New requirements under anti-money laundering laws

On 28 July 2023, the State Bank of Vietnam ("SBV") issued Circular No. 09/2023/TT-NHNN, providing guidelines for implementation of a number of articles of the Law on Anti-Money Laundering 2022 ("Circular 09"). Circular 09 took effect on 28 July 2023; except for regulations on money laundering risk management process, regulations on reporting high value transactions subject to report, regulations on electronic money transfer transaction reporting, and the suspicious transaction reporting forms in Appendix II to this Circular, which shall take effect on 01 December 2023.

In brief, Circular 09 imposes certain new notable requirements as follows:

1. Money laundering risk management process and classification of clients according to money laundering risk levels

(a) Based on the results of assessment and update of money laundering risks, a reporting entity develops and promulgates its own process of money laundering risk management. The process of money laundering risk management must be made subject to the size, scope and specificity of the reporting entity's activities to manage money laundering risks. A process document must contain the following minimum contents:

(i) Determining the scope and objectives of money laundering risk management activities;
(ii) Identifying and assessing the impact of money laundering risks at the reporting entity;
(iii) Classifying clients according to low, medium and high risks of money laundering based on the following factors: clients; products or services clients are using or intend to use; geographical location where clients reside or have their

head offices; and other factors determined and classified by the reporting entity in accordance with the arising reality and specified in the risk management process;
(iv) Process to identify and assess money laundering risks before providing new products or services; existing products and services applying innovative technology;
(v) Risk management process for conducting, rejecting, suspending, post-transaction control or reviewing and reporting suspicious transactions; electronic money transfers, of which information are inaccurate or insufficient as requested; and
(vi) Measures to be applied corresponding to the level of client's money laundering risk, including the frequency of updating, verifying client identification information, and the level of supervising over the client's transactions according to levels of money laundering risk, mitigated and enhanced client identification measures.

(b) For clients with low risk of money laundering, after establishing a relationship with the client for the first time, when applying client identification measures in accordance with the laws on anti-money laundering (AML), the reporting entity is entitled to select application of one or all of the following mitigated client identification measures:

(i) Not collecting information about the purpose and nature of business relationships if through established types of transactions or business relationships, the purpose and nature of business relationships can be determined;
(ii) Reducing the frequency of updating client identification information compared to medium-risk clients; and
(iii) Reducing level of supervising over clients' transactions compared to medium-risk clients.

(c) For clients with medium risk of money laundering, the reporting entity must apply client identification measures in accordance with the provisions of the AML laws.

(d) For clients with a high level of risk of money laundering, in addition to applying client identification measures under the AML laws, the reporting entity must apply enhanced measures, including:

(i) There is management approval from at least one level higher than that applicable to medium-risk clients in terms of establishing or continuing a business relationship with high-risk clients;
(ii) Collecting, updating and verifying additional information of individual clients to serve the assessment and management of client risk, including the following minimum information: Average income per month of the client for at least the last 6 months before the time of assessment; contact information of the agency, organization or owner of the place where the client works or gains the main income (if any); information related to the source of money or the source of assets in the client's transaction;
(iii) Collecting, updating and verifying additional information of institutional clients to serve the assessment and management of client risks, including the following minimum information: manufacturing industry, business sector and service generating main revenue; total revenue in the last 2 years before the time of assessment; information related to the source of money or the source of assets in the client's transaction;
(iv) Collecting, updating, and verifying other additional information (if any) for client risk assessment and management;
(v) Conducting enhanced supervision over client transactions conducted through the reporting entity, business relationships through the application of control measures and selection of transaction samples to check and secure the client's transactions in accordance with the purpose and nature of the client's business relationship with the reporting entity and the client's business activities; promptly detecting suspicious signs and reviewing suspicious transaction reports;

and
(vi) Increasing the frequency of updating client identification information compared to medium-risk clients.

2. Internal regulations on AML

(a) Some contents in the AML internal regulations of the reporting entity being an organization are specifically guided as follows:

(i) Client identification process and procedures include the collection, updating and verification of information according to the provisions of the AML laws and have provisions on cases of identification, know your client (KYC) information, update; decentralize responsibility for identifying clients according to the levels of risk and according to the size, scope and characteristics of the reporting entity;
(ii) The process of money laundering risk management at the reporting entity must include the minimum contents specified in Clause (a), Section 1 above;
(iii) Regulations on storage and confidentiality of information: as per Articles 38 and 40 of the AML Law;
(iv) Provisions on application of provisional measures: as per Article 44 of the AML Law and the Government's Decree detailing a number of articles of the AML Law;
(v) Regulations on reporting and information provision to the SBV and other competent State authorities, including regulations on reporting methods and procedures for reporting and information provision to ensure the time-limit and contents of the report as prescribed by law;
(vi) Regulations on personnel recruitment must include provisions for identifying and selecting recruited personnel to meet job position requirements; training in basic AML knowledge within 6 months from the date of being recruited;
(vii) Content of professional AML knowledge training and improvement, including: provisions of AML laws and internal regulations; responsibility for failure to comply with the provisions of AML laws and internal regulations; money

laundering methods and tricks; money laundering risks related to products and services; and tasks assigned to do by leaders and employees;
(viii) Contents of internal AML audit, including: independently and objectively examining, reviewing and evaluating internal control system, compliance with AML laws and internal regulations; petitioned and proposed measures to improve the effectiveness and efficiency of the AML work. The internal AML audit can be conducted independently or in combination with other contents but must be a separate content in the audit report. In case where the reporting entity is not required to conduct internal audit in accordance with the laws, the reporting entity must ensure the implementation of control over compliance with internal regulations and provisions of AML laws; and
(ix) Contents of responsibilities of individuals and departments involved in the AML work implementation must ensure:
• Assigning a manager of the reporting entity or a person authorized by the manager to be responsible for organizing, directing, and inspecting the compliance with the provisions of the AML laws; and
• Depending on the scale, scope and characteristics of activities, the reporting entity must establish a specialized department (group, division, department) or appoint a person responsible for AML at the head office; assign one or a number of persons or a department to be responsible for AML at the branch or subsidiary of the reporting entity related to the professional AML knowledge (if any).

(b) Reporting entities have the following responsibilities:

(i) Annually, conducting professional AML knowledge training and improvement for leaders and employees related to AML work (including employees assigned tasks directly relating to money and property transactions with clients);
(ii) Annually, reviewing and updating the provisions of the

AML laws, risk management policies and procedures in accordance with the results of the risk assessment on money laundering at the reporting entity and the actual situation of implementation to evaluate internal regulations and consider amending, supplementing and replacing accordingly; send AML internal regulations to the authority performing the AML functions and tasks under the SBV ("AML Authority") within 30 days from the date of promulgation or amendment, supplement to or replacement of AML internal regulations;
(iii) Annually, sending the internal AML audit report at the reporting entity to the AML Authority within 60 days from the end of the fiscal year, except for the reporting entities that are not required to carry out the internal audit as prescribed by law;
(iv) Registering information about the full name, working address, phone number, and email address to contact when necessary of the person in charge of AML or the contact person belonging to this department; the department's email address (if any) to the AML Authority; and
(v) Notifying in writing to the AML Authority when the information specified at point (iv) changes within 15 days from the date of information change.

3. Reporting mode for high-value transactions subject to report

(a) The reporting entity responsible for reporting high-value transactions subject to report according to regulations to the AML Authority by means of electronic data or a written report when a compatible information technology system has not yet been established in service of reporting.

(b) In case where a client pays a large amount of cash in foreign currency to buy Vietnam Dong or makes a cash payment in Vietnam Dong to buy a foreign currency in cash, only the cash payment transaction should be reported.

4. Suspicious transaction reporting mode

(a) When detecting a suspicious transaction as prescribed, the reporting entity is responsible for reporting to the AML Authority:

(i) in paper form according to the prescribed form; or
(ii) by electronic data when a compatible information technology system has been established for reporting by electronic data as prescribed (not applicable in case of detecting a suspicious transaction requested by the client has signs related to the crimes that the reporting entity must report to the competent State authority and the SBV within 24 hours from the time of detection).

(b) The reporting of a suspicious transaction does not depend on the amount of the client's transaction amount, whether the transaction has been completed or not.

(c) The AML Authority is responsible for confirming receipt of a suspicious transaction report by sending an email to the email address of the individual or department responsible for AML or by paper documents, within 5 working days from the date of receiving the suspicious transaction report; exchange opinion with the subject entity on the arising issues (if any).

(d) Organizations and individuals providing accounting services; providing notarization services; providing legal services of lawyers, law-practicing organizations must consider, collect and analyze information to report suspicious transactions when doing business in accounting services; carrying out notarization procedures, and on behalf of clients, preparing conditions for implementation of transactions or performing transactions on transferring land use rights, ownership of houses and other land-attached assets; managing clients' monies, securities or other assets; managing clients' accounts at banks and securities companies; directing and managing the company; and, on behalf of clients participating in M&A activities.

5. Electronic Funds Transfer (“EFT”) transactions in AML

(a) Financial institutions involved in EFT transactions include:

(i) Originating financial institution is the organization that initiates a EFT order and conducts the transfer on behalf of the originator;
(ii) An intermediary financial institution means an organization that receives and transmits an ETF order on behalf of the originating financial institution and the beneficiary financial institution or on behalf of another intermediary financial institution; and
(iii) Beneficiary financial institution is an organization that receives an EFT order directly from the originating financial institution or through an intermediary financial institution and makes payments to the beneficiary.

A domestic financial institution being an originating financial institution that initiates an EFT transaction may only conduct an EFT transaction when the EFT order has complete and accurate information as prescribed by laws on cashless payments and foreign exchange control.

A domestic financial institution that is an intermediary financial institution participating in an EFT transaction must ensure:

(i) Taking measures to identify EFT transactions with incomplete and inaccurate information in accordance with the laws on non-cash payments and foreign exchange control; and
(ii) Take appropriate action including denying or suspending transactions or applying post-transaction controls or reviewing and reporting suspicious transactions for EFT transactions of which information is incomplete or inaccurate in accordance with the laws on non-cash payment and foreign exchange control.

A domestic financial institution that is a beneficiary

financial institution in an EFT transaction must ensure:

(i) Taking measures to identify incomplete and inaccurate electronic money transfers in accordance with the laws on non-cash payments and foreign exchange control; and
(ii) Taking appropriate action including denying or suspending transactions or applying post-transaction controls or reviewing and reporting suspicious transactions for wire transfers, of which information is inaccurate or insufficient in accordance with the laws on non-cash payment and foreign exchange control.

(b) EFT reporting mode:

(i) The reporting entity is responsible for collecting information and reporting to the AML Authority with electronic data as prescribed when conducting an EFT transaction in the following cases:
• An EFT transaction in which all participating financial institutions are located in Vietnam ("Domestic EFT transaction") with a transaction value of VND 500,000,000 or more or equivalent value in a foreign currency; and
• An EFT transaction where at least one of the financial institutions participating in the EFT transaction established and operating in countries and territories outside of Vietnam ("International EFT transactions") with transaction value of USD1,000 or more or in another foreign currency of equivalent value.
(ii) In case where the reporting entity is an intermediary financial institution in the EFT transaction, the report is not required.
(iii) The minimum contents of a report on EFT transaction include the following information:
• Information about the originating financial institution and the beneficiary, including: transaction name of the organization or transaction branch; head office address (or bank code for Domestic EFT transactions, SWIFT code for International EFT transactions); Remittance and transfer

country;
• Information about individual clients participating in EFT transactions: full name; date, month, year of birth; ID card number or Citizen’s identification card number or personal identification number or passport number; entry visa number (if any); registered address of permanent residence or other current residence (if any); nationality (according to transactional documents);
• Information about clients being organizations participating in EFT transactions: full transaction name and abbreviated transaction name (if any); head office address; establishment license number or enterprise code or tax code; the country where the head office is located;
• Transaction information: account number (if any); amount of money; currency; the amount to be converted into Vietnamese Dong (if the transaction currency is a foreign currency); transaction reasons and purposes; trading code; trading day; and
• Other information at the request of the AML Authority to serve the State management on AML from time to time.
(iv) Information about date, month, year of birth, ID card number or Citizen’s identification card number or personal identification number or Passport number, entry visa number (if any); Establishment license number or enterprise code or tax code are optional for:
• Beneficiaries of outbound International EFT transactions; and
• Originators of inbound International EFT transactions.
(v) EFT transactions not subject to report include:
• A money transfer transaction that originates from a transaction using a debit card, credit card or prepaid card to pay for goods and services; and
• Money transfer and payment transactions between financial institutions where both the originator and the beneficiary are financial institutions.

(c) Format and time limit for electronic data reporting:

(i) Format for electronic data reporting:

• The reporting entity establishes a transmission line and connects the communication network with the SBV through the Information Technology Department to send AML reports and information;

• Electronic data reporting is transmitted via transmission lines or communication networks mentioned above. Electronic data reporting must follow the correct data format and file structure according to the guidelines of the AML Authority; and

• A reporting entity permitted to conduct EFTs must build a compatible information technology system in service of electronic data reporting and must have a software system to scan and filter according to black list, alert list, list of politically influential individuals; detect and warn suspicious signs for the purpose of AML.

(ii) Time limit for electronic data reporting:

The reporting entity must submit a report on a transaction with a large value to report and report on an electronic money transfer transaction before 16:00 of the next working day immediately after the transaction occurs. If the report submission date coincides with a public holiday, Tet holiday or weekend, the report submission date is the next working day immediately following the holiday, Tet holiday or weekend.

(iii) Editing and supplementing electronic data reporting:

• When detecting that the report is missing, the reporting entity must provide a written explanation and send an additional report within 1 working day after receiving a written confirmation from the AML Authority. When detecting that the reported information and data sent to the AML Authority have errors, the reporting entity must have a written explanation or an email to explain, correct and resend the report within 1 working day from the date of discovery;

• When the reporting entity receives a notice from the AML Authority about the missing or error of the report, the reporting entity must provide a written explanation or an email to explain, supplement or amend and resend the report

within 7 working days from the date of receiving the notice; and

• When the reporting entity receives a notice from a competent State authority in accordance with the laws, the reporting entity must notify the AML Authority thereof, provide a written explanation, and send the amended or supplemented report after obtaining the written confirmation of the AML Authority.

(iv) The reporting entity must register in writing with the AML Authority the person in charge of the electronic data reporting, including the following information: full name, position, working address, number phone, email address and must notify in writing when there is a change in information about the person in charge of this report.

—