Identomat

COMPLIANCE GUIDE

Fintech & Digital Payments Compliance in Armenia

COUNTRY Armenia

INDUSTRY Fintech & Digital Payments

LAST UPDATED 13 November 2026

KEY REGULATORS Central Bank of Armenia · Financial Monitoring Center

Key takeaways

- Money transfer, payment processing and lending businesses need a licence from the Central Bank of Armenia before they serve customers. A payment company must hold at least AMD 100 million of capital.
- Only a bank or a licensed money transfer company can issue e-money (stored value in a wallet); a money transfer company needs an extra Central Bank permission. A user's wallet balance may never exceed AMD 1,000,000.
- Fully remote onboarding is allowed, but a relationship with no face-to-face contact is a high-risk criterion: remote customers are high risk and get enhanced due diligence by default, unless a documented analysis submitted to the Central Bank supports a medium rating. No specific technology, such as video or liveness checks, is prescribed.
- A remotely onboarded customer's first payment must come from an account in their own name at a regulated financial institution. Identity checks may finish up to seven days after onboarding, within limits set in the firm's own policy.
- The Central Bank fined nine payment companies for anti-money laundering failures in August 2026. Since 21 August 2026, money transfer and e-money companies must also run risk-based controls against circumvention of international sanctions, not only UN sanctions.

Armenia is open to online payment and lending businesses, but in practice only through entities licensed in Armenia. One authority covers almost everything: the Central Bank of Armenia licenses and supervises payment and settlement organisations, credit organisations and e-money issuers, and its Financial Monitoring Center receives suspicious and threshold reports from all of them.

The biggest obstacle for a new entrant is that the licence comes before the customer: the payment law reserves payment services to the Central Bank, banks, licensed payment and settlement organisations and those authorised by another law or an international treaty. Once licensed, onboarding rules are principles-based, which leaves room for digital channels but puts the burden of proving their adequacy on the firm.

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 Armenia (CBA)	Licenses and supervises banks, payment and settlement organisations, credit organisations and e-money issuers; sets payment rules and AML minimum requirements; imposes sanctions	National	cba.am
Financial Monitoring Center (FMC)	Armenia's financial intelligence unit, part of the CBA; receives suspicious and threshold reports, keeps the register of reporting entities, issues AML guidance and publishes sanctions lists	National	cba.am (FMC)
Personal Data Protection Agency of the Ministry of Justice	Authorised body under the Law on Protection of Personal Data, acting independently (article 24(2)); must be notified before biometric data are processed (article 23(3))	National	moj.gov.am (structure)
MONEYVAL (Council of Europe)	Evaluates Armenia against the FATF Recommendations; does not supervise firms	Supranational	coe.int/moneyval

2 Licensing and authorisation

The Law on Payment and Settlement Systems and Payment and Settlement Organisations («Վճարահաշվարկային համակարգերի և վճարահաշվարկային

կազմակերպությունների մասին», HO-150-N of 2004, ARLIS 224826) defines payment services broadly, including e-money issuance, processing and clearing (article 17). Under article 18 only the CBA, banks, licensed payment and settlement organisations, the Treasury and persons authorised by another law or an international treaty may provide them. Providing payment services without a CBA licence is prohibited (article 19(4)).

Money transfer licence

For remittance, payment collection and payout services (article 19(1)(a)); holders may also process, clear and convert currency tied to a transfer (article 19(5)).

Processing and clearing licence

For processors and clearing houses for payment instruments and settlement documents (article 19(1)(b)).

E-money permission

Money transfer companies need a separate CBA permission under Regulation 16/1 (Decision 74-N of 13 April 2010, point 2); banks may also issue e-money.

Credit organisation licence

Lending apps need a credit organisation licence under the Law on Credit Organisations (ARLIS 209997, article 3); only licensees may use the term "credit organisation" in advertising (article 4).

The application covers participants and managers (including criminal records of 10% holders), service rules, a business plan and capital; the CBA decides within two months (article 20). Regulation 17/02 (CBA Board Decision 269-N of 14 October 2011) sets minimum total capital at **AMD 100 million** and highly liquid assets of at least 60% of current liabilities, both met on a monthly average basis (points 3, 4 and 7). State duty is AMD 1,000,000 per licence per year (Law on State Duty, articles 8 and 19). E-money issuers' systems must meet the CBA's minimum information security requirements (Regulation 16/1, point 4(3); Decision 173-N of 9 July 2013, based on ISO/IEC 27001).

3 AML, KYC and customer due diligence

The Law on Combating Money Laundering and Terrorism Financing («Փողերի լվացման և ահաբեկչության ֆինանսավորման դեմ պայքարի մասին», HO-80-N of 26 May 2008, ARLIS 210014) makes banks, credit organisations, currency exchange businesses, persons carrying out money transfers and most crypto-asset service providers reporting entities (article 3(1)(4)). Each must register with the FMC within one month of being licensed (article 9). The CBA's minimum requirements regulation (CBA Board Decision 279-N of 7 October 2014, ARLIS 220114, amended by Decision 11-N of 22 January 2026, in force 30 January 2026) adds detail.

When customer due diligence applies

Article 16(2) requires customer due diligence (CDD) when a business relationship is established; for an occasional transaction, including linked transactions and domestic or international money or crypto-asset transfers, of 400 times the minimum wage or more; when there are doubts about identification data; and on suspicion. For thresholds in legal acts the "minimum wage" is a fixed calculation base of AMD 1,000 (Law on Minimum Monthly Wage, article 3), so the occasional-transaction trigger is **AMD 400,000**.

What must be collected

Identity is established and verified from reliable, valid documents issued by a competent state body and other information (article 16(4)). For an individual: name, surname, citizenship, registration address (if any), date and place of birth, and the identity document's series, number and date of issue; the place of residence must also be established. The firm must also verify representatives' authority, identify and take reasonable steps to verify the beneficial owner, and understand the relationship's purpose (article 16(5) and (7)).

Beneficial ownership

A beneficial owner is a natural person who directly or indirectly holds **20% or more** of the voting shares or of the charter capital, or who exercises actual control by other means; the senior manager is the fallback (article 3(1)(14)).

Enhanced due diligence, monitoring and reporting

Enhanced due diligence applies when a high-risk criterion is present, emerges during the relationship, or the FMC instructs it (article 18(2)). Monitoring runs at least annually for standard-risk and six-monthly for high-risk customers (regulation 279-N, point 37), and at least quarterly for politically exposed persons (point 41); other periods need a documented analysis submitted to the CBA (point 41.1). Identification and verification data must be refreshed at least once a year (article 17(2)); point 38's schedule covers other CDD information only.

Report	Trigger for financial institutions	Deadline (money transfer form 105)
Suspicious transaction or relationship	Any amount, including attempts (articles 3(1)(30), 6(2) and 7(1))	Same working day the suspicion criterion is found, or by 12:00 the next working day if impossible

Threshold report, non-cash	AMD 20 million or more (article 6(3)(1))	Within three working days, by 18:00 on the third day
Threshold report, cash	AMD 5 million or more	Within three working days
Threshold report, crypto-assets	AMD 1 million or more	Within three working days

Deadlines follow CBA Board Decision 266-N of 7 October 2014. Records are kept for at least **five years** after the relationship ends or the transaction is carried out (article 22), on paper or electronically (regulation 279-N, point 51).

4 Identity verification and onboarding

Neither the AML law nor regulation 279-N lists approved remote methods, sets a liveness or presentation-attack standard, or certifies identity providers. Instead, article 18(3) requires policies for managing non-face-to-face risks, including identification and verification, and the evidence must still be a valid state-issued document (article 16(4)). Since 1 August 2026, e-money issuers must document their wallet-opening CDD procedures (Regulation 16/02, point 8(20)).

Delayed verification

Verification may follow onboarding within no more than **seven days** if the risk is effectively managed and delay avoids interrupting normal business (article 16(1)); policy must limit the transactions allowed meanwhile (article 18(3.1)).

Reliance on third parties

A firm may rely on another institution's CDD but keeps ultimate responsibility and must obtain the information immediately from an AML-regulated party outside non-compliant countries (article 16(8)).

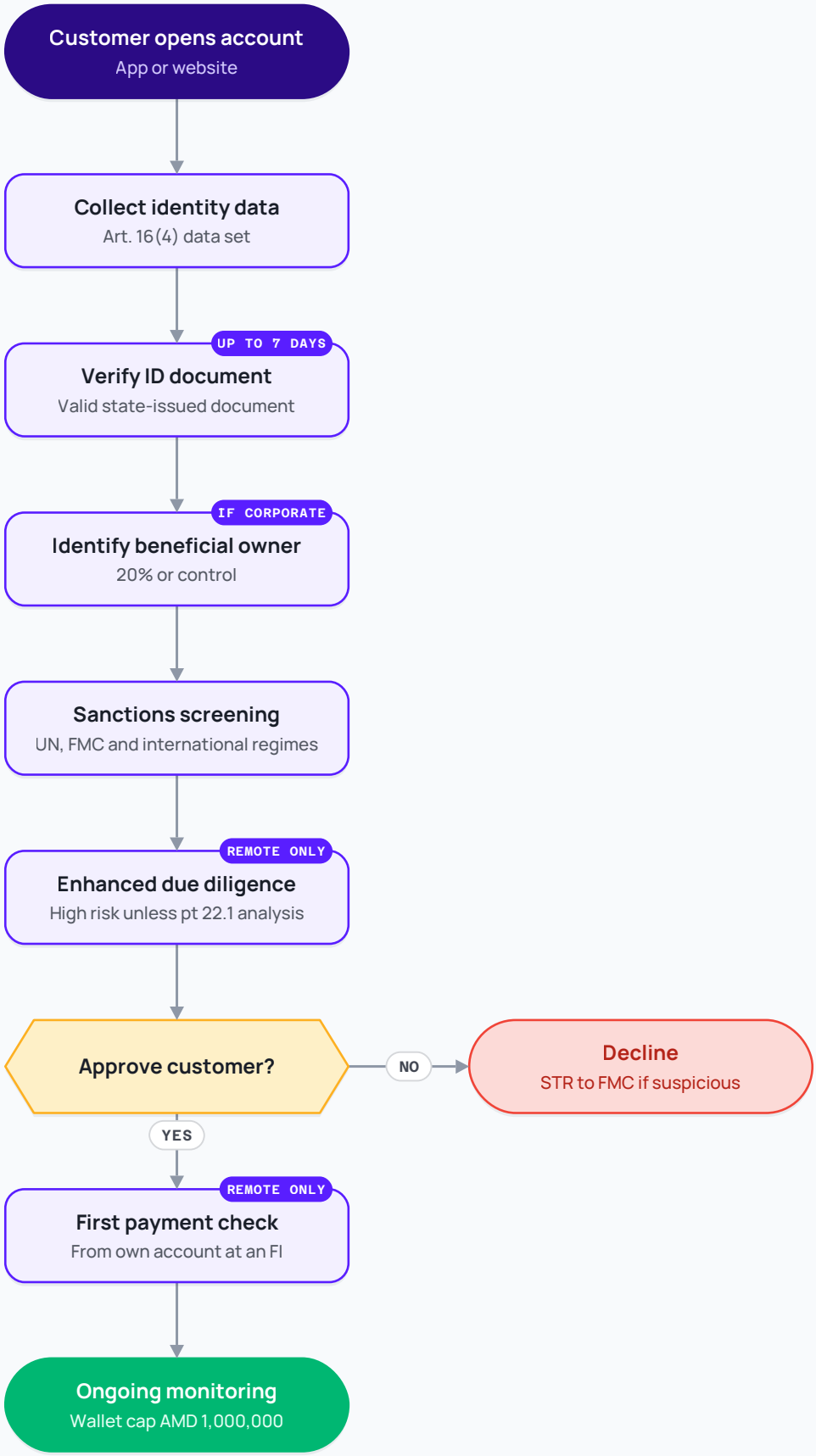


Figure 1. Fully remote onboarding for an Armenian payment or e-money app.

5 Digital channels: what's different

Bottom line: remote onboarding is permitted, but a relationship with no face-to-face contact is high risk by default, bringing enhanced due diligence unless a documented analysis submitted to the CBA supports a medium rating, plus a first payment from the customer's own account.

Requirement	In person / branch	Online / remote	Difference
Permission to onboard	Allowed	Allowed, with non-face-to-face risk policies (art. 18(3))	Differs
Risk classification	Risk-based	High risk by default unless a documented analysis supports medium (reg. 279-N pts 27(6), 22.1, 23)	Differs
First payment	No specific rule	From the customer's own account at a regulated FI (pt 40)	Differs
CDD data and documents	Art. 16(4) data, state-issued document	Same	Same
Approved verification methods	None prescribed	None prescribed	Same
Verification timing	Up to 7 days after onboarding (art. 16(1))	Same	Same
E-money balance limit	AMD 1,000,000 per user	Same	Same
Record retention	5 years, paper or electronic	Same	Same

Remote onboarding as a high-risk criterion

Regulation 279-N lists a transaction or business relationship without face-to-face contact as a high-risk criterion (point 27(6)). Risk is high if even one high-risk criterion applies

(points 23 and 25), triggering enhanced due diligence (article 18(2)). The exceptions: a firm may rate it medium after a comprehensive, documented analysis concluding the risks are effectively managed, submitted to the CBA as authorised body (point 22.1), and listed low-risk transactions can lower the rating (point 24). The CBA Guideline limits the criterion to relationships run entirely without face-to-face contact, payments included; face-to-face identification at some stage takes a relationship out of it (paragraph 1.3.2, note 40). App-only onboarding is therefore high risk by default.

The first-payment rule

For a non-face-to-face relationship, the first payment must come from an account in the customer's name at a financial institution meeting the article 16(8)(3)(a) to © conditions: AML-regulated, able to provide CDD data, outside non-compliant countries (regulation 279-N, point 40).

Wallets after the August 2026 reform

Regulation 16/02 (CBA Board Decision 2-N of 13 January 2015) caps e-money held in each user's accounts at AMD 1,000,000 equivalent at any time, however many accounts the user has (point 19). CBA Decision 177-N, in force since 1 August 2026, removed the requirement to link a bank account or card in the user's name before opening a wallet and identification through Armenian bank cards, allowed cash top-ups and redemptions, and repealed the 2022 restrictions on transfers combining cash and e-money accounts.

6 Data protection and biometrics

The Law on Protection of Personal Data («Անձնական տվյալների պաշտպանության մասին», HO-49-N, ARLIS 229131, amended 7 May 2026) governs identity data collected at onboarding. Biometric data need the data subject's consent unless a law provides otherwise (article 13), and the AML law does not mandate biometrics. Consent is given in writing, or electronically certified with an electronic digital signature; oral consent only through reliable actions that clearly show it (article 9(7)), and the processor must prove it (article 9(8)). A tick-box alone may therefore not meet the standard. Before processing biometric data, the processor must notify the Personal Data Protection Agency (article 23(3)). Vendors need written instructions (article 14).

7 Sector-specific obligations

Wire transfer information

Payment orders carry payer and payee names and account numbers or a unique reference; above AMD 400,000 they also carry the payer's document details, address, or date and place of birth (article 20).

Sanctions and asset freezing

Property of persons on lists under United Nations Security Council resolutions, or published by the authorised body in line with them, must be frozen immediately and without notice (article 28). The FMC's 2018 guidance (Decision 1/435-A) requires matching customers and counterparties against the lists, freezing or denying access on a match, and filing a suspicious transaction report (points 8 and 9).

Sanctions-circumvention controls

CBA Board Decision 25-N of 30 January 2026 (published 20 February 2026, in force 21 August 2026) applies to money transfer licensees and e-money issuers. "International sanctions" means measures by any international organisation or state, applied as they affect the firm (points 2 and 3). Risk-based controls must cover assessment, mitigation, monitoring, testing and reporting (point 2). Monitoring covers customers, counterparties, currencies and place of operation, and at least annually participants, staff and management (point 24). Customer checks consider linked persons, beneficial owners, citizenship, actual residential address and tax residence (point 25), at onboarding and within one working day of list or data changes (point 27); transactions are screened before execution (point 28). Firms weigh geography, keywords and the origin of goods (point 23) and run transaction-monitoring scenarios (point 31).

Safeguarding customer funds

Customer funds not yet paid out, including against e-money issued, must be kept separate and, from the end of the working day after receipt, held in a dedicated bank account or covered by insurance or a bank guarantee (Regulation 17/02, point 19). In July 2026 the CBA fined one organisation AMD 1,500,000 for breaches including 111 days of unprotected funds.

8 Risk indicators and red flags

PAYMENT AND E-MONEY INDICATORS FROM THE CBA GUIDELINE (1/711-A, AMENDED BY 1/347-A) AND DECISION 25-N

- **High-risk IP addresses**: online transactions where a participant's IP address is in a non-compliant (high-risk) country (2.2.2.59).
- **Betting flows**: transfers of large number or volume to the accounts of online bookmakers (2.2.2.61).
- **Overpay and refund**: overpaying into the tax authority's account from cards of unknown origin or foreign cards, then claiming a refund soon after without reasonable grounds (2.2.2.63).
- **Document anomalies**: only copies of identity documents, documents bearing signs of alteration or falsification, or a different identity document each time (2.1.1.4 to 2.1.1.6).
- **Unreachable contacts**: phone numbers that do not answer, are disconnected or do not exist; mail-drop addresses (2.1.1.9, 2.1.1.10).
- **Crypto links**: funds from or to a platform not registered in the country of the customer or of the wallet provider, or an address known to be linked to terrorism or its financing (2.2.2.64, 2.2.2.66).
- **Sanctions evasion**: exposure to heavily sanctioned countries, cities or regions, sanctions keywords, or goods and technology from sanctioned sources (Decision 25-N, point 23).

9 Enforcement and penalties

The AML law does not fine financial institutions directly: breaches of the AML law or the acts adopted under it lead to the measures in the institution's own sector legislation (article 30(2)). For payment and settlement organisations, article 27 of the payment law provides a warning with an order to remedy, a fine, withdrawal of a manager's qualification certificate, and licence suspension or revocation. The first three can be combined for each breach (article 27(2)), so total fines can exceed the per-breach cap.

Measure	Limit	Basis

Fine on the organisation	Up to 500 times the minimum wage (AMD 500,000) per breach, unless legislation provides otherwise	Payment law, art. 27(4)
Fine on a manager	Up to 300 times the minimum wage (AMD 300,000), unless legislation provides otherwise	Payment law, art. 27(4)
Licence suspension or revocation	Revocation by CBA Board decision	Payment law, art. 27(1)(d), (e) and (5)

On 10 and 11 August 2026 the CBA sanctioned nine payment and settlement organisations for breaches of the AML law and its implementing acts, after a risk-based assessment. Fines ranged from AMD 800,000 to AMD 2,100,000, with warnings.

10 Recent changes and what to watch

- **31 January 2027** `Deadline, 31 Jan 2027` Crypto-asset service providers active before the Law on Crypto-assets must be CBA-licensed or stop.
- **17 November 2026** `Proposed, comments close 17 Nov 2026` A draft Law on Electronic Identification and Trust Services would set assurance levels for electronic identification and create an Armenian digital identity wallet.
- **21 August 2026** `In force` CBA Decision 25-N on sanctions-circumvention risk applies to money transfer and e-money companies.
- **10 to 11 August 2026** `Enforcement` The CBA fines nine payment and settlement organisations for AML breaches after a risk-based assessment.
- **1 August 2026** `In force` CBA Decision 177-N reforms wallet opening and funding.
- **9 July 2026** `Published` MONEYVAL publishes Armenia's sixth-round evaluation, adopted at its 71st Plenary (26 to 29 May 2026), and places Armenia in enhanced follow-up. It rates financial-sector preventive measures moderately effective.
- **30 January 2026** `In force` CBA Decision 11-N of 22 January 2026 rewrites the low-risk criteria in regulation 279-N (point 28).
- **24 September 2025** `In force` Decision 1/347-A amends the CBA Guideline on the Criteria of High Risk and the Indicators of Suspicious Activity, including the scope of the non-face-to-face criterion.

11 What this means for identity verification

- **Documents:** capture the full article 16(4) data set from a valid state-issued document, not only an image.
- **Remote methods:** document capture, face match, liveness and NFC are permissible; justify the mix in the non-face-to-face policy.
- **Enhanced due diligence by default:** treat app-only customers as high risk unless a documented point 22.1 analysis, submitted to the CBA, supports a medium rating.
- **Funding check:** require the first payment from the customer's own account at a regulated institution.
- **Seven-day window:** limit transactions until verification completes, and stop activity after seven days.
- **Re-verification:** refresh identification data at least once a year and whenever data are in doubt, and retain evidence for five years.
- **Sanctions:** screen customers at onboarding and within one working day of list changes, and transactions before execution, against all relevant regimes.
- **Biometrics:** capture consent in a form that can be evidenced, notify the Agency before processing, and keep a non-biometric fallback.

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 KYC onboarding that captures the full identity data set required by Armenian AML law, with ID document capture and verification, including NFC.
- Face match and biometric liveness with consent capture, plus a configurable non-biometric fallback.
- AML screening against UN and other international sanctions lists and PEP lists at onboarding and through ongoing monitoring.
- KYB and beneficial owner verification for corporate customers at the 20% ownership threshold.
- No-code workflow builder to enforce transaction limits during the seven-day verification window, 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

- **Law on Combating Money Laundering and Terrorism Financing** («Փողերի լվացման և ահաբեկչության ֆինանսավորման դեմ պայքարի մասին», HO-80-N, 26 May 2008, as amended), articles 3, 6, 7, 9, 16, 17, 18, 20, 22, 28 and 30, ARLIS, arlis.am/hy/acts/210014
- **CBA Board Decision 279-N of 7 October 2014, Regulation on minimum requirements for reporting entities in the field of preventing money laundering and terrorism financing** (amended by Decision 11-N of 22 January 2026, in force 30 January 2026), points 22.1, 23, 24, 25, 27, 28, 37, 38, 40, 41, 41.1 and 51, ARLIS, arlis.am/hy/acts/220114; Decision 11-N, point 2, arlis.am/hy/acts/220094

- **Law on Payment and Settlement Systems and Payment and Settlement Organisations** («Վճարահաշվարկային համակարգերի և վճարահաշվարկային կազմակերպությունների մասին», HO-150-N, 24 November 2004, as amended), articles 17 to 20 and 27, ARLIS, arlis.am/hy/acts/224826
- **CBA Board Decision 269-N of 14 October 2011, Regulation 17/02 on the regulation of payment and settlement organisations and their economic standards**, points 3, 4, 7 and 19, ARLIS, arlis.am/hy/acts/127480
- **Law on State Duty** («Պետական տուրքի մասին», as amended), articles 8 and 19 (points 5.9 and 5.10), ARLIS, arlis.am/hy/acts/232761
- **CBA Board Decision 74-N of 13 April 2010, Regulation 16/1 on permission to issue e-money** (as amended by Decision 256-N of 25 September 2026, in force 28 October 2026), points 2 and 4, ARLIS, arlis.am/hy/acts/232744
- **CBA Board Decision 2-N of 13 January 2015, Regulation 16/02 on issuing and servicing (circulating) e-money** (version in force from 1 August 2026), points 8(20) and 19, ARLIS, arlis.am/hy/acts/228432
- **CBA Board Decision 177-N of 30 June 2026 amending Regulation 16/02 and repealing Decision 46-N of 22 March 2022**, ARLIS, arlis.am/hy/acts/228428
- **CBA Board Decision 173-N of 9 July 2013, Procedure on minimum information security requirements**, point 1, ARLIS, arlis.am/hy/acts/160271
- **CBA Board Decision 266-N of 7 October 2014, report form 105 for money transfer providers and the procedure for submitting it**, points 14 and 16, ARLIS, arlis.am/hy/acts/124727
- **Law on Credit Organisations** («Վարկային կազմակերպությունների մասին», 29 May 2002, as amended), articles 3 and 4, ARLIS, arlis.am/hy/acts/209997
- **Law on Minimum Monthly Wage** («Նվազագույն ամսական աշխատավարձի մասին», 17 December 2003, as amended), article 3, ARLIS, arlis.am/hy/acts/172160
- **Law on Protection of Personal Data** («Անձնական տվյալների պաշտպանության մասին», HO-49-N, 18 May 2015, as amended), articles 9, 13, 14, 23 and 24, ARLIS, arlis.am/hy/acts/229131; official English title, arlis.am/en/acts/117034
- **Ministry of Justice, structure: Personal Data Protection Agency**, moj.gov.am
- **CBA Board Decision 25-N of 30 January 2026, Procedure for managing the risk of circumvention of international sanctions by payment and settlement organisations** (published 20 February 2026, in force 21 August 2026), points 1 to 3, 23 to 25, 27, 28 and 31, ARLIS, arlis.am/hy/acts/221300
- **Law on Crypto-assets** («Կրիպտոակտիվների մասին», as amended), article 94, ARLIS, arlis.am/hy/acts/219036; **CBA Board Decision 227-N of 30 December 2025, Regulation 7/01** (in force 31 January 2026), ARLIS, arlis.am/hy/acts/219788
- **CBA Guideline on the Criteria of High Risk and the Indicators of Suspicious Activity in Relation to Money Laundering and Terrorist Financing**, CBA Chairman's Decision 1/711-A of 11 October 2016, amended by Decision 1/347-A of 24 September 2025, paragraphs 1.3.2 (note 40), 2.1.1 and 2.2.2, official English version, cba.am (PDF); Armenian version, cba.am (PDF)

- **FMC guidance on freezing property of persons linked to terrorism or proliferation**, CBA Chairman's Decision 1/435-A of 26 June 2018, cba.am (PDF)
- **CBA sanctions register**, notices of 27 July 2026 and 10 to 11 August 2026 on payment and settlement organisations, cba.am/hy/punishments
- **Draft Law on Electronic Identification and Trust Services and related laws**, Ministry of High-Tech Industry and Artificial Intelligence, public consultation 2 to 17 November 2026, e-draft.am project 10832, e-draft.am
- **MONEYVAL, Armenia: Sixth Round Mutual Evaluation Report** (adopted at the 71st Plenary, May 2026), rm.coe.int; Executive Summary, MONEYVAL(2026)8 SUMM, key findings and ratings table, rm.coe.int; Outcome of the 71st Plenary (26 to 29 May 2026), coe.int; press release of 9 July 2026, coe.int