** file shall be in **Excel** format while the **CP** file shall be in **Portable Document Format**, submitted using the prescribed file naming convention, as illustrated below:

File Naming Convention for CP:
[CP]_[BSI NAME]_[DATE OF REPORT format: YYYYMMDD]_[Series format: XXXX]

File Naming Convention for DET:
[DET]_[BSI NAME]_[DATE OF REPORT format: YYYYMMDD]_[Series format: XXXX]

For example:

CP_ABC BANK_20250106_0001.pdf
DET_ABC BANK_20250106_0001.xls

The BSI may attach one or more DET files with the corresponding CP files in a single submission, provided that the total combined size does not exceed 25 megabytes. The file size limit refers to the total size of all elements in the email, including text, headers, and attachments. Submissions that exceed the prescribed size limit will be automatically rejected by the system.

If the submission exceeds the maximum allowable file size, the BSI may send multiple submissions, provided that submissions for the reference period must be emailed no later than the prescribed reporting deadline.

BSIs shall use only the email addresses officially registered with the *Bangko Sentral* Department of Supervisory Analytics (DSA) when electronically submitting the DET and CP files. Email submissions shall be automatically acknowledged by the system.

Submissions that do not receive an automatic acknowledgement shall be considered unsubmitted. It shall be deemed as non-submission of the THF Report for the reference month.

The DET and CP files must be encrypted and transmitted using Transport Layer Security to ensure the confidentiality and integrity of the information contained within.

Updating of Status of Held Funds. Reporting BSIs shall submit an updated THF Report (DET and CP) not later than the deadline for the next reporting period to update the status of funds placed on temporary hold and previously reported as **"Ongoing" in the "Status of Held Funds at the Time of Reporting"** column.

As appropriate, the **"Status of Held Funds at the Time of Reporting"** column must be updated from **"Ongoing"** to **"Released"**, and the **"Date of Release of Held Funds"** and **"Time of Release of Held Funds"** column should be populated. To ensure that the update is accurately reflected, the **Reference Number** used in the previous report must be retained in the updated report.

Compliance with Reporting Standards. The THF Report shall be considered as a Category B report in accordance with Sections 171 and 173/171-Q and 172-Q. For stand-alone operators of payment systems, non-submission, erroneous submission, and delayed submission shall be subject to applicable penalties under the MORPS.

Inquiries. Queries regarding the THF Report, its related regulations and guidelines may be sent to the *Bangko Sentral's* **Consumer Account Protection Office** via email to capoinquiry@bsp.gov.ph following the prescribed subject line: **[INQUIRY] THF REPORT [BSI Name).**

FOR THE MONETARY BOARD:

(sgd.)
ELI M. REMOLONA, JR.
Governor

READ MORE
ABOUT AFASA:

WWW.BSP.GOV.PH

KNOW MORE: bit.ly/4mNhZYZ

"BSP IN FOCUS: PAANO MAKATUTULONG ANG AFASA SA PAGLABAN SA SCAMS"