Identomat

COMPLIANCE GUIDE

Fintech & Digital Payments Compliance in Azerbaijan

COUNTRY Azerbaijan

INDUSTRY Fintech & Digital Payments

LAST UPDATED 13 November 2026

KEY REGULATORS Central Bank of the Republic of Azerbaijan · Financial Monitoring Service

Key takeaways

- Any non-bank that moves money, issues cards or wallets, or acquires card payments in Azerbaijan needs a licence from the Central Bank of the Republic of Azerbaijan (CBAR); a firm that only shows customers their account data needs a CBAR registration instead.
- Licensed payment and e-money institutions must run full anti-money laundering (AML) checks; only firms that solely initiate payments or aggregate account data are outside the AML law.
- Opening an account remotely for a new customer requires an enhanced electronic signature, a database check, two-factor authentication and video identification with a liveness test and a face match against the state photo record.
- Online onboarding is treated as higher risk by law, remote accounts cannot be opened for non-resident companies or through an authorised representative, and document verification may finish up to 5 working days after opening only with usage limits in place.
- From 1 January 2027, transfers by individuals must also be reported once their monthly total passes AZN 50,000, and crowdfunding platforms become AML obliged entities on 24 January 2027.

Azerbaijan is open to fintech, but only through a domestic licence. The Law on Payment Services and Payment Systems, in force since 9 November 2023, gave payment institutions and e-money institutions their own licensing regime under CBAR, which also supervises their AML compliance. The Financial Monitoring Service (FMS), the national financial intelligence unit, sets the customer due diligence (CDD) detail and receives all reports.

The biggest obstacle for a new entrant is the remote onboarding standard: two overlapping rulebooks, one from the FMS and one from CBAR, prescribe the checks for every first-time remote customer, and remote relationships with non-resident legal entities are not allowed at all.

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

Regulator	Remit	Level	Official site
Central Bank of the Republic of Azerbaijan (CBAR)	Licenses and supervises payment institutions, e-money institutions and payment system operators; registers payment agents; AML supervisor of all financial institutions	National	cbar.az
Financial Monitoring Service of the Republic of Azerbaijan (FMS)	Financial intelligence unit; sets CDD, risk and reporting rules; receives threshold and suspicious transaction reports	National	fiu.gov.az
Ministry of Digital Development and Transport	Personal data authority (Presidential Decree No 361); since 2 June 2026 its National Cybersecurity Agency keeps the register of personal data systems and examines complaints	National	mincom.gov.az
MONEYVAL (Council of Europe)	Evaluates Azerbaijan against the FATF standards	Supranational	coe.int

Banks and the postal operator use their own licences (art. 48.4).

2 Licensing and authorisation

The Law of the Republic of Azerbaijan on Payment Services and Payment Systems No 987-VIQ of 14 July 2023 lists seven payment services (art. 3.1). Payment institutions, e-money institutions and payment system operators may operate only after receiving a CBAR licence (art. 48.1). Only banks, foreign bank branches, the postal operator and e-money institutions may issue e-money (art. 12.1).

CBAR decides within 60 calendar days (art. 50.1), with 15 working days to flag correctable deficiencies. Licences have no expiry date and cannot be transferred (art. 48.5). CBAR refuses a licence where controllers or beneficial owners fail the fit-and-proper test or the source of initial capital is unknown (art. 50.6). The state duty is AZN 2,000 for a payment institution and AZN 3,000 for an e-money institution (Law on State Duty, art. 22.0.34-2).

Activity	Authorisation	Minimum charter capital
Cash services, transfers, cards, issuing or acquiring	Payment institution licence	AZN 500,000
Money remittance only	Payment institution licence	AZN 100,000
Payment initiation only	Payment institution licence	AZN 100,000
Account information only	CBAR registration (art. 48.3)	None; liability insurance or guarantee of at least AZN 50,000 per 100,000 users
E-money issuance	E-money institution licence	AZN 750,000

Source: CBAR Board Decision No 01/2 of 10 January 2024, sections 3.1 to 3.3; volume-linked total capital also applies (section 4).

Foreign providers. A foreign payment or e-money institution may serve the market through a licensed local branch (art. 52), or a local provider may contract with it if the foreign firm is licensed and AML-supervised at home; CBAR must be notified within 5 working days of signing or ending the contract (art. 53). **Agents.** Banks, payment institutions and e-money institutions may use domestic payment agents for cash, transfer and remittance services after CBAR enters the agent in its register, within 10 working days of notification (art. 9.2 to 9.3).

CBAR can order corrective measures, suspend payment services or agent networks (art. 63), and revoke a licence, including for AML violations or for not starting operations within 12 months (art. 54).

3 AML, KYC and customer due diligence

The Law on the Prevention of the Legalization of Criminally Obtained Property and the Financing of Terrorism (No 781-VIQ of 30 December 2022) (the AML/CFT Law) names payment institutions and e-money institutions as financial institutions and obliged entities, except payment institutions that provide only payment initiation or account information services (art. 1.1.8). CBAR is their AML supervisor (art. 16.1.1), and the AML/CFT Law applies to them in the manner CBAR determines (art. 16.5).

When CDD applies

Before a business relationship; before any occasional transaction of AZN 20,000 or more, including linked transactions; before one-off electronic transfers under CBAR rules; on suspicion; and when earlier data are doubtful (art. 4.2).

What CDD covers

Identify and verify the customer, any representative and the beneficial owner from reliable independent sources, establish the purpose of the relationship and build a customer profile (art. 4.4). If CDD cannot be completed, no account, no transaction, and a report to the FMS (art. 4.14).

Beneficial ownership

Natural persons holding a significant participation of 10% or more of capital or votes, then those with control by other means, then senior management (art. 1.1.20, 4.7). Beneficial owner data found in CDD go to the FMS within 3 working days (art. 11.11).

Politically exposed persons

Risk system to detect politically exposed persons (PEPs), management approval, source of wealth and ongoing enhanced due diligence (EDD) (art. 7.1). Every transaction by a foreign PEP is reported regardless of amount (art. 11.3.1).

The FMS "Rules on verification measures, identification of risk factors and attribution of the customer profile to risk groups during the application of customer compliance and new technologies" (Decision No 3-21-28/3-6-4/2023 of 21 February 2023, the FMS Rules) list the data to collect, including FİN (personal identification number), employer and income (point 2.1.1). Profiles are refreshed at least yearly for high-risk, every two years for medium-risk and every three years for low-risk customers, and continuously for PEPs (point 8.1). Simplified due diligence requires assessed low risk (AML/CFT Law art. 4.18).

Reporting, holds and retention

FMS Decision No 3-21-28/3-6-8/2023 of 27 April 2023 sets the reporting thresholds for financial institutions: cash transactions and electronic transfers of AZN 20,000 or more (AML/CFT Law art. 11.1). Threshold and foreign-PEP reports are due within 3 working days; reports where CDD failed and on sanctioned persons' assets immediately, and in any case by the end of that working day (art. 11.4). On suspicion, a financial institution must hold for 2 working days, and report before execution, transactions linked to high-risk profiles, transactions of AZN 200,000 or more and transactions moving funds out of an account (art. 11.5). Tipping off is prohibited (art. 11.10). Records are kept for at least 5 years after the transaction or the end of the relationship (art. 6.1, 6.2).

Under the Law of the Republic of Azerbaijan on Targeted Financial Sanctions No 782-VIQ of 30 December 2022, obliged entities freeze designated persons' assets without delay (immediately or within a few hours) once the designation is published on the targeted financial sanctions information resource, without notice, and inform the designated body and the FMS immediately through it (art. 1.1.11, 5.1).

4 Identity verification and onboarding

Accepted documents. The annex to the FMS Rules lists, among others, the national identity card for citizens; a foreign passport, Azerbaijani residence permit or treaty border-crossing document for foreigners; and the stateless person's identity card or residence permit. Name, date of birth, registered address and citizenship are verified against one of these (point 6.1.1.1).

FMS Rules: four mandatory measures. For a first-time relationship created through new technologies without direct contact, four verification measures are mandatory together (point 7.2):

- confirmation of the application with the customer's enhanced electronic signature;
- checking the data provided against electronic databases or independent external sources;
- strong customer authentication using two or more independent elements of knowledge, possession and inherence (such as face recognition);
- identity verification through a real-time video call or a video recording made through the system.

CBAR Regulation on remote opening of accounts. CBAR Board Decision No 44/5 of 16 December 2025, in force since 30 March 2026, applies to payment accounts at payment institutions (other than initiation-only or information-only firms) and e-money institutions.

It allows identification by photo capture, video recording or video call (point 5.4), but also requires the FMS verification measures (point 4.4), so a first-time remote customer still needs the FMS video step: a real-time video call or a system video recording (which CBAR's automated video recording satisfies), not a still photo alone. Software-based liveness detection must ask for at least three actions in random order, and the face is matched by software against the customer's photo in the state information system (points 5.7, 5.8). Data and documents are confirmed, and the account contract signed, with an enhanced electronic signature (points 4.2, 6.3); the State Tax Service names ASAN İmza (certificates issued by its ASAN Certification Services Center), e-imza and SİMA İmza as enhanced electronic signatures.

If identity cannot be established, remote onboarding must be refused (FMS Rules point 7.3; Decision No 44/5 point 6.5), and the account contract is concluded only after CBAR's identification steps are passed (point 6.1). Document-based verification of the CDD data may finish after the relationship starts, within 5 working days, only with limits on the number, type and amount of transactions meanwhile (FMS Rules points 6.4, 6.5).

Reliance. A firm may rely on another obliged entity's CDD but stays responsible (AML/CFT Law art. 5.1).

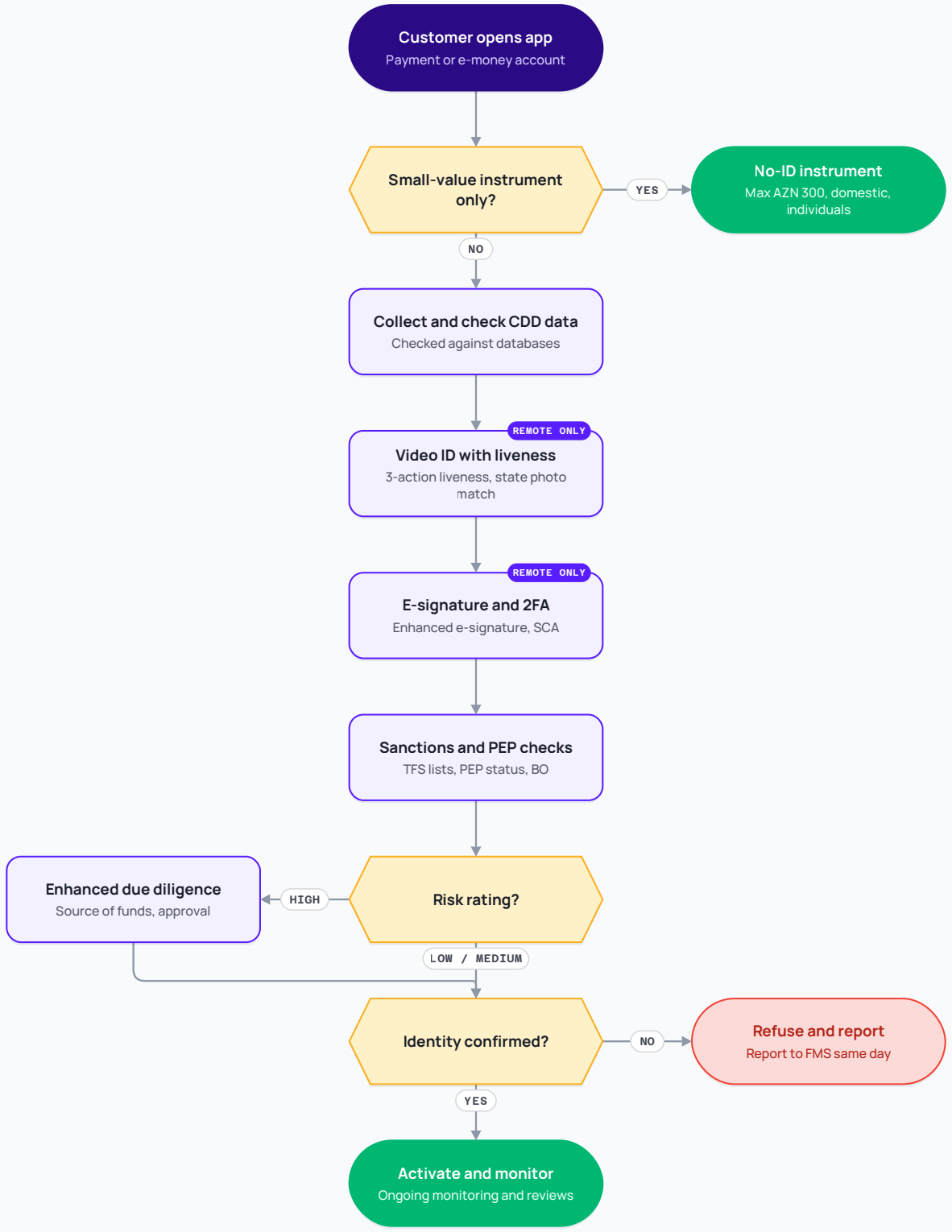


Figure 1. Remote onboarding of a new customer by a payment or e-money institution in Azerbaijan.

5 Digital channels: what's different

Bottom line: remote onboarding is permitted but is classed as high risk by statute, and every first-time remote customer must pass an enhanced e-signature, a database check, two-factor authentication and biometric video identification; in-person onboarding has no equivalent list.

Requirement	In person	Online / remote	Difference
Risk treatment	Risk-based; face-to-face channels may be low risk	Treated as high risk (AML/CFT Law art. 8.1)	Differs
Verification methods	Identity document checked	E-signature, database check, 2FA and video all required	Differs
Biometrics	None prescribed	Liveness (3 random actions) and face match to state photo	Differs
Who can be onboarded	Residents, non-residents, representatives	No non-resident legal entities; no authorised representatives	Differs
Timing of verification	Before the relationship	Document checks up to 5 working days after, with limits	Differs
Account access and payments	Card at terminal; SCA for cash withdrawal	SCA for remote access and electronic payments	Differs
CDD triggers and thresholds	AZN 20,000 occasional; all relationships	Same	Same
Reporting and record keeping	FMS reports; 5-year retention	Same; video, audio, images and logs kept too	Same
Sanctions freezing	Without delay	Same	Same

Remote means high risk, by law

AML/CFT Law art. 8.1 treats relationships created through new technologies as high-risk. The FMS Rules list non-face-to-face channels, mobile banking and cards ordered online among high-risk delivery channels (point 3.11).

Who cannot be onboarded remotely

The FMS Rules bar remote relationships through an authorised representative (other than a legal entity's legal representative) and with non-resident legal entities (point 7.4). CBAR's rules likewise bar representatives, except a legal entity's legal representative and parents, adopters or guardians acting for an individual (Decision No 44/5 point 3.2).

Strong customer authentication

The Payment Services Law requires strong customer authentication (SCA) for remote account access and electronic payments (art. 35). CBAR Board Decision No 12/2 of 13 March 2024 caps failed attempts at three, limits idle app sessions to 5 minutes, and exempts contactless payments of up to AZN 100 (AZN 500 a day) and remote payments of up to AZN 60 within cumulative limits. The exemption for e-commerce payments ended on 1 January 2026.

6 Data protection and biometrics

The Law of the Republic of Azerbaijan "On Personal Data" No 998-IIIQ of 11 May 2010 applies in full to biometric data, expressly including facial images, voice and signatures (art. 9.5), which covers selfie, liveness and video-call data. Outside processing mandated by law, consent is required, and can be given through the Electronic Government Information System (EGIS) (art. 8.1, 8.2); CBAR Decision No 44/5 requires written consent before remote identification (point 5.2). Personal data information systems must be registered before processing (art. 15.1, 15.2). The Ministry of Digital Development and Transport remains the authority (Presidential Decree No 361, point 3.1), but since 2 June 2026 the state register is kept, and complaints are examined, by the National Cybersecurity Agency under the Ministry (Presidential Decree No 676, Charter points 3.1.24, 3.1.25). Data are destroyed once the purpose is achieved (art. 9.4); for CDD records, not before the AML/CFT Law's 5-year retention ends. Cross-border transfer is prohibited where the recipient country's protection falls short, unless the subject consents (art. 14).

7 Sector-specific obligations

Electronic transfer data (wire transfer rule)

CBAR's Regulation on customer due diligence during wire transfers (Decision No 09/1 of 22 February 2023, extended to payment and e-money institutions by Decision No 52/2 of 24 December 2024) requires the payer's name, identification data and account or card number, and the payee's name and account, to travel with each transfer (point 3.1). The payer's institution verifies the payer first; where CDD cannot be performed, this does not apply to one-off domestic transfers of up to AZN 500 to a bank account (point 3.2). The payee's institution applies CDD to the payee, except domestic one-off transfers of AZN 100 or less (point 5.2), and must detect incomplete transfers in real time or within 5 working days (point 5.3).

Small-value and unidentified instruments

The Payment Services Law allows payment instruments whose users need not be identified under CBAR rules (art. 20.2, 40.1.2), and the AML/CFT Law applies to payment and e-money institutions as CBAR determines (art. 16.5). CBAR Decision No 12/3 of 13 March 2024 (Regulation on maintaining payment operations and on payment instruments, as amended 12 November 2025) sets the conditions: monthly top-ups and the stored balance each at or below AZN 300, domestic payments only and individuals only; balances are refunded non-cash under the wire transfer rule, or in cash up to AZN 50 a month (points 12.1, 12.2, 13.2). The FMS Rules still class prepaid and anonymity products as potentially high-risk (point 3.10).

Safeguarding and carrier billing

Funds received by payment and e-money institutions are not deposits; no interest may be paid and they cannot fund lending (Payment Services Law art. 5.4). Mobile operators may charge digital content to phone bills without a licence only up to AZN 50 per transaction and AZN 250 per subscriber per month (CBAR Decision No 01/2, point 1.3).

8 Risk indicators and red flags

PAYMENT AND E-MONEY TYPOLOGIES (FMS)

- **Money mules**: accounts used for other people's purposes (FMS Rules point 3.9.8).
- **Wallet to card to cash**: several customers' cards funded from e-wallets, then cashed out quickly at ATMs.
- **Micro top-ups**: intensive small credits from e-wallets to a single card account.
- **Unknown-source layering**: e-wallet funds of unknown origin forwarded to other people's accounts.
- **Anonymous payments**: electronic payments that cannot be fully identified or verified.
- **Unrelated payers**: payments received from unrelated or unknown third parties (point 3.13.3).

Wallet items: FMS special indicators, 11 December 2019. FMS criteria are non-binding; firms set their own (FMS FAQ).

9 Enforcement and penalties

AML breaches are administrative offences under art. 598 of the Code of Administrative Offences (restated by Law No 783-VIQD of 30 December 2022), decided by district courts; institution and official are fined separately:

Breach	Institution	Official
CDD, record keeping or reliance (per customer and transaction); internal controls; PEP rules (per PEP and transaction); new technologies (art. 598.1)	AZN 20,000 to 30,000	AZN 2,000 to 4,000
Reporting to the FMS, per transaction (art. 598.4)	AZN 20,000 to 30,000	AZN 2,000 to 4,000
Not holding a transaction as required, per transaction (art. 598.5)	AZN 30,000 to 40,000	AZN 3,000 to 5,000

Ignoring an FMS suspension order, per transaction (art. 598.6)	AZN 40,000 to 50,000	AZN 4,000 to 6,000

Because fines accrue per count, CBAR-published totals exceed the single ranges: in September 2025 AFB Bank was fined AZN 50,000 and an official AZN 10,000 under articles 598.1.1, 598.1.2 and 598.1.5; in August 2026 non-bank credit organisation İdeal Kredit was fined AZN 50,000 and an official AZN 6,000.

10 Recent changes and what to watch

- **24 January 2027** `Adopted, effective 24 Jan 2027`: Law No 451-VIIQD of 14 July 2026, adopted with the new Law on Crowdfunding, adds crowdfunding platform operators to the AML/CFT Law's financial institutions.
- **1 January 2027** `Adopted, effective 1 Jan 2027`: FMS Decision No 3-21-28/3-6-7/2026 of 21 April 2026 adds a monthly aggregation test: once an individual's (not a sole proprietor's) electronic transfers exceed AZN 50,000 in a calendar month, every further transfer that month is reported. FMS Decision No 3-21-28/3-6-17/2026 moved the start from 1 October 2026.
- **30 March 2026** `In force`: CBAR Decision No 44/5 set uniform remote account opening rules, including liveness detection and face matching against the state photo record, for banks, payment institutions and e-money institutions.
- **23 January 2026** `Published`: MONEYVAL(2025)16 (adopted 10 November 2025) re-rated R.8, R.14 (money transfer services), R.16 (wire transfers), R.24, R.26, R.33 and R.34; R.15 (new technologies) remains partially compliant.
- **1 January 2026** `In force`: the transitional SCA exemption for e-commerce payments expired.
- **12 November 2025** `In force`: CBAR Decision No 40/11 measured the AZN 300 small-value limit by monthly top-ups and allowed balance refunds of unidentified instruments, in cash up to AZN 50 a month.

11 What this means for identity verification

- **Combine checks:** remote flows need an enhanced e-signature, a registry check, two-factor authentication and video identification, not a choice between them.
- **Liveness and face match:** active liveness with at least three random actions, plus a software match against the state photo record.

- **Biometric data:** obtain written consent and register the processing system in the state register kept by the National Cybersecurity Agency.
- **Limits while pending:** if document verification is deferred, cap transactions until it completes, within 5 working days.
- **Retention:** keep video, audio, images, logs and CDD results for at least 5 years after the relationship ends.

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:

- Remote onboarding that combines ID document capture, database checks and video KYC, matching the four checks required for first-time remote customers.
- Biometric liveness and face match as an inherence factor alongside phone verification for two-factor authentication.
- AML screening against sanctions and PEP lists at onboarding and through ongoing monitoring.
- KYB and beneficial owner verification down to the 10% significant participation threshold.
- No-code workflow builder to apply limits while verification is pending and to route high-risk customers to enhanced checks, with an audit trail.

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

- **Law on the Prevention of the Legalization of Criminally Obtained Property and the Financing of Terrorism (No 781-VIQ of 30 December 2022)** (Cinayət yolu ilə əldə edilmiş əmlakın leqallaşdırılmasına və terrorçuluğun maliyyələşdirilməsinə qarşı mübarizə haqqında), arts 1, 4 to 8, 11, 16, e-qanun, e-qanun.az/framework/53369
- **Law No 987-VIQ of 14 July 2023 on Payment Services and Payment Systems** (Ödəniş xidmətləri və ödəniş sistemləri haqqında), arts 3, 5, 9, 12, 13, 20, 35, 40, 48 to 54, 63, e-qanun, e-qanun.az/framework/54872
- **FMS Decision No 3-21-28/3-6-4/2023 of 21 February 2023, Rules on verification measures, identification of risk factors and attribution of the customer profile to risk groups during the application of customer compliance and new technologies**, as amended 14 June 2024, e-qanun, e-qanun.az/framework/53641
- **FMS Decision No 3-21-28/3-6-8/2023 of 27 April 2023 on reporting rules and thresholds**, e-qanun, e-qanun.az/framework/54120
- **FMS Decision No 3-21-28/3-6-7/2026 of 21 April 2026 amending Decision No 3-21-28/3-6-8/2023**, effective 1 January 2027, points 1.1, 3, and **FMS Decision No 3-21-28/3-6-17/2026 of 25 September 2026** (start date moved from 1 October 2026; point 2 repealed), e-qanun, e-qanun.az/framework/62373
- **CBAR Board Decision No 44/5 of 16 December 2025, Regulation on remote opening of accounts**, in force 30 March 2026, e-qanun, e-qanun.az/framework/61120
- **CBAR Board Decision No 09/1 of 22 February 2023, Regulation on customer due diligence during wire transfers**, as amended by Decision No 52/2 of 24 December 2024, e-qanun, e-qanun.az/framework/53633
- **CBAR Board Decision No 01/2 of 10 January 2024, Regulation on the organization and implementation of activities by payment and electronic money institutions**, sections 1.3, 3, 4, cbar.az/page-831/regulations
- **CBAR Board Decision No 12/3 of 13 March 2024, Regulation on maintaining payment operations and on payment instruments**, as amended 12 November 2025, sections 12, 13, e-qanun, e-qanun.az/framework/56659
- **CBAR Board Decision No 12/2 of 13 March 2024, Regulation on the application of strong customer authentication**, sections 2, 3, e-qanun, e-qanun.az/framework/56660
- **Law No 782-VIQ of 30 December 2022 on Targeted Financial Sanctions**, arts 1.1.11, 5.1, e-qanun, e-qanun.az/framework/53362
- **Law No 998-IIIQ of 11 May 2010 "On Personal Data"**, arts 8, 9, 14, 15, e-qanun, e-qanun.az/framework/19675; **Presidential Decree No 361** on ensuring its implementation, point 3.1, e-qanun.az/framework/21035; **Presidential Decree No 676 of 2 June 2026** on cybersecurity governance and the Charter of the National Cybersecurity Agency, points 3.1.24, 3.1.25, e-qanun.az/framework/61938
- **Code of Administrative Offences**, art. 598 (as restated by Law No 783-VIQD of 30 December 2022), e-qanun, e-qanun.az/framework/46960

- **Law on State Duty**, art. 22.0.34-2, e-qanun, frameworks.e-qanun.az/2/f_2860.html
- **Law No 451-VIIQD of 14 July 2026 amending laws in connection with the Law on Crowdfunding**, arts 11 to 13, President of the Republic of Azerbaijan, president.az/az/articles/view/73098
- **State Tax Service, notices on enhanced electronic signatures**, 15 March 2024 and 26 April 2024, taxes.gov.az/az/post/3246, taxes.gov.az/az/post/3171; ASAN Certification Services Center of the State Tax Service, taxes.gov.az/en/page/asan-imza
- **CBAR, Supervisory actions imposed**, accessed 13 November 2026, cbar.az/page-843
- **CBAR, Register of payment institutions**, cbar.az/page-854
- **FMS, Special indicators for detecting suspicious transactions**, approved 11 December 2019, points 2.1.108 to 2.1.111, fiu.gov.az/az/special-indicators; FMS frequently asked questions, fiu.gov.az/az/faq
- **MONEYVAL, Azerbaijan: fifth round mutual evaluation (13 December 2023) and 1st Enhanced Follow-up Report and Technical Compliance Re-Rating, MONEYVAL(2025)16**, adopted by written procedure 10 November 2025, pages 2 and 5, rm.coe.int; Council of Europe press release of 23 January 2026, coe.int/en/web/portal