

Vietnam: Updates to Banking, AML and Crypto Regulations

Amendments expand crypto-asset AML oversight, strengthen customer due diligence and SBV supervision, and permit a new bank role in bond markets.

In brief

On 24 August 2026, the National Assembly passed Law No. 23/2026/QH16, amending the Law on the State Bank of Vietnam, the Law on Anti-Money Laundering ("**AML Law**") and the Law on Credit Institutions ("**Law No. 23**"). Law No. 23 brings crypto-asset services within the AML reporting framework and introduces 15 crypto-specific suspicious transaction indicators. It also expands customer due diligence requirements, particularly for legal arrangements, strengthens the State Bank of Vietnam (SBV)'s supervisory powers, and expressly permits commercial banks to act as security-asset management agents for corporate bonds. Law No. 23 will take effect from 1 December 2026.

Key takeaways

Key highlights of Law No. 23 are as follows:

- **The SBV's supervisory and prudential powers are strengthened:** The SBV may apply institution-specific prudential ratios and require supervised entities to implement its recommendations and risk and operational safety warnings.
- **Expanded KYC for legal arrangements:** Beneficial ownership and CDD requirements are expanded for entrustment arrangements and other legal arrangements of a similar nature, and persons on whose behalf customers conduct transactions.
- **Crypto-asset services are added to the AML framework:** Crypto-asset services are added to the AML reporting framework, together with 15 crypto-specific suspicious transaction indicators.
- **Greater transparency for entrustment arrangements and similar legal arrangements:** Entrusted parties and persons performing equivalent roles in other legal arrangements of a similar nature must collect and update prescribed information on entrusting parties, beneficiaries, potential beneficiaries, supervisors and persons exercising ultimate control, and retain that information for at least five years after ceasing to participate in the arrangement.
- **Suspicious transaction reporting and reporter protection:** Reporting entities must report transactions where there are reasonable grounds to suspect that the assets involved are proceeds of crime. Law No. 23 also expands recordkeeping obligations and protects persons making truthful reports from liability.
- **New role for commercial banks:** Commercial banks can now act as security-asset management agents for corporate bonds.

Contents

Key takeaways

In more detail

The SBV's supervisory and prudential powers are strengthened
Expanded KYC for legal arrangements
Crypto-asset services are added to the AML framework
Greater transparency for entrustment arrangements and similar legal arrangements
Suspicious transaction reporting and reporter protection
New role for commercial banks

Why this matters

In more detail

The SBV's supervisory and prudential powers are strengthened

Law No. 23 reallocates the existing supervisory functions under Article 57 from the Banking Inspection and Supervision Agency to the SBV. The substantive obligations of the financial institutions remain unchanged: they must provide timely, complete and accurate information and documents; report and provide explanations in relation to recommendations and risk and operational safety warnings; and implement those recommendations and warnings.

More substantively, Law No. 23 expands the SBV's prudential powers. In addition to applying one or more prudential ratios above the prescribed levels, the SBV may, based on the nature and level of risk of each supervised entity, apply one or more ratios different from the prescribed levels to meet socio-economic development requirements. The relevant financial institution must develop and implement a roadmap to ensure compliance with the prescribed levels and remain subject to the SBV's inspection and supervision.

Expanded KYC for legal arrangements

Law No. 23 revises the definition of **"beneficial owner"** to cover one or more natural persons who ultimately own or actually exercise ultimate control over a customer, including a legal arrangement, or over a person on whose behalf the customer conducts a transaction. It also clarifies that customer due diligence is required where there is suspicion that the customer, the customer's transaction or a party related to the transaction is connected with money laundering, including where the transaction has not been completed.

For organizational customers, the required identifying information now expressly includes legal form, head office and any separate business location, organizational identification number (if any), and prescribed information on founders, legal representatives, authorized representatives, directors or general directors, and chief accountants or persons in charge of accounting. Additional requirements include the following:

- Where a customer participates in an entrustment arrangement, the reporting entity must collect prescribed information on the entrusted party, entrusting party, beneficiaries or class of beneficiaries, potential beneficiaries, supervisor (if any), any individual exercising ultimate control over the arrangement, and other relevant persons (if any)
- Equivalent information must be collected for all persons performing corresponding roles where the customer participates in another form of legal arrangement of a similar nature
- Reporting entities must identify and collect prescribed information on life-insurance beneficiaries when they are designated, with verification required at the time of payout
- Where a reporting entity can lawfully connect to and retrieve required information from a national or specialized database, it need not require the customer to provide information already available from that database.

Law No. 23 also updates the documents and data that may be used to verify customers, including electronic identity cards for individuals and electronic identification accounts for organizations and documents relating to legal arrangements. More broadly, reporting entities must establish and fully implement policies and procedures to identify and assess money-laundering risks before offering new products or services, or applying innovative technology to existing products or services.

Crypto-asset services are added to the AML framework

Law No. 23 adds **"crypto-asset services"** to the financial-sector activities covered by Article 4.1 of the AML Law. Accordingly, organizations and individuals providing crypto-asset services are reporting entities and must comply with the AML Law's applicable requirements.

Under the revised suspicious-transaction reporting standard, reporting entities must report to the SBV where there are reasonable grounds to suspect that assets involved in a transaction are proceeds of crime. That assessment is based on analysis of customer and transaction information, including the statutory suspicious indicators and any other indicators identified by the reporting entity. For crypto-asset activities, Law No. 23 introduces the following 15 specific indicators, which crypto-asset service providers should reflect in their customer risk assessments and transaction-monitoring procedures:

- Structuring crypto-asset transactions into multiple amounts below the applicable customer identification or reporting thresholds, or conducting numerous high-value crypto-asset transactions within a short period without a clear business purpose.

- Depositing, transacting and withdrawing crypto-assets in rapid succession shortly after establishing the customer relationship; making an unusually large initial deposit immediately after opening a crypto-asset account; or a previously dormant crypto-asset account suddenly generating transactions of large value or unusual frequency.
- Immediately transferring crypto-assets to multiple crypto-asset service providers in countries or territories identified by the Financial Action Task Force as posing money laundering, terrorist financing, or proliferation financing risks, or in countries or territories that have not enacted or have not fully enacted a legal framework on anti-money laundering, counter-terrorist financing, or counter-proliferation financing applicable to crypto-assets, and to crypto-asset service providers on the Financial Action Task Force's relevant lists, without a reasonable connection to the customer's place of residence or business location.
- Converting crypto-assets into multiple different types of crypto-assets without a reasonable business or investment purpose, or converting crypto-assets into fiat currency under unfavorable pricing conditions, accepting losses, or incurring transaction fees that are unusually high relative to prevailing blockchain network conditions at the time of the transaction.
- Multiple accounts or wallet addresses with no apparent connection transferring crypto-assets to the same wallet address, or a single account transferring crypto-assets to multiple different wallet addresses in comparable amounts in rapid succession over a short period.
- Conducting crypto-asset transactions using features that enhance anonymity, mixing services, or repeatedly converting crypto-assets from a public, transparent distributed ledger into crypto-assets with anonymity-enhancing features, thereby disrupting the ability to trace the transaction.
- Conducting crypto-asset transactions from wallet addresses or crypto-asset service providers that have been identified or flagged by competent authorities as connected to darknet marketplaces trading illegal goods or services, extortion, fraud, illegal online gambling, stolen assets, or other criminal activity.
- A customer accessing a crypto-asset service provider's platform through tools that enable anonymization of identity or IP address, or operating multiple crypto-asset accounts under different identities that show signs of being operated from the same device or IP address.
- A customer refusing or delaying the provision of customer identification documents or information on the source of assets; providing documents that appear falsified or inconsistent; or being unable to reasonably explain the purpose of the transaction, the source of assets, or the relationship with the counterparty.
- A customer's crypto-asset wallet address appearing in public sources of information connected to illegal activity, or crypto-asset deposits and withdrawals having a history of passing through cross-chain bridges assessed as high risk.
- A customer showing signs of holding assets on behalf of another person, being used as an intermediary, or being a victim of fraud, including cases where a customer with limited understanding of crypto-assets conducts transactions of a frequency and value disproportionate to their profile and characteristics, or conducts transactions on the instructions of a third party.
- A customer's source of assets being derived predominantly from initial crypto-asset offerings that lack transparency or show signs of fraud, or the customer's crypto-assets originating directly from mixing services or from crypto-asset service providers with inadequate anti-money laundering controls.
- Transacting with a crypto-asset service provider whose legal status cannot be verified, including providers operating in a country or territory without a legal framework on crypto-assets under the Financial Action Task Force's relevant list, or not appearing on the licensed list of the competent authority of the host country, or having been warned, suspended, or had its operating license revoked by a competent authority.
- Notes or memos accompanying a crypto-asset transaction showing signs connected to illegal activity; a customer frequently changing important identification or authentication information in a manner inconsistent with normal usage behavior; conducting transactions from an IP address inconsistent with previously provided customer information; or repeatedly opening crypto-asset accounts from the same IP address.
- A customer conducting transactions through a crypto-asset service provider headquartered or operating in a country or territory identified by the Financial Action Task Force as posing money laundering, terrorist financing, or proliferation financing risks, or in a country or territory that has not enacted or has not fully enacted a legal framework on anti-money laundering, counter-terrorist financing, or counter-proliferation financing applicable to crypto-assets, and crypto-asset service providers on the Financial Action Task Force's relevant lists concerning crypto-assets.

Greater transparency for entrustment arrangements and similar legal arrangements

The former Article 22 of the AML Law already required entrusted parties to collect, update and retain identifying information on entrusting parties, entrusted parties, beneficiaries, related parties (if any) and individuals exercising ultimate control over an entrustment arrangement, and to provide prescribed information upon request. Law No. 23 retains these core duties but expands and clarifies their scope. Entrusted parties must now expressly collect and update information on beneficiaries or classes of beneficiaries, potential beneficiaries and supervisors (if any). Where a relevant party is a legal person or legal arrangement, the information must also include its basic and beneficial ownership information. Corresponding obligations apply to persons performing equivalent roles in other forms of legal arrangement of a similar nature, and basic information must also be collected on regulated agents or other service providers to the arrangement. The prescribed information must be retained for at least five years after the entrusted party or equivalent person ceases to participate in the arrangement. The revised Article 22 preserves the right of the SBV and other competent state authorities performing AML, investigation, prosecution or adjudication functions to request that information.

Suspicious transaction reporting and reporter protection

Law No. 23 reframes and simplifies the statutory trigger for suspicious transaction reporting. The former Article 26 of the AML Law separately addressed transactions conducted at the request of an accused, defendant or convicted person and transactions reasonably suspected of being connected with money laundering. Under the revised Article 26, a reporting entity must report to the SBV whenever there are reasonable grounds to suspect that assets involved in a transaction are proceeds of crime. The assessment must be based on analysis of customer and transaction information, including the statutory suspicious indicators and any additional indicators identified by the reporting entity.

The recordkeeping obligation is also broadened. Whereas the former Article 38.1 referred in several respects to transactions required to be reported, the revised provision requires reporting entities to retain records relating to all customers and all transactions, including customer identification records; analysis and assessment results concerning customers and transactions; other related information and documents; and statutory transaction reports with their supporting materials. In addition, an entity, organization or individual that truthfully submits a report to a competent authority in accordance with the AML Law is not liable for making that report. Persons who report, denounce or provide information for AML purposes are also entitled to protective measures equivalent to those available to whistleblowers under the law on denunciations.

New role for commercial banks

Law No. 23 adds acting as a security-asset management agent for corporate bonds to the business activities that commercial banks may conduct under Article 114.2 of the Law on Credit Institutions. This role may provide corporate bondholders with greater assurance that the security assets supporting their bonds are administered by a regulated financial institution, while enabling issuers to appoint commercial banks as professional security-asset management agents.

Why this matters

Law No. 23 reshapes Vietnam's banking and AML framework by expanding AML requirements for crypto-asset services and legal arrangements, and strengthening the SBV's prudential powers. The most significant implementation impact will fall on crypto-asset service providers, banks, insurers, securities firms and other reporting entities dealing with complex ownership structures or technology-enabled products. With Law No. 23 taking effect on 1 December 2026, affected organizations should act now to assess gaps in customer data, transaction-monitoring systems, internal policies, product governance and regulatory reporting processes. Early preparation will be critical to achieving operational readiness by the effective date.

Khoi Nguyen Hoang, Trainee, has contributed to this legal update.

Contact Us



Oanh Nguyen
Managing Partner
oanh.nguyen@bakermckenzie.com



Thuy Van Pham
Special Counsel
thuyvan.pham@bakermckenzie.com



Hang Phan
Senior Associate
thiHang.phan@bakermckenzie.com

© 2026 Baker & McKenzie. **Ownership:** This site (Site) is a proprietary resource owned exclusively by Baker McKenzie (meaning Baker & McKenzie International and its member firms, including Baker & McKenzie LLP). Use of this site does not of itself create a contractual relationship, nor any attorney/client relationship, between Baker McKenzie and any person. **Non-reliance and exclusion:** All information on this Site is of general comment and for informational purposes only and may not reflect the most current legal and regulatory developments. All summaries of the laws, regulation and practice are subject to change. The information on this Site is not offered as legal or any other advice on any particular matter, whether it be legal, procedural or otherwise. It is not intended to be a substitute for reference to (and compliance with) the detailed provisions of applicable laws, rules, regulations or forms. Legal advice should always be sought before taking any action or refraining from taking any action based on any information provided in this Site. Baker McKenzie, the editors and the contributing authors do not guarantee the accuracy of the contents and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the contents of this Site. **Attorney Advertising:** This Site may qualify as "Attorney Advertising" requiring notice in some jurisdictions. To the extent that this Site may qualify as Attorney Advertising, PRIOR RESULTS DO NOT GUARANTEE A SIMILAR OUTCOME. All rights reserved. The content of the Site is protected under international copyright conventions. Reproduction of the content of this Site without express written authorization is strictly prohibited.

