



Identomat

COMPLIANCE GUIDE

Banking & Digital Banking Compliance in Ukraine

COUNTRY **Ukraine**

INDUSTRY **Banking & Digital Banking**

LAST UPDATED **16 October 2026**

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

Key takeaways

- Taking deposits in Ukraine requires a banking licence from the National Bank of Ukraine (NBU), with share capital of at least UAH 200 million; a separate limited licence now exists for "financial inclusion banks" that serve individuals and small businesses.
- Fully remote account opening is allowed. Banks may verify customers by live video call, through the NBU's BankID identity network, or with a Diia e-passport (the state app's digital passport) combined with a liveness check.
- Video verification done to the NBU's rules counts as verifying the customer in person, but it has strict conditions: recorded consent, an uninterrupted live session, document security checks and a one-time password at the end.
- Banks must report transactions of UAH 400,000 or more that match set features (cash, transfers abroad, politically exposed persons, links to Russia) to the State Financial Monitoring Service, and report suspicious activity immediately, whatever the amount.
- Ukraine has been under martial law since February 2022. Extra NBU rules restrict accounts linked to Russia and Belarus, ease document acceptance and allow a larger simplified remote-onboarding tier until martial law ends.

Ukraine's banking market is open to new entrants, including digital-first banks, but only through a full NBU licence or the new limited licence for financial inclusion banks. There is no separate digital bank licence: an app-only bank holds the same licence and the same anti-money laundering (AML) duties as a branch-based bank.

The NBU is both the prudential supervisor and the AML supervisor for banks, and it fines banks under the Law on Banks and Banking. The State Financial Monitoring Service receives reports. The biggest obstacle for a new entrant is the licensing threshold itself, followed by the detailed, prescriptive NBU rules on how each remote verification method must be run and evidenced.

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

Ukraine is a unitary state, so licensing and supervision are national. The table lists the authorities that matter for a bank's onboarding and AML programme.

Authority	Remit	Level	Official site
National Bank of Ukraine (NBU)	Bank licensing, prudential supervision, AML/CFT supervision of banks and other NBU-licensed financial institutions, BankID system	National	bank.gov.ua
State Financial Monitoring Service (SFMS)	Financial intelligence unit: receives threshold and suspicious transaction reports, can suspend transactions	National	fiu.gov.ua
National Securities and Stock Market Commission (NSSMC)	AML supervision of capital markets participants other than banks	National	nssmc.gov.ua
National Security and Defence Council (NSDC)	Sanctions decisions; State Register of Sanctions	National	rnbo.gov.ua
Ukrainian Parliament Commissioner for Human Rights	Personal data protection supervision	National	ombudsman.gov.ua
Ministry of Digital Transformation	Diia state services app and portal, including e-passports	National	thedigital.gov.ua

The Deposit Guarantee Fund also has statutory powers over banks (deposit coverage and resolution); its own rules are not covered in detail here. A bank that offers securities services remains under NBU AML supervision, because Article 18(1)(2) of the AML law assigns the NSSMC only capital markets participants "other than banks".

2

Licensing and authorisation

Full banking licence

Under Article 19 of the [Law on Banks and Banking No. 2121-III](#), a legal entity intending to carry on banking activity must apply to the NBU within one year of state registration. The application includes evidence that at least three management board members are appointed, that senior managers, the chief risk officer, the chief compliance officer and the head of internal audit meet qualification requirements, a three-year strategy and business plan, and internal policies on risk management and internal control. The NBU decides within three months of receiving the application and may extend this by up to 30 working days. Minimum share capital is UAH 200 million (Article 31), and the NBU may set higher individual minimums. An entity becomes a bank only once the licence is issued.

Financial inclusion banks

Law No. 4465-IX, in effect from 26 June 2026, added Article 8-1 and a limited banking licence (Article 19-2). A financial inclusion bank may serve only individuals, businesses and non-profits with annual income up to the equivalent of EUR 5 million, plus public bodies; it may not invest in securities other than government bonds and NBU certificates of deposit, and its lending to each customer is capped by multiples of the minimum wage. It may offer payment services and sign up customers outside its premises, including through commercial agents.

Deposit insurance

Banks participate in the household deposit guarantee system. Article 26 of the [Law on the Household Deposit Guarantee System No. 4452-VI](#) sets the coverage limit at not less than UAH 200,000 per depositor per bank; the actual limit is set by the Fund's administrative board.

Banks are primary financial monitoring entities under the [Law on Prevention and Counteraction to Legalisation \(Laundering\) of the Proceeds of Crime No. 361-IX](#) (edition of 26 June 2026). The NBU's detailed rules are in the [Regulation on Financial Monitoring by Banks, NBU Board Resolution No. 65](#).

When due diligence applies

On establishing a business relationship, on suspicion, for payments without an account, when earlier data is in doubt, and for one-off transactions of UAH 400,000 or more, including linked transactions (Article 11(4)).

Identification data

For a resident individual: full name, date of birth, identity document details, address, taxpayer number (RNOKPP) and, if available, the Unified State Demographic Register number (Article 11(9)).

Beneficial ownership

Obtain the ownership structure and verify beneficial owners on a risk basis; the bank may not rely solely on the state register and must report discrepancies to the register holder within 10 working days (Articles 8(2) (8-1), 11(8)).

Record keeping

Keep all CDD documents, records and analysis for at least five years after the relationship ends or the one-off transaction is completed (Article 8(2) (18)).

Mandatory high risk and enhanced due diligence

Article 7(5) requires a high-risk rating for, among others, clients from jurisdictions that do not apply FATF standards, sanctioned persons, foreign politically exposed persons (PEPs), clients from offshore zones listed by the Cabinet, citizens and residents of the state carrying out armed aggression against Ukraine (with narrow exceptions), entities owned by them, and clients moving funds through institutions located in that state. High-risk clients receive enhanced due diligence (Article 12). For PEPs, management approval, source of wealth and source of funds checks and ongoing enhanced monitoring are required, and a PEP who is refused must receive a written explanation within five working days (Article 11(14)). NBU Resolution No. 65 (paragraph 60) adds clients active in virtual assets and suspected shell companies to the high-risk list.

Reporting to the SFMS

A transaction is a threshold transaction if it equals or exceeds UAH 400,000 and has at least one feature listed in Article 20: a party linked to the aggressor state or a non-compliant jurisdiction; a PEP or related person; a transfer abroad; a cash operation; or an e-resident's operation. Reports on aggressor-state, PEP and e-resident features are due within five working days; reports on transfers abroad and cash are due by the fifth working day of the following month. Suspicious transactions are reported immediately once suspicion arises, regardless of amount (Article 8(2)(8)).

4

Identity verification and onboarding

Verification must rest on official documents or information from official or reliable sources, and documents must be valid when presented (Article 11(8)). Annex 2 to NBU Resolution No. 65 sets out the permitted methods and, since July 2026, expressly forbids banks and their agents from using any method not listed (paragraph 39).

Permitted ways to verify an individual

The baseline (Annex 2, paragraph 12) is presentation of the original document either in person or during video verification. In person, the bank evidences presence by staff-certified paper copies, by electronic copies plus a photo of the person holding the document taken on a bank device with geotags, by reading the chip of an ID card with at least passive authentication, or by receiving a Diia e-passport sealed by the state enterprise DIIA plus a photo of the person with the device showing it. Paragraph 30 adds two remote routes: identification data from the NBU BankID System together with a document copy signed with the customer's qualified electronic signature (QES), or a Diia e-passport combined with a liveness-checked photo or a QES-signed document or questionnaire.

Simplified remote tier

For low-risk clients whose total outgoing limit is UAH 40,000 a month and UAH 400,000 a year, with a balance not above UAH 40,000, paragraphs 32 and 33 allow lighter methods: a QES-signed document copy, BankID data alone (except for lending), a symbolic first transfer from the customer's own account at another Ukrainian bank plus liveness and a selfie with the document, chip reading of an ID card, or credit bureau data plus a one-time password and liveness photo.

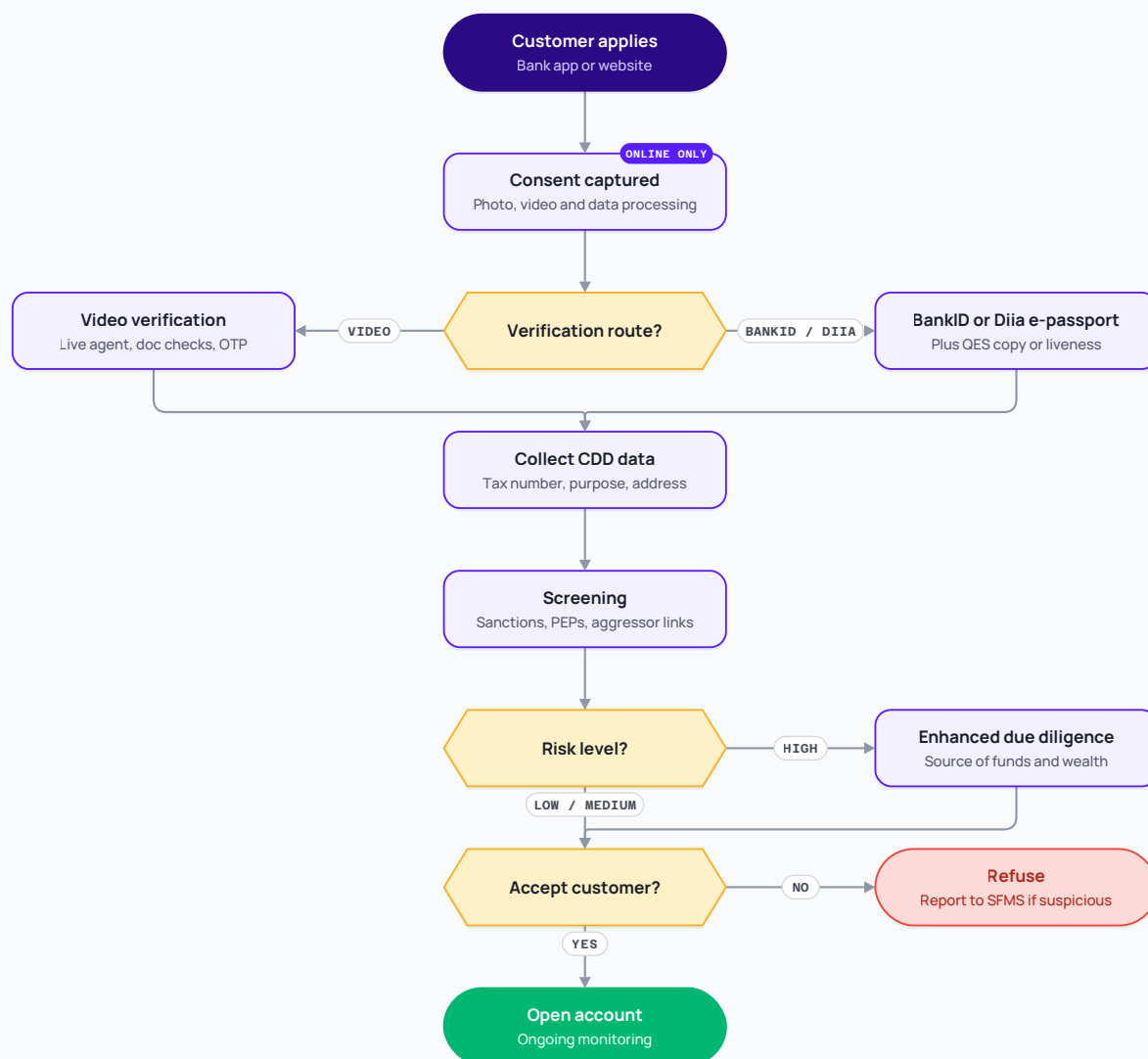


Figure 1. Remote onboarding of an individual by a Ukrainian bank.

Reliance and agents

A bank may use an agent for identification only under a written contract, and it remains responsible for due diligence (Article 11(18)). A bank acting as a BankID identity provider may pass on customer data only if it verified the customer in person or by video verification (Annex 2, paragraph 31). The [Regulation on the NBU BankID System](#), restated from 10 January 2026, also allows non-bank account-servicing payment providers to act as identity providers.

Bottom line: the AML duties are channel-neutral, but the NBU prescribes exactly which remote methods are acceptable and how each must be run and evidenced; anything outside that list is prohibited.

Requirement	In person	Online / remote	Difference
Remote onboarding permitted	Original document in branch	Video verification, BankID with QES copy, Diia e-passport with liveness	Differs
Legal effect of video verification	Baseline	Equal to in-person verification if Annex 3 is followed	Same
Risk treatment of remote channel	Risk-based	Delivery method is a risk criterion; no automatic EDD	Same
When verification is completed	Before first transaction	Before first transaction	Same
Simplified methods with limits	Not applicable	Low-risk tier capped at UAH 40,000 a month	Differs
Evidence kept	Certified copies or geotagged photos	Full video recording, QES and timestamps on e-copies	Differs
Consent to photo capture	Explicit consent required	Explicit consent, recorded in the video	Same
Sanctions and PEP screening	Required	Required	Same

Video verification is tightly specified

Annex 3 to Resolution No. 65 requires a private setting, an encrypted real-time session that restarts in full if interrupted, varied question scripts, the customer stating the document number and a "financial" phone number on the recording, photos of the person and of the person with the document, checks for forgery and visible security features (which may be skipped if the chip is read with passive authentication or a Diia e-passport is received), checks for third-party pressure, and a final one-time password. Results may not be used if any step fails or doubts remain.

Booklet passports need extra steps

If a bank accepts booklet-style documents without a chip by video, it must add at least one control: BankID data comparison, a second document, a symbolic first transfer from the customer's own account in another Ukrainian bank, or credit bureau data plus a one-time password (Annex 3, paragraph 12).

Martial-law adjustments

NBU Resolution No. 153 of 20 December 2024, applicable during martial law, lets banks open accounts remotely for residents abroad and non-residents (except Russian and Belarusian residents) solely to buy military bonds, using copies received through remote channels and a video call instead of full video verification. It also raises the simplified-tier limits to UAH 400,000 a month and a year.

6 Data protection and biometrics

The [Law on Personal Data Protection No. 2297-VI](#) applies, supervised by the Parliament Commissioner for Human Rights. Article 2(2) of the AML law states that processing personal data to meet AML requirements does not need the data subject's consent, but the bank must tell the customer about its AML processing duties at identification.

Biometric data is a special category under Article 7 of Law No. 2297-VI, which prohibits processing it unless an exception applies, such as the person's unambiguous consent. The NBU rules align with this: banks must obtain clear consent before photo capture and video verification, and the consent must be part of the recording or signed. Video recordings, electronic copies and check results are kept in the client file for the statutory period, protected under banking secrecy rules and stored so they cannot be modified (Annex 3, paragraphs 17 to 21).

7 Sector-specific obligations

Correspondent banking

Banks may not keep anonymous accounts or deal with shell banks or institutions that serve them (Article 11(1)). Before opening correspondent relationships with a foreign institution, a bank must assess its reputation, supervision and AML controls, obtain senior management approval and document responsibilities (Article 11(13)). Foreign correspondents outside the EU and FATF members are high risk by law.

Restrictions linked to Russia and Belarus

[NBU Resolution No. 18 on the banking system under martial law](#) (edition of 17 September 2026) suspends outgoing operations from accounts of Russian and Belarusian residents and of companies they beneficially own, apart from listed exceptions such as taxes, utilities, salaries and transfers to state accounts. Banks must therefore capture residence and beneficial ownership in a way that allows these restrictions to be applied.

Accounts for service members

During martial law, banks identify and verify members of the Armed Forces and conscripts on the basis of a military ID or officer's certificate when opening accounts (Resolution No. 18, paragraph 20-2). Resolution No. 153 also allows banks to accept certain expired passports and residence permits when a person has no other document, provided data is updated later.

8

Risk indicators and red flags

BANKING ONBOARDING AND ACCOUNT RISK INDICATORS

- **Aggressor-state links:** owners, residence or funds traced to Russia, or transfers through institutions located there.
- **Third-party pressure:** signs during video verification that someone else is directing the applicant.
- **Register mismatch:** beneficial ownership data differs from the state register or ownership is opaque.
- **Shell company features:** the applicant cannot rebut indications of fictitious activity.
- **Virtual asset activity:** clients operating in virtual assets, which the NBU treats as high risk.
- **Unexplained cash:** cash deposits at the threshold level without documents on their source.
- **Refused documents:** customers who do not provide information needed for due diligence.

Enforcement and penalties

Since 1 January 2025, the NBU sanctions banks for AML breaches under Article 73 of the Law on Banks rather than Article 32 of the AML law (Article 32(9)). Measures include written warnings, fines, removal of officials and licence revocation. The 1% of share capital cap on general bank fines does not apply to AML fines, which are capped at 7,950,000 times the non-taxable minimum income of citizens. Measures can be applied within six months of detecting a breach and no later than three years after it was committed, and the NBU publishes them.

For other entities, Article 32(5) of the AML law sets tiered maximums expressed in non-taxable minimums: up to 12,000 for due diligence breaches, up to 20,000 for reporting failures, up to 100,000 for asset freezing breaches, and up to 10% of annual turnover (capped at 7,950,000) for failing to organise financial monitoring.

In June 2026 the NBU fined PUMB UAH 10 million for inadequate due diligence on new and existing clients, failing to apply enhanced measures to a high-risk client, not rating as high risk clients whose beneficial owners are citizens of the aggressor state, late threshold reporting and failing to end relationships with clients who withheld CDD documents ([NBU release, 7 July 2026](#)).

Recent changes and what to watch

- **10 October 2026** **In force, 3-month transition** NBU Resolution No. 116 amends Resolution No. 65, including stricter rules on liveness photos in the credit bureau verification method; banks must update procedures by January 2027.
- **17 July 2026** **In force** NBU Resolution No. 81 adds rules for commercial agents of financial inclusion banks and prohibits identification methods not listed in Resolution No. 65.
- **26 June 2026** **In force** Law No. 4465-IX introduces financial inclusion banks with a limited licence and lets the NBU set special due diligence rules for them.
- **10 January 2026** **In force** The restated BankID Regulation lets non-bank payment providers act as identity providers.
- **Pending** **Proposed, second reading pending** Bill No. 8153 on personal data protection, adopted at first reading on 20 November 2024, would replace Law No. 2297-VI with a GDPR-style regime and a new supervisory authority.
- **When martial law ends** **Temporary relief** Resolution No. 153 measures, including the larger simplified tier, lapse; under the AML law, banks must then check the source of

restricted cash deposits and report assets frozen under the martial-law rule within 30 days.

11 What this means for identity verification

Remote onboarding must map to one of the NBU's listed methods; a generic document-plus-selfie flow is not, on its own, a permitted method. Supporting chip reading of ID cards with passive authentication and accepting Diia e-passports removes the need for visual security-feature checks in video sessions. Liveness detection is required for several routes, and photo metadata must match the verification date and must not be edited. Every session needs explicit recorded consent, a qualified electronic seal or signature and timestamp on electronic copies, and storage that prevents modification for at least five years after the relationship ends. Screening must cover sanctions, PEPs and aggressor-state links at onboarding and through ongoing monitoring, and expired-document relief during martial law requires data updates later.

IDENTOMAT

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:

- Video KYC sessions with recorded consent, document checks and a final one-time password, mapped to the NBU's video verification steps.
- ID document capture and verification, including NFC chip reading with passive authentication for ID cards and biometric passports.
- Biometric liveness and face match for remote verification routes that require a liveness-checked photo.
- AML screening against sanctions, PEP and watchlists at onboarding and through ongoing monitoring.
- KYB and beneficial owner verification for business customers, with an audit trail for each check.

[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, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення" № 361-IX від 06.12.2019 [Law on Prevention and Counteraction to Money Laundering, Terrorist Financing and Proliferation Financing], edition of 26.06.2026, Articles 2, 7, 8, 11, 12, 18, 20, 32, Section X, zakon.rada.gov.ua
- Закон України "Про банки і банківську діяльність" № 2121-III від 07.12.2000 [Law on Banks and Banking], edition of 04.10.2026, Articles 8-1, 19, 19-2, 31, 73, zakon.rada.gov.ua
- Закон України № 4465-IX від 03.06.2025 щодо розвитку фінансової інклюзії [Law on developing financial inclusion], Final Provisions, zakon.rada.gov.ua
- Закон України "Про систему гарантування вкладів фізичних осіб" № 4452-VI [Law on the Household Deposit Guarantee System], edition of 04.10.2026, Article 26, zakon.rada.gov.ua
- Закон України "Про захист персональних даних" № 2297-VI [Law on Personal Data Protection], edition of 14.06.2025, Article 7, zakon.rada.gov.ua
- Постанова Правління НБУ № 65 від 19.05.2020, Положення про здійснення банками фінансового моніторингу [Regulation on Financial Monitoring by Banks], edition of 17.07.2026, paragraph 60, Annexes 2 and 3, zakon.rada.gov.ua
- Постанова Правління НБУ № 116 від 07.10.2026 [Amendments to NBU financial monitoring regulations], officially published 09.10.2026, bank.gov.ua
- Постанова Правління НБУ № 153 від 20.12.2024 [Regulation on financial monitoring requirements during martial law], paragraphs 14 to 24, bank.gov.ua
- Постанова Правління НБУ № 18 від 24.02.2022 "Про роботу банківської системи в період запровадження воєнного стану" [Operation of the banking system under martial law], edition of 17.09.2026, paragraphs 15 and 20-2, zakon.rada.gov.ua
- Постанова Правління НБУ № 32 від 17.03.2020, Положення про Систему BankID НБУ [Regulation on the NBU BankID System], edition of 10.01.2026, zakon.rada.gov.ua
- NBU release on measures applied in June 2026, 7 July 2026, bank.gov.ua
- Verkhovna Rada Human Rights Committee, transcript of 3 December 2025 on bill No. 8153, kompravlud.rada.gov.ua