



Identomat

COMPLIANCE GUIDE

Fintech & Digital Payments Compliance in Ukraine

COUNTRY **Ukraine**

INDUSTRY **Fintech & Digital Payments**

LAST UPDATED **16 October 2026**

KEY REGULATORS **National Bank of Ukraine · State Financial Monitoring Service of Ukraine**

Key takeaways

- A non-bank that moves money, issues e-money or runs a wallet in Ukraine needs an authorisation from the National Bank of Ukraine (NBU) and an entry in the NBU's Payment Infrastructure Register before it serves a single customer.
 - Fully remote onboarding is allowed. The NBU accepts live video verification, NBU BankID combined with a document copy signed with a qualified electronic signature, and a Diia e-passport combined with a liveness photo.
 - Payment and e-money firms are anti-money laundering (AML) obliged entities: they must verify customers before the business relationship starts, screen for sanctions and politically exposed persons (PEPs), and report suspicious transactions to the State Financial Monitoring Service.
 - Online access to accounts and remote payments require strong customer authentication with at least two independent factors, with narrow exemptions for small payments and trusted recipients.
 - Ukraine remains under martial law: NBU emergency rules on foreign exchange and cross-border payments still apply, and a reform of the personal data law is a bill, not yet law (as of October 2026).
-

Ukraine's payments market is open to non-bank providers, and the 2021 Law on Payment Services, built on the EU's PSD2 and E-Money Directive, lets payment institutions and e-money institutions open payment accounts, issue cards and issue e-money without a banking licence. Open banking regulations adopted in July 2025 add account information and payment initiation services.

One authority dominates: the NBU licenses payment and e-money providers and financial companies, supervises their prudential position and conduct, and is their AML supervisor. Suspicious and threshold reports go to the State Financial Monitoring Service of Ukraine, the national financial intelligence unit.

The biggest obstacle for a new entrant is not remote onboarding, which Ukrainian rules accommodate well, but the depth of the NBU's AML and governance expectations for non-banks, combined with martial-law restrictions on cross-border flows and close scrutiny of person-to-person transfers used by "drop" account networks.

CONTENTS

- 1 Who regulates this sector
- 2 Licensing and authorisation
- 3 AML, KYC and customer due diligence
- 4 Identity verification and onboarding
- 5 Digital channels: what's different
- 6 Data protection and biometrics
- 7 Sector-specific obligations
- 8 Risk indicators and red flags
- 9 Enforcement and penalties
- 10 Recent changes and what to watch
- 11 What this means for identity verification
 - Sources

1 Who regulates this sector

Authority	Remit for fintech	Level	Official site
National Bank of Ukraine (NBU)	Authorises payment, e-money and non-financial payment service providers and financial companies; prudential, conduct and AML supervision; operates NBU BankID	National	bank.gov.ua
State Financial Monitoring Service of Ukraine (SFMS)	Financial intelligence unit; registers obliged entities and receives threshold and suspicious transaction reports	National	fiu.gov.ua
Ministry of Finance of Ukraine	Forms state AML policy and sets reporting procedures for obliged entities	National	mof.gov.ua
Ministry of Digital Transformation	Diia portal and app; integrated electronic identification system used to verify business representatives	National	thedigital.gov.ua
Ukrainian Parliament Commissioner for Human Rights	Supervises compliance with the personal data protection law	National	ombudsman.gov.ua
National Security and Defence Council	Sanctions decisions under the Law on Sanctions; the resulting list must be screened	National	rnbo.gov.ua

Ukraine is a unitary state, so licensing and supervision are national. Ukraine is an EU candidate, but EU regulations do not apply directly; EU payment rules matter only to the extent Ukrainian law transposes them.

2 Licensing and authorisation

The Law of Ukraine "Про платіжні послуги" [On Payment Services], No. 1591-IX of 30 June 2021, defines nine types of payment service providers and nine payment services, seven of them financial and two non-financial (payment initiation and account information). Non-bank providers, including payment institutions, e-money institutions and postal operators, may open payment accounts, issue payment cards and issue e-money, and no longer need to join a payment system to transfer funds ([NBU, 2021](#)).

Under Article 57 of the law, only banks, e-money institutions, branches of foreign payment institutions, postal operators, the NBU and public authorities may issue e-money. Every provider other than a bank needs an NBU licence and an entry in the Payment Infrastructure Register, and an entity not recorded in the register may not provide the services the law regulates ([NBU, Cashless Payments](#)).

Payment and e-money institutions

Authorised under the NBU Regulation on the authorisation of financial and limited payment service providers (Resolution No. 217 of 7 October 2022), with e-money operations governed by Resolution No. 210 of 29 September 2022 and prudential ratios by Resolution No. 190 of 25 August 2022.

Open banking providers

Payment initiation and account information providers are authorised under NBU Resolution No. 81 of 25 July 2025 and need a qualified open banking certificate under Resolution No. 82 ([NBU, Open Banking](#)).

Lenders and other financial companies

Lending apps operate as financial companies licensed under the Law on Financial Services and Financial Companies (No. 1953-IX) and NBU Resolution No. 199 of 29 December 2023.

Agents and ownership

Commercial agents distributing payment services are governed by NBU Resolution No. 168 of 2 August 2022; owners must meet the transparency rules of NBU Resolution No. 30 of 14 April 2021.

These instruments are listed in the NBU's own reference list of the rules that apply to non-bank payment service providers ([NBU](#)). Licensing is national; there is no separate online licence, and the same authorisation covers app-only and agent-based models.

The Law on Prevention and Counteraction to Legalisation (Laundering) of Criminal Proceeds, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction, No. 361-IX of 6 December 2019 (the AML Law), lists banks and other financial institutions, payment system operators and postal operators providing financial payment services as reporting entities (Article 6). The NBU sets AML requirements for, and supervises, the non-bank financial institutions it licenses ([NBU, Financial Monitoring](#)). Its detailed rulebook for non-banks is the Regulation on the Implementation of Financial Monitoring by Institutions, NBU Resolution No. 107 of 28 July 2020 (Regulation 107).

When due diligence is required

Article 11 of the AML Law requires customer due diligence on establishing a business relationship, on payment transactions made without opening an account, when there is suspicion, when earlier data is doubtful, and on one-off transactions at or above the Article 20 threshold of UAH 400,000, including linked transactions ([NBU, 2020](#)). Identification and verification must happen before the relationship starts; verification may finish shortly after first contact if risk is managed, but always before the first transaction. Financial institutions may not keep anonymous accounts.

Data, beneficial owners and PEPs

For a resident individual the firm records full name, date of birth, identity document details, address and taxpayer registration number (RNOKPP). Beneficial ownership starts at 25 per cent, and the Unified State Register cannot be the only source; discrepancies with the register must be reported to the SFMS by the tenth working day of the following month. Foreign PEPs require senior approval, source of wealth and funds checks and enhanced monitoring, which continue for at least twelve months after the person leaves office.

Reporting and records

Reporting entities report threshold transactions within five working days or by the fifth working day of the following month, depending on the Article 20 criterion, and suspicious transactions or attempts immediately, regardless of amount (Article 8). Records must be kept for at least five years after the relationship ends. Regulation 107 requires customer data to be refreshed at least yearly for high-risk customers, every three years for medium risk and every five years otherwise.

Annex 2 to Regulation 107 sets the verification methods for non-banks. Verification relies on the identity document, which must be valid, checked for forgery and matched to the person. In person, the firm records the original document; remotely, Regulation 107 recognises three full methods:

Video verification

A live, uninterrupted session with explicit recorded consent, photo capture of the person and the document, checks of security features, and varied question scripts (Annex 3). Reading the chip of a biometric document, with at least passive authentication under ICAO Doc 9303, replaces the visual security check.

NBU BankID

Identification data received through NBU BankID, plus a copy of the identity document signed with the customer's qualified electronic signature, matched against each other.

Diia e-passport

An e-passport sealed by state enterprise Diia with a qualified timestamp, plus either a liveness-checked photo or a document copy signed with the customer's qualified electronic signature.

Regulation 107 defines liveness detection as real-time photo capture that distinguishes a live person from any reproduction, including digital copies, make-up and masks. Business representatives can be verified through their qualified electronic signature and the integrated electronic identification system run by the Ministry of Digital Transformation. Firms may use agents under a written agreement and rely on another regulated firm's due diligence, but responsibility stays with the firm (Article 11(17) of the AML Law).

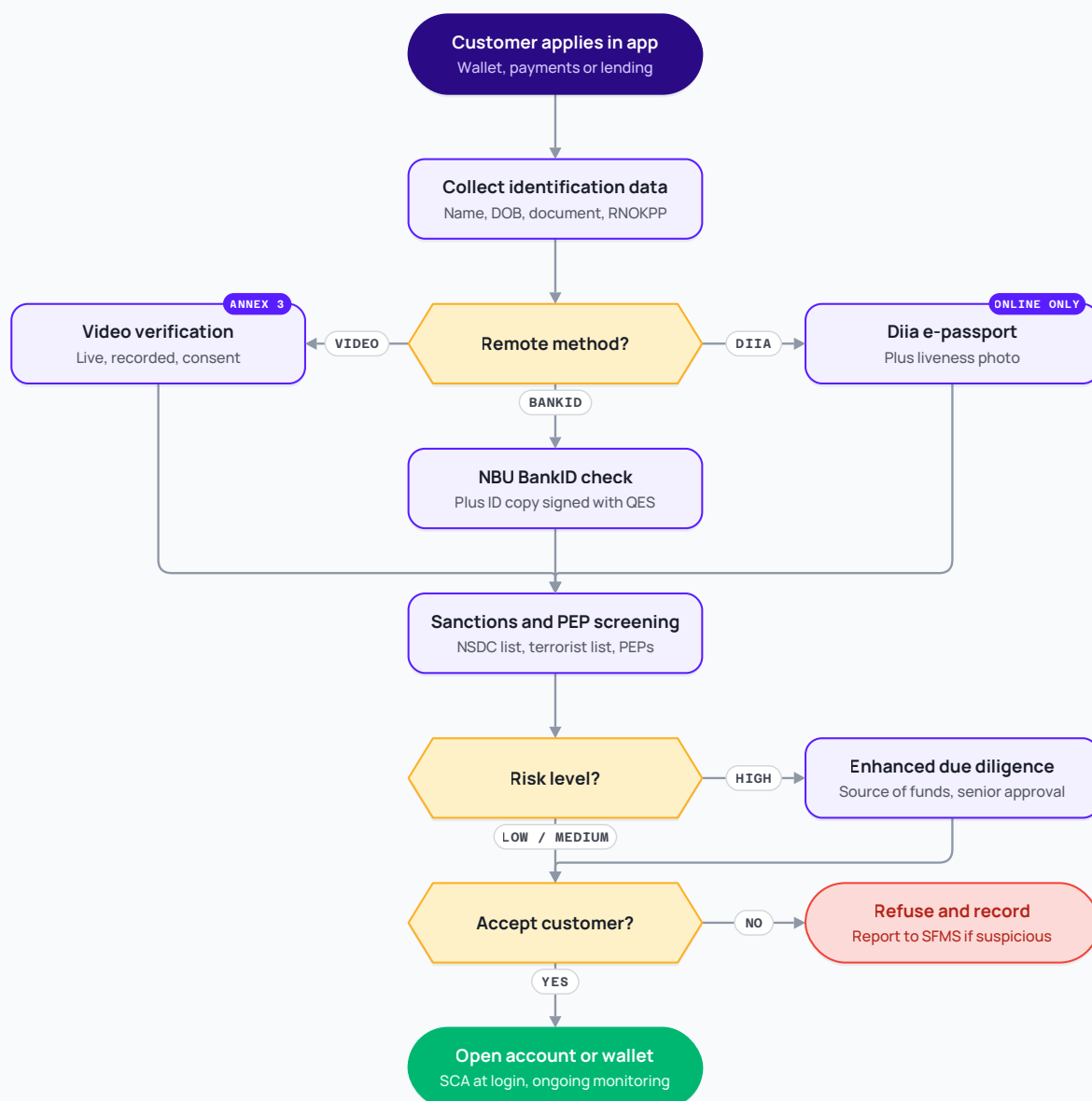


Figure 1. Remote onboarding of an individual by a Ukrainian payment or e-money institution.

5

Digital channels: what's different

Bottom line: the due diligence duties are channel-neutral, but Ukrainian rules prescribe exactly which remote methods count, what evidence must be captured, and add strong authentication for every remote session and payment.

Requirement	In person / branch or agent	Online / remote	Difference
Due diligence triggers and timing	Before the relationship or transaction	Same (AML Law, Article 11)	Same
Accepted verification methods	Original identity document presented	Video verification, BankID plus QES copy, Diia e-passport plus liveness	Differs
Evidence captured	Signed paper copies or certified e-copies	Session recording, liveness photo, chip authentication log	Differs
Risk treatment	Standard risk assessment	Remote relationships a named risk factor; not automatically high risk	Differs
Simplified tier	Not used	Lighter remote methods for low-risk customers within monthly and yearly caps	Differs
Authentication	Physical presence	Strong customer authentication for remote access and payments	Differs
Sanctions and PEP screening	Required	Required	Same
Record retention	At least five years	At least five years	Same

Remote onboarding is a risk factor, not a ban

The AML Law requires firms to manage risks of technologies that allow transactions without direct contact (Article 8(2)(25)), and Regulation 107 asks firms to give separate attention to remote establishment of relationships, agents and reliance when assessing their own risk profile. Nothing in either instrument makes a remote customer high risk by default.

A capped simplified tier

Where the customer is low risk, outgoing transactions stay at or below UAH 40,000 a month and UAH 400,000 a year, and balances or obligations stay at or below UAH 40,000, Regulation 107 (Annex 2, paragraphs 31 and 32) allows lighter remote methods: a document

copy signed with the customer's qualified electronic signature, BankID data alone, chip reading with a PIN or liveness photo, or credit bureau data plus a one-time password to the customer's financial phone number and a liveness photo. The firm must control these limits.

Strong customer authentication

The NBU Regulation on Authentication and Use of Strong Authentication in the Payment Market (Resolution No. 58 of 3 May 2023) requires two or more factors from different categories (knowledge, possession, inherence), at most five consecutive failed attempts and a ten-minute inactivity limit. Firms may skip it for remote payments up to UAH 2,000 while cumulative unauthenticated payments stay within UAH 10,000 or five transactions, for trusted recipients, and for low-risk transactions that meet fraud-rate benchmarks. The authentication code must be dynamically linked to the amount and payee.

6 Data protection and biometrics

Personal data processed to meet the AML Law does not require the customer's consent, but the firm must tell the customer at identification about its data processing obligations (AML Law, Article 2(2); Regulation 107, Annex 2, paragraph 34). Video verification is the exception in practice: Annex 3 requires clear, explicit consent before the session, including to photo capture, and the recording must show that consent. Onboarding files, recordings and liveness images fall under the five-year AML retention rule.

The general regime is the Law on Personal Data Protection, supervised by the Ukrainian Parliament Commissioner for Human Rights. A replacement law aligned with the EU's GDPR, bill No. 8153, passed first reading and in December 2025 was being moved to the parliamentary committee on legal policy for second reading; it would create a separate data protection authority. **Bill, second reading pending**

7 Sector-specific obligations

E-money wallets

An issuer must carry out due diligence when opening a reloadable e-wallet. A consumer may hold a non-reloadable wallet accessed only through a prepaid card, capped at UAH 5,000 ([NBU, Cashless Payments](#)).

Transfer data and monitoring systems

Article 14 of the AML Law requires every transfer to carry payer and payee data. At or above UAH 30,000 the full payer data must be verified; below that, verification may be skipped unless there is suspicion or the payer pays cash. A provider may not execute a transfer that lacks the required data. Regulation 107 (paragraph 16) requires a payment institution to run an automated system that freezes terrorist-linked assets, logs every user action and monitors transactions continuously for suspicious indicators.

Person-to-person transfer limits

A temporary NBU cap of UAH 150,000 a month on outgoing card-to-card transfers by individuals ran from 1 October 2024 and lapsed on 1 April 2025. Providers that signed the December 2024 Memorandum to Ensure Transparency of Payment Services Market Operation now set limits, including on IBAN transfers, for customers without confirmed income ([NBU, 1 April 2025](#)).

NBU BankID as a service provider

A fintech that wants to receive identity data through NBU BankID must be a resident legal entity, apply to the BankID System Council and sign accession and clearing agreements ([NBU BankID](#)).

PAYMENT AND E-MONEY RED FLAGS IN NBU RULES

- **Drop accounts:** individuals lending accounts or cards to third parties, shown by abnormal surges in person-to-person transfers and new card issuance.
- **Impostors:** a person using another's identity data or document during remote verification.
- **Forged or altered documents:** pasted photos, misaligned text or inconsistent issue and expiry data.
- **Shell companies:** corporate customers with no real activity, staff or premises, or registered at an address shared by more than 50 entities.
- **Social engineering:** customers manipulated into authorising payments they would not otherwise make.
- **Virtual asset activity:** customers active in virtual assets, which Regulation 107 places in the high-risk category.
- **Anomalous authentication:** new devices, first-seen locations, malware signs or spending outside the customer's pattern.
- **Aggressor-state links:** customers or counterparties connected with states carrying out armed aggression against Ukraine.

The NBU applies measures of influence to the payment and non-bank providers it supervises, including written warnings, fines and, ultimately, licence revocation; Regulation 107 treats a licence revocation or the appointment of temporary administration as a stain on the business reputation of the managers in office at the time. Under the AML Law, the head of the reporting entity and the responsible employee bear personal responsibility for improper financial monitoring (Article 8(5) and (6)).

Penalties for breaches of payment legislation were increased by Law No. 3994-IX of 8 October 2024 on the consolidation of financial services market regulation **In force** ([NBU, 1 April 2025](#)).

Recent changes and what to watch

- **December 2025** **Bill, second reading pending** Personal data bill No. 8153 moved to the legal policy committee; if adopted, onboarding data processing will need reassessment against GDPR-style rules and a new regulator.
- **25 July 2025** **In force** NBU Resolutions No. 80, 81 and 82 put open banking into operation; payment initiation and account information providers need NBU authorisation and a qualified open banking certificate.
- **1 April 2025** **Regulatory limit lapsed** The NBU's UAH 150,000 monthly card-to-card cap ended; memorandum signatories keep income-based limits.
- **December 2024** **Industry memorandum** Banks and licensed payment providers signed the payment market transparency memorandum targeting drop accounts.
- **8 October 2024** **In force** Law No. 3994-IX increased penalties for violations of payment legislation.

What this means for identity verification

A Ukrainian onboarding flow should support all three full remote methods: live video verification with document security checks and optional NFC chip reading, NBU BankID matched to a document copy signed with a qualified electronic signature, and Diia e-passport intake combined with liveness detection. Each path needs its own evidence package: the recording and consent, the BankID file and signature, or the sealed e-passport with a timestamp, plus liveness photos certified with the firm's qualified signature and timestamp.

Accepted documents are the passport of a citizen of Ukraine (booklet or ID card) and other documents usable for transactions in Ukraine; the RNOKPP must be captured, with a separate certificate where the document lacks it. Non-residents need nationality and Ukrainian address. A simplified tier needs hard limit controls at UAH 40,000 a month and UAH 400,000 a year. Screening must cover the NSDC sanctions list, the terrorist list and PEPs at onboarding and on change. Re-verification triggers include document expiry or replacement (within six months), changes of ownership or management, PEP status, and the scheduled one, three or five-year refresh.

How Identomat helps

Identomat runs identity verification, screening and monitoring for regulated businesses on one platform, with workflows you configure for each market. For the requirements in this guide, that means:

- Live video KYC with document security checks and NFC chip reading, matching the NBU's video verification requirements.
- Biometric liveness and face match for remote onboarding flows that combine a Diia e-passport with a live photo.
- AML screening against sanctions, PEP and watchlists at onboarding and on an ongoing basis.
- KYB and beneficial owner verification for corporate and merchant customers.
- No-code workflows with a full audit trail of each check for record-keeping.

[Request a meeting](#)

DISCLAIMER

This article is intended for informational purposes only and does not constitute legal advice. It is a compilation of information from various sources and reflects the information available as of the last updated date indicated above. Laws, regulations, and regulatory guidance may change, so readers should consult qualified legal professionals for advice specific to their circumstances.

Sources

- Закон України "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом..." [Law on Prevention and Counteraction to Money Laundering], No. 361-IX of 6 December 2019, unofficial English translation as of 1 August 2022, State Financial Monitoring Service, fiu.gov.ua
- Постанова Правління НБУ № 107 "Про затвердження Положення про здійснення установами фінансового моніторингу" [Regulation on the Implementation of Financial Monitoring by Institutions], 28 July 2020, Annexes 1 to 3, bank.gov.ua
- Постанова Правління НБУ № 58 "Про затвердження Положення про автентифікацію та застосування посиленої автентифікації на платіжному ринку" [Regulation on Authentication and Strong Authentication in the Payment Market], 3 May 2023, bank.gov.ua

- NBU, Cashless Payments (e-money issuers, Article 57 of the Law on Payment Services), bank.gov.ua
- NBU, "New quality of payment services: The Verkhovna Rada adopted a modern law on payment services", 2021, bank.gov.ua
- NBU, list of laws and regulations applicable to non-bank payment service providers, bank.gov.ua
- NBU, Open Banking (Resolutions No. 80, 81 and 82 of 25 July 2025), bank.gov.ua
- NBU, "NBU Unveils New Procedure for Financial Monitoring by Banks", 2020, bank.gov.ua
- NBU, "NBU Not Extending Regulatory Restriction of UAH 150,000 per Month for Individual P2P Transfers", 1 April 2025, bank.gov.ua
- NBU, How to become a BankID subscriber, bank.gov.ua
- NBU, Financial Monitoring, bank.gov.ua
- Стенограма засідання Комітету ВРУ з питань прав людини [Transcript, Verkhovna Rada Human Rights Committee] on bill No. 8153, 3 December 2025, rada.gov.ua