

Special Alert

CIRCULAR 41 - KEY REGULATORY UPDATES FOR E-WALLETS AND INTERMEDIARY PAYMENT SERVICES

January 2026

On 5 November 2025, the State Bank of Vietnam (“**SBV**”) issued Circular No. 41/2025/TT-NHNN (“**Circular 41**”), amending and supplementing a number of provisions of Circular No. 40/2024/TT-NHNN on the provision of intermediary payment services (“**Circular 40**”). While most provisions of Circular 41 take effect as of 5 November 2025, certain provisions relating to the opening of e-wallets, customer authentication, and information provision became effective from 1 January 2026. This article summarizes the key updates under Circular 41.

Ensuring safety in the provision of intermediary payment services

Under Circular 41, intermediary payment services providers (“**IPSPs**”) are required to carry out the procedures for amending and supplementing their licenses in accordance with applicable regulations when they cease to provide one or more intermediary payment services. In addition, such IPSPs must publicly disclose the cessation of the relevant services on their official websites at least three (3) months prior to the intended cessation date.

Furthermore, IPSPs are obligated to conduct regular reviews and ensure that customers are permitted to use only legitimate funding sources, including payment accounts, bank cards, and e-wallets, to execute payment transactions on browsers and applications offering intermediary payment services, in compliance with applicable laws and regulations.

E-wallet opening documentation

Compared to Circular 40, Circular 41 expands the scope of acceptable identification documents for individual customers who are foreign nationals. Accordingly, in addition to passports, foreign individuals may submit other valid identification documents evidencing their personal identity as issued by competent foreign authorities when applying for the opening of an e-wallet.

With respect to documents, information, and data of organizational customers, Circular 41 introduces additional requirements concerning the documents, information, and data of the chief accountant or the person in charge of accounting of the organization (if any). Where an organizational customer uses an electronic identification account, the e-wallet service provider is not required to request documents, information, or data that are already available in such electronic identification account. This amendment is expected to streamline the e-wallet opening process and enhance its efficiency, accuracy, and transparency.

Opening e-wallets via electronic means

With respect to the opening of e-wallets via electronic means, Circular 41 requires e-wallet service providers to ensure the full, detailed, and proper retention and preservation of customer identification documents, information, and data collected during the electronic e-wallet opening and usage process, including, but not limited to:

- customer identification information;
- biometric data of the individual e-wallet holder or the lawful representative of the organization opening the e-wallet;
- audio, images, video recordings, and audio recordings;
- the phone number registered on the e-wallet service application;
- the unique identification information of the transaction device;
- transaction log; and
- results of biometric data verification and matching.

All such information and data must be securely stored, kept confidential, and backed up, ensuring their completeness and integrity for the purposes of inspection, cross-checking, verification of the e-wallet holder during use, handling inquiries, complaints, and disputes, as well as for information provision upon request by competent authorities. The retention period for such information and data must comply with the applicable laws on anti-money laundering and electronic transactions.

The opening of e-wallets via electronic means does not apply to cases where individual customers open e-wallets through their legal representatives or guardians.

Use of e-wallets

Circular 41 permits the withdrawal of funds from an e-wallet to a debit card linked to the e-wallet holder's Vietnamese-dong-denominated account maintained with a partner bank. E-wallet users may also transfer funds from their e-wallets to debit cards linked to Vietnamese-dong-denominated accounts opened at banks or foreign bank branches.

Notably, Circular 41 does not allow e-wallet users to withdraw cash directly from their e-wallets at e-wallet service providers.

E-wallet service providers are responsible for guiding users in the proper use of e-wallets and ensuring that appropriate authentication measures are applied to each type of electronic payment transaction, in accordance with the SBV's

regulations on safety and security in the provision of online banking services.

E-wallet transaction limits

The transaction limit applicable to a customer's personal e-wallet maintained with a single e-wallet service provider (including fund transfers and payment transactions) is capped at VND100 million per month. This limit does not apply to personal e-wallets of individuals who have entered into contracts or agreements with e-wallet service providers to act as merchants or payment acceptance units.

In addition to the above limit, e-wallet service providers are permitted to set additional transaction limits, provided that the aggregate monthly limit does not exceed VND300 million, for the following categories of payment transactions:

- Online payments via the National Public Service Portal;
- Electricity, water, and telecommunications services
- Fees, charges, prices, and service payments related to road traffic activities;
- Tuition fees;
- Hospital fees;
- Payments of social insurance and health insurance contributions;
- Insurance premium payments in accordance with the Law on Insurance Business; and
- Repayment of due and overdue debts, interest, and related charges to credit institutions and foreign bank branches in accordance with applicable laws.

These limits are expected to strike a balance between practical usage needs and risk management objectives, facilitating user convenience while mitigating the risks of misuse of e-wallets for money laundering, illegal fund transfers, or terrorist financing.

Information provision

No later than the 10th day of each month, e-wallet service providers are required to submit to the SBV, upon request, information on e-wallets showing signs of fraud, scams, or other legal violations. In the event of any changes to such information, e-wallet service providers must promptly update and resubmit the information to the SBV, and remain responsible for the truthfulness and accuracy of the information and data provided.

When conducting fund transfer transactions between e-wallets, or between e-wallets and Vietnamese-dong–denominated accounts or debit cards linked to Vietnamese-dong–denominated accounts opened at banks or foreign bank branches, the service provider serving the transaction initiator is responsible, upon request, for providing the service provider serving the beneficiary with the following minimum information relating to the transaction initiator: (i) the name of the transaction initiator; (ii) the initiator's e-wallet number or account number; and (iii) the initiator's permanent residential address, identification number, or transaction reference number (where no account exists).

Provisions effective from 1 January 2026

Procedures for opening e-wallets

Circular 41 set out more stringent customer identification and verification requirements applicable to e-wallet holders. Accordingly, e-wallet service providers are required to review the legality and validity of, and cross-check to ensure the accuracy and consistency of, the documents, information, and data provided by customers; and to verify customer identification information in accordance with applicable laws on anti-money laundering, as well as the following specific requirements:

Individual customers	Organizational customer
<p>Where the e-wallet holder or the representative is an individual using a citizen identification card, electronic citizen identification, citizen identity card (having an embedded data storage component), or an electronic identity, the e-wallet service provider is required to:</p> <ul style="list-style-type: none"> ✓ Conduct an in-person meeting; and ✓ Verify and cross-check the identity documents, and perform biometric verification and matching of the e-wallet holder or the representative of the e-wallet holder, in accordance with the regulations on opening e-wallets via electronic means. 	<p>Where the e-wallet holder is an organization established and operating in Vietnam, the e-wallet service provider is required to conduct an in-person meeting with the lawful representative of the e-wallet holder and to verify the identification information of such lawful representative in the same manner as applicable to individual customers.</p>
<p>Where the e-wallet holder or the representative is an individual using a citizen identity card without an embedded data storage component, or a birth certificate in the case of individuals under the age of 14 who do not yet hold a citizen identity card or a passport, the e-wallet service provider is required to:</p> <ul style="list-style-type: none"> ✓ Conduct an in-person meeting; and ✓ Verify and cross-check the identity documents, and match the biometric information of the e-wallet holder or the representative of the e-wallet holder with the biometric information displayed on such identity documents. 	<p>Where the e-wallet holder is a foreign legal entity, the e-wallet service provider may verify the identification information of the lawful representative of the e-wallet holder through a third party or by engaging another organization, provided that such third party or engaged organization conducts an in-person meeting with the lawful representative and verifies and cross-checks the identity documents, including biometric verification and matching, against the biometric information displayed on such identity documents.</p>
<p>Where the e-wallet holder is a foreign individual not physically present in Vietnam, the e-wallet service provider may verify customer identification information through a third party or by engaging another organization to carry out such verification.</p>	<p>The above requirements are not mandatorily applicable to the following categories of organizational customers:</p> <ul style="list-style-type: none"> ✓ State authorities and public service units;

Individual customers	Organizational customer
	<ul style="list-style-type: none"> ✓ Listed organizations in accordance with the Law on Securities; and ✓ Organizations included in the Fortune Global 500 list as published by Fortune magazine in the immediately preceding year.
Where a customer registers for transactions via the e-wallet service application, the e-wallet service provider is required to verify the mobile phone number of the e-wallet holder or the representative of the e-wallet holder, ensuring that the subscriber information of such mobile number corresponds with the information stated in the relevant identity documents.	The e-wallet service provider is required to verify the mobile phone number of the lawful representative of the e-wallet holder, ensuring that the subscriber information corresponds with the information stated in the relevant identity documents.

Ensuring safety and security in the opening and use of e-wallets

From 1 January 2026, e-wallet service providers are required to adopt internal regulations on risk management in relation to the opening and use of e-wallets. Such internal regulations must provide for the periodic review, cross-checking, and re-verification of customer identification information throughout the e-wallet usage lifecycle.

In addition, based on the identification of potential risks arising from the opening and use of e-wallets and the corresponding risk mitigation measures, e-wallet service providers are required to specify cases in which transactions may be refused or temporarily suspended, including payment transactions where the provider is unable to contact the customer using the contact details provided by the customer.

Responsibilities of e-wallet service providers

From 1 January 2026, an e-wallet service provider may use only one trade name or e-wallet brand that has been approved by the SBV under its license.

In the event of any change to the trade name or e-wallet brand after the license has been granted, the IPSP must submit a written notification to the SBV (via the Payment Department) and publicly disclose such change on its official website at least one (1) month prior to the effective date of the change.

Circular 41 clearly reflects the SBV's continued regulatory direction toward further strengthening the legal framework for digital payments, in a manner that both promotes financial inclusion and enhances risk management, system safety, and the protection of e-wallet users' rights. The new requirements are expected to contribute to the transparent, safe, and sustainable development of the e-wallet market in Vietnam in the period ahead.

About Indochine Counsel

Established in October 2006, Indochine Counsel is a premier commercial law firm in Vietnam. We're ideally positioned to help international investors and foreign firms navigate the legal landscape in one of Asia's most dynamic and exciting countries. We also take pride in our services for domestic clients searching for opportunities abroad. With over 45 lawyers and staff in two offices, Ho Chi Minh City and Hanoi, Indochine Counsel offers expertise in a dozen practice areas assisting you throughout the entire life cycle of your business. We're your trusted partner in Vietnam for international and domestic legal solutions.

Indochine Counsel represents and advises clients on all legal aspects in the following major areas of expertise:

- Anti-trust & Competition
- Banking & Finance
- Corporate & Commercial
- Energy, Natural Resources & Infrastructure
- Intellectual Property
- Inward Investment
- Labour & Employment
- Litigation & Dispute Resolution
- Mergers & Acquisitions
- Real Estate & Construction
- Securities & Capital Markets
- Technology, Media & Telecommunications

Contact Us

For further information or assistance, please contact the following professionals at Indochine Counsel:



Dang The Duc

Managing Partner

E duc.dang@indochinecounsel.com



Trinh Ngoc Ly

Associate

E ly.trinh@indochinecounsel.com

Ho Chi Minh City

Unit 305, 3rd Floor, Centec Tower
72-74 Nguyen Thi Minh Khai, Xuan Hoa Ward
Ho Chi Minh City, Vietnam

T +84 28 3823 9640
F +84 28 3823 9641
E info@indochinecounsel.com

Hanoi

Unit 705, 7th Floor, CMC Tower
Duy Tan Street, Cau Giay Ward
Hanoi, Vietnam

T +84 24 3795 5261
F +84 24 3795 5262
E hanoi@indochinecounsel.com

This Special Alert is designed to provide our clients and contacts with general information of the relevant topic for reference only, without the assumption of a duty of care by Indochine Counsel. The information provided is not intended to be nor should it be relied upon as a substitute for legal or other professional advice.

© 2006 – 2026 Indochine Counsel. All Rights Reserved



You can reach us at
[Indochinecounsel.com](https://www.indochinecounsel.com)



LinkedIn



Facebook



YouTube