BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE 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:

Digitally signed by Eli M. Remolona Jr.
Date: 2025.05.30 19:30:10 +08'00'

ELI M. REMOLONA, JR.
Governor