



BANGKO SENTRAL NG PILIPINAS

OFFICE OF THE DEPUTY GOVERNOR | FINANCIAL SUPERVISION SECTOR

MEMORANDUM NO. M-2026-003

To : **All BSP Supervised Financial Institutions (BSFIs)**

Subject : **Reminders on Sound Risk Management Practices when Dealing with Virtual Asset Service Providers (VASPs)**

Consistent with Parts 9 and 2 of the Manual of Regulations for Banks (MORB) and Manual of Regulations for Non-Bank Financial Institutions – M regulations (MORNBFI – M), respectively, BSFIs are reminded to ensure the soundness and adequacy of their risk management policies and practices when dealing with VASPs. BSFIs, at the onset of their relationship with counterparties (i.e., whether local or offshore VASPs and other offshore counterparty institutions) are expected to perform appropriate level of due diligence, exercise extra caution and vigilance, as well as enhanced due diligence (EDD), when necessary, in accordance with their Money Laundering and Terrorist Financing Prevention Program (MTPP). Therefore, to promote consumer protection and financial integrity, BSFIs are expected to observe the following:

1. Deal only with:
 - a. VASPs that are duly registered with and authorized by the Bangko Sentral ng Pilipinas (BSP).
 - b. Crypto Asset Service Providers (CASPs) that are duly registered with and authorized by the Securities and Exchange Commission (SEC).
 - c. Offshore VASPs that are duly registered/licensed/authorized to operate as a VASP or CASP in their home country.
 - d. Other foreign counterparties that are duly registered and/or licensed in their home country.

BSFIs are expected to require the submission of proof of registration (e.g., Certificate of Registration or Certificate of Authority) with the BSP, the SEC, and the Anti-Money Laundering Council (AMLC), or its equivalent in foreign jurisdictions, and independently validate vis-à-vis the list of registered BSFIs and covered persons in the BSP and AMLC websites, and publicly available and reliable list of registered/licensed institutions in foreign jurisdictions.

Dealings, transactions, and/or business relationships with VASPs and other foreign counterparties, whether local or offshore, that are neither registered with nor authorized by the BSP, the SEC, the AMLC, or by any other equivalent competent regulatory/supervisory agencies locally and abroad (i.e., unlicensed, unauthorized, or unregistered VASPs and institutions) are strictly prohibited.

Direct access of retail customers residing in the Philippines, both natural or juridical persons, to offshore VASPs, whether licensed or unlicensed/unregistered in their home countries, unless these are registered with the BSP or the SEC, is not allowed.

2. Conduct risk assessment of the VASPs and other counterparties to identify, understand and assess money laundering/terrorism financing/proliferation financing (ML/TF/PF) risks arising from their operations and apply appropriate standard of due diligence. The risk assessment should consider relevant factors such as business operations, AML/ Counter Terrorist and Proliferation Financing (CTPF) processes and controls, types of customers, product/service offered, distribution channels, jurisdictions they are exposed to, expected

account activity, and results of the national/sectoral AML and CTPF risk assessment where those counterparties operate.

3. Perform an appropriate level of due diligence and EDD on counterparties, as warranted, which includes, among others:
 - a. Obtaining proof of current company registration, or its equivalent for foreign VASPs and counterparties, with appropriate regulatory agencies;
 - b. Verifying registration with the AMLC, or its equivalent for foreign VASPs and counterparties, to comply with the reporting requirements;
 - c. Scanning for adverse media reports and other negative information on the VASP counterparty, including its owners, officers, beneficial owners, among others;
 - d. Verifying and determining whether the offshore VASP can comply with the FATF Recommendation 16 on Payment Transparency¹;
 - e. Gather information and fully understand the nature of business, the reputation, and the quality of supervision over its counterparty, including whether it has been subjected to ML/TF/PF investigation or regulatory action; and
 - f. Obtaining information as to whether AML/CFT training is provided to staff, and details on the record-keeping policies, and conducting validation procedures as provided under existing rules and regulations.
4. Perform continuing account and transaction monitoring, which includes, but is not limited to:
 - a. Proactively monitoring transactions, based on appropriate parameters or alert scenarios that capture their financial profile and behavioral account activities, and identify unusual movements of funds or transactions for further investigation and determination if filing of a suspicious transaction report (STR) is warranted. Similarly, there should be a transaction monitoring system for personal accounts of the owners, directors, principal officers, and ultimate beneficial owners of the VASP and foreign counterparties;
 - b. Periodically updating the counterparty records/information and risk assessment, including sanction screening, based on risk and materiality, to ensure that their risk profile remains current and relevant;
 - c. Establishing policies and guidelines, with defined criteria or grounds for termination of business relationship as a result of ongoing monitoring. This shall cover, but not limited to, material non-compliance with AML/CTPF obligations, the review of account relationships once a counterparty VASP becomes the subject of a suspicious transaction report, among others;
 - d. Strengthening transaction monitoring to detect unusual patterns linked to VA dealings (in line with BSFI's obligation to monitor accounts for suspicious activity); and
 - e. Implementing appropriate controls or limits based on the institution's risk appetite (e.g., limiting large transfers to unknown offshore crypto exchanges unless certain conditions are met [e.g. verified source of funds], allow such transfers with robust monitoring mechanisms).
5. Throughout the business relationship, BSFIs shall adopt appropriate risk identification and mitigation measures in line with FATF Recommendation 15 and adopt other risk-based measures (e.g., cybersecurity and anti-fraud measures) to ensure continuing compliance with the above requirements.

¹ Previously known as the Travel Rule

BSFIs are further reminded that violation of any of the rules provided in Parts 9 and 2 of the MORB and MORNBFI - M, respectively, shall be subject to applicable sanctions and penalties provided under Sections 941 and Part 9 of the MORB and MORNBFI-Q regulations, respectively.

This supersedes the provisions under BSP Memorandum M-2019-021 dated 23 July 2019.

For guidance and strict compliance.

Digitally signed by
 Judith E. Sungsaï
Date: 2026.01.30
17:09:39 +08'00'
JUDITH E. SUNGSAI
Sector-in-Charge

30 January 2026