Identomat

COMPLIANCE GUIDE

Banking & Digital Banking Compliance in Armenia

COUNTRY Armenia

INDUSTRY Banking & Digital Banking

LAST UPDATED 13 November 2026

KEY REGULATORS Central Bank of Armenia · Financial Monitoring Center

Key takeaways

- Only a company holding a banking licence from the Central Bank of Armenia (CBA) may carry on banking activity (taking deposits and lending or investing them at its own risk) or call itself a bank. A new commercial bank needs at least AMD 30 billion of total capital, and the licence process runs in three stages: preliminary approval, registration, then the licence.
- Opening accounts fully online is allowed, but the bank's own rules must cover how it identifies and verifies remote customers. No specific technology, such as video calls or a national digital ID, is prescribed or approved by name.
- A relationship opened without meeting the customer in person is a high-risk criterion under CBA rules. Unless the bank documents an analysis showing the risk is managed and files it with the CBA (which allows a medium rating), or only listed low-risk payments are involved, it triggers enhanced checks, including senior management approval before the account is opened. The customer's first payment must always come from an account in their own name at a regulated financial institution.
- Identity may be verified up to 7 days after the account is opened, but only where the risk is managed and the bank's written policy limits what the customer can do in the meantime.
- Every bank must report cash transactions of AMD 5 million or more, non-cash transactions of AMD 20 million or more and crypto-asset transactions of AMD 1 million or more to the Financial Monitoring Center (FMC, Armenia's financial intelligence unit). Suspicious activity must be reported the same working day.

Armenia's banking market is open to new entrants, including foreign bank branches and subsidiaries, but it is a single-regulator system: the CBA licenses banks, supervises their prudential and anti-money laundering (AML) compliance, and hosts the FMC. There is no separate digital bank licence; a digital-only bank holds the same banking licence as a branch-based one.

The biggest practical obstacle for a digital entrant is the treatment of remote onboarding. The rules permit it, but by classing non-face-to-face relationships as high risk they push fully remote customers into enhanced due diligence unless the bank has documented and filed an analysis supporting a medium rating, so onboarding flows and that analysis have to be designed from the start.

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	Level	Official site
Central Bank of Armenia (CBA)	Bank licensing, prudential supervision, AML supervision of banks and authorised body under the AML law, sanctions for breaches, bank resolution (from 1 January 2027)	National	cba.am
Financial Monitoring Center (FMC)	Financial intelligence unit inside the CBA: receives threshold and suspicious transaction reports and runs the CBA's AML functions, such as registering reporting entities	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 (art. 24(2); Government Decision 734-N of 2 July 2015); receives mandatory notifications before biometric processing	National	moj.am
MONEYVAL (Council of Europe)	Evaluates Armenia's AML and counter-terrorist financing (CFT) regime against the FATF Recommendations	Supranational	coe.int/moneyval

The CBA is the banks' AML supervisor under their sector legislation (AML law, article 3(1)(8)).

2 Licensing and authorisation

The CBA has the exclusive right to grant a banking licence, which is perpetual and not transferable (Law on Banks and Banking, article 23). Only licensed entities may use the word "bank" or its derivatives in their name or advertising (article 6). The licence covers all channels: Armenian law has no separate licence for digital-only or app-based banks.

Step or requirement	Rule	Source
Preliminary approval	Draft charter, three-year business plan, data on significant shareholders; CBA decides within one month; no court appeal	Law on Banks and Banking, arts 25 and 26
Registration	Bank or foreign bank branch registered with the CBA	Art. 27
Licence	Apply within one year of preliminary approval; granted within one month once capital is paid in, premises, systems and managers meet CBA requirements	Art. 29
Capital	Minimum charter capital AMD 1 billion; minimum total capital AMD 30 billion; total capital adequacy at least 11%	CBA Regulation 2 (Decision 39-N of 9 February 2007), points 15 to 17
Owners	Prior CBA consent to acquire 10% or more of voting shares, with evidence of the lawful origin of funds; beneficial owners reported to the CBA	Arts 9 and 18
Deposit guarantee	Cover up to AMD 16 million (dram deposits only) or AMD 7 million (foreign currency only); new bank pays AMD 15 million within ten days of licensing	Law on Guaranteeing Compensation of Bank Deposits of Natural Persons, arts 3 and 13
Registration as a reporting entity	With the CBA as authorised body (via the FMC), within one month of licensing	AML law, art. 9(1)

Deposit-guarantee amendments linked to the new resolution regime (Law HO-368-N) take effect on 1 January 2027 `Adopted, effective 1 Jan 2027`; they leave the coverage amounts unchanged.

3 AML, KYC and customer due diligence

Banks, including branches of foreign banks, are reporting entities under article 3(1)(4) of the AML law. The detailed rules sit in the CBA's Regulation on Minimum Requirements to Reporting Entities in the Field of Preventing Money Laundering and Terrorism Financing (Board Decision 279-N of 7 October 2014, last amended by Decision 11-N of 22 January 2026, in force 30 January 2026).

When customer due diligence applies

Customer due diligence (CDD) is required when a business relationship is established, for occasional transactions (including linked transactions and money or crypto-asset transfers) of 400 times the minimum wage or more, when there are doubts about identification data, and on any suspicion (article 16(2)). Thresholds in laws are calculated on a base of AMD 1,000 rather than the actual minimum wage (Law on Minimum Monthly Wage, article 3), so the occasional-transaction threshold is AMD 400,000; MONEYVAL's 2026 report puts it at about EUR 900. Investment service providers are reporting entities under the same law and CDD rules. Anonymous and numbered accounts, bearer shares and shell banks are prohibited (article 15).

Beneficial ownership

A beneficial owner is a natural person who directly or indirectly holds 20% or more of the voting shares or charter capital, or exercises control by other means; if nobody qualifies, the senior manager is treated as the beneficial owner (article 3(1)(14)). Banks must identify the beneficial owner, take reasonable steps to verify identity from reliable sources and document their reasoning (article 16(5) and (5.1)). The CBA regulation requires a declaration on the presence or absence of a beneficial owner (point 43). The CBA's Guidance on Determining the Beneficial Owner (22 October 2024) expects, depending on risk, a cross-check against the beneficial ownership database of the State Register of Legal Entities; if it shows inconsistencies, the customer should be given a reasonable time to correct the register, and an uncooperative customer refused or exited (points 41 and 42).

Risk-based tiers

Tier	When	What it requires

Enhanced due diligence	Risk is high if even one high-risk criterion applies (point 23), for example politically exposed persons (PEPs), private banking, complex ownership, non-compliant countries, life insurance beneficiaries, non-face-to-face relationships (Regulation 279-N, point 27); exceptions in points 22.1 and 24(3)	At a minimum senior management approval before the relationship starts, source of funds and wealth, closer scrutiny of purpose (AML law, arts 3(1)(22) and 18(2))
Simplified due diligence	CBA low-risk criteria only, for example salary and pension payments, budget payments, regulated financial institutions (point 28); never with suspicion or a high-risk criterion	Reduced ongoing measures (art. 18(5); points 35 and 36)
Ongoing monitoring	Whole relationship	Reviews at least annually (standard risk), six-monthly (high risk) and every three months for PEPs, unless the bank's documented analysis, submitted to the CBA, justifies other periods (points 37, 41 and 41.1). Identification and verification data refreshed at least annually (art. 17(2)); point 38's update schedule covers other CDD information only
Correspondent banking	Foreign respondent institutions	Respondent assessment, senior management approval, no shell banks (art. 19)

Reporting and records

Report	Trigger for banks	Deadline
Threshold report (cash)	Cash transactions of AMD 5 million or more	Immediately after the transaction via the FMC web service; incoming international transfers by 12:00 the next working day
Threshold report (non-cash)	Non-cash transactions of AMD 20 million or more	

Threshold report (crypto-assets)	Crypto-asset transactions of AMD 1 million or more	
Suspicious transaction report	Any amount, including attempted transactions	Same working day; if impossible, by 12:00 the next working day

Thresholds come from article 6(3)(1) of the AML law; deadlines from CBA Board Decision 75-N of 8 May 2020 on bank reporting (points 11 and 12). Tipping off is prohibited (article 6(5)). A bank may suspend a suspicious transaction for up to 5 days and must do so on the CBA's instruction; the CBA, as authorised body, may suspend it for up to 15 days (article 26). Records, including CDD documents, are kept for at least five years after the relationship ends or the transaction is completed (article 22(2)), and may be kept electronically (Regulation 279-N, point 51).

4 Identity verification and onboarding

Banks identify and verify customers on the basis of reliable and valid documents and other information issued by a competent state authority (article 16(4)). For an individual the bank must record, at a minimum, the name, citizenship, registration address (if any), date and place of birth, and the series, number and issue date of the identity document, and must establish the customer's place of residence.

Timing and reliance

Since 8 August 2025, a bank may verify the identity of the customer, representative and beneficial owner after establishing the relationship, within a reasonable period of no more than seven days, if the risk is managed effectively and this is needed not to disrupt normal business (article 16(1)). It must adopt a policy setting the conditions, such as the type, number or value of transactions, under which the customer can transact before verification (article 18(3.1)); banks had to adopt it and file it with the CBA, the authorised body under the AML law, within two months of 8 August 2025. If verification then cannot be completed, the bank must end the relationship and consider whether to report it as suspicious (article 27(2)).

A bank may rely on CDD by another supervised institution outside non-compliant countries if it gets the data immediately and copies on request; it keeps ultimate responsibility (article 16(8)).

Methods

Neither the AML law nor Regulation 279-N prescribes a verification technology. Document capture, biometric face matching, liveness detection, video calls and electronic signatures are not named, approved or prohibited; the bank chooses its methods in its non-face-to-face risk policy (article 18(3)). Where an ID card is used to log in or sign, its electronic signature certificate is valid for the life of the card (Law on Electronic Document and Electronic Digital Signature, article 14), but only cards issued before 15 February 2023 and new-model cards under the Law on Identity Document (HO-210-N, in force 30 October 2026) have a usable chip. Holders of chipless cards use Mobile ID, a SIM-based credential issued at mobile operators' service centres.

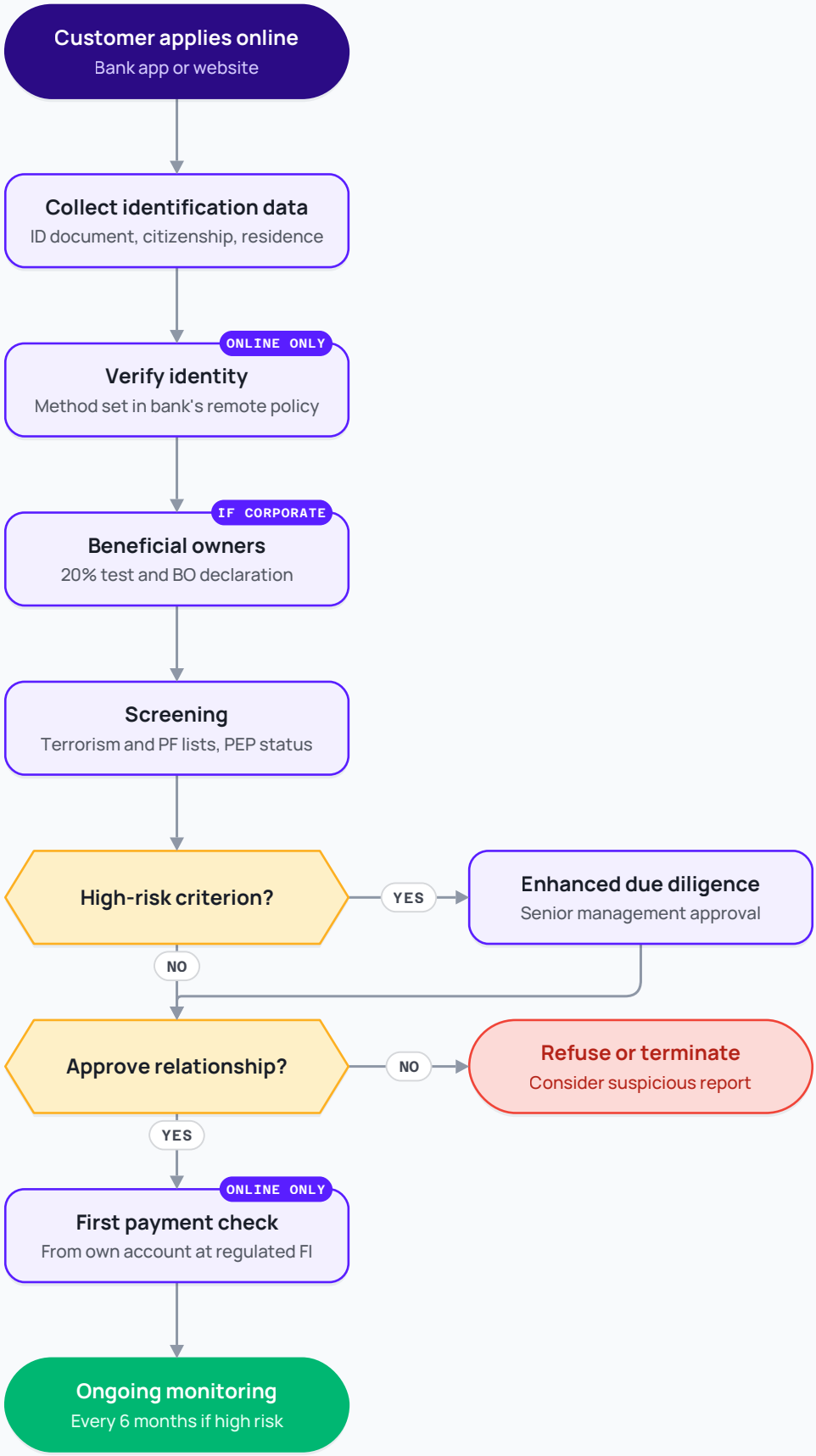


Figure 1. Remote account opening for an individual or company at an Armenian bank.

Banks must screen customers and transactions against the UN Security Council lists and the terrorism and proliferation lists published by the CBA, freeze matches without prior notice and report each freeze as a suspicious transaction (article 28).

5 Digital channels: what's different

Bottom line: remote account opening is allowed and the identification data are the same as in a branch, but a relationship opened without face-to-face contact carries a CBA high-risk criterion, so it triggers enhanced due diligence unless the bank has filed a documented analysis supporting a medium rating, and it always requires a first-payment check that a branch customer does not face.

Requirement	In person / branch	Online / remote	Difference
Permission to onboard	Permitted	Permitted; bank must have a written non-face-to-face risk policy	Differs
Risk classification	Set by other factors	Non-face-to-face is a high-risk criterion; medium after a documented analysis submitted to the CBA; low for listed low-risk payments	Differs
Enhanced due diligence	Only if a high-risk criterion applies	Required, including senior management approval, unless rated medium (point 22.1) or low (point 24(3))	Differs
First payment	No requirement	From an account in the customer's name at a regulated institution	Differs
Identification data	Article 16(4) data set	Same data set	Same
Verification timing	Up to 7 days after onboarding, with limits	Same	Same
Prescribed technology	None	None (no video, eID or biometric standard)	Same

Monitoring frequency	Annual at standard risk	Every six months while rated high risk (every three months for PEPs), unless a documented analysis submitted to the CBA supports other periods	`Differs`
Reporting and record keeping	Thresholds, same-day STR, 5 years	Same; electronic records allowed	`Same`
Payment security	Card monitoring and alerts	Internet card payments also need 3-D Secure or one-time codes	`Differs`

Non-face-to-face 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), redrafted by Decision 11-N, adopted 22 January and in force 30 January 2026). High-risk criteria are set by the CBA's legal acts and the bank's internal acts (AML law, article 3(1)(21)), and enhanced due diligence follows a high rating (article 18(2)). MONEYVAL found that Armenian banks themselves rate remote onboarding among their highest risks.

Rating for a remote customer	When	Source
High (default)	One high-risk criterion is enough; where criteria for different levels coexist, the highest governs	Points 23 and 25
Medium	A comprehensive, documented analysis concludes the risks are effectively managed and contained, and the bank submits it to the CBA as authorised body	Point 22.1
Low	Only budget payments, or salary, pension, social benefit or public service payments up to 1,000 times the minimum wage	Points 24(3) and 28

The CBA's Guideline on the Criteria of High Risk and the Indicators of Suspicious Activity in Relation to Money Laundering and Terrorist Financing (Chairman's Decision 1/711-A of 11 October 2016, amended by Decision 1/347-A of 24 September 2025) explains that the delivery-channel criteria target fully remote processes; a customer first identified face to face does not carry the criterion.

The first-payment rule

When a relationship is established without face-to-face contact, the bank must require the first payment to be made from an account opened in the customer's name at a financial institution that meets the reliance conditions in article 16(8)(3) of the AML law (Regulation 279-N, point 40).

Pending: electronic identification law

A draft Law on Electronic Identification and Trust Services `Proposed, comments close 17 Nov 2026`, published by the Ministry of High-Tech Industry and Artificial Intelligence, would set assurance levels for electronic identification schemes, introduce an Armenian digital identity wallet, regulate trust services and repeal the current electronic signature law.

6 Data protection and biometrics

The Law on Protection of Personal Data («Անձնական տվյալների պաշտպանության մասին», HO-49-N, last amended 7 May 2026) governs identity capture; the AML law provides the basis for CDD data and its five-year retention.

Biometric data, defined as information on a person's physical, physiological and biological characteristics, may be processed only with the data subject's consent, unless a law provides otherwise and the aim can be achieved only by processing that data (article 13). As the AML law does not mandate biometrics, face matching or liveness checks need the customer's consent. Consent must be given in writing or electronically, certified with an electronic digital signature; oral consent counts only through reliable actions that clearly show it (article 9(7)). A tick-box alone may therefore not meet the rule, so remote flows should capture consent in one of these forms. Before processing biometric data, the controller must notify the Personal Data Protection Agency of the Ministry of Justice; this notification is mandatory (article 23(3)).

7 Sector-specific obligations

Wire transfers

The originating bank must include the names and account numbers (or a unique reference) of payer and payee in every transfer, and for transfers above 400 times the minimum wage (AMD 400,000) also the payer's identity document data, address, or date and place of birth

(article 20). A transfer that lacks this information must be refused and considered for reporting (article 27(3)).

Outsourcing and third-party providers

Rule	Source
Outsourcing banking operations, or auxiliary operations that support normal banking activity, needs the CBA's prior consent; a contract without it is void	Law on Banks and Banking, art. 34(5) and (6)
The CBA decides within 30 days; consent is deemed given if it does not refuse or suspend the period in time	CBA Board Decision 118-N of 20 July 2018, points 6 and 7
The bank stays liable for outsourced operations; CBA inspection powers extend to the contractor; the CBA can order the contract changed or ended	Art. 34(9) to (11)
IT infrastructure may be outsourced in whole or part	CBA Decision 173-N, point 94

Card security and tokenised payments

The CBA's card security rules (Board Decision 300-N of 4 November 2014, last amended by Decision 176-N of 30 June 2026) require banks that enable internet card payments to use a security system consistent with international standards, such as 3-D Secure or one-time codes, to prevent unauthorised transactions (point 18), to run real-time transaction monitoring 24/7 (point 19), and to send SMS or email alerts for card transactions when the cardholder opts in (point 21). Where cards issued by Armenian banks are serviced by banks in Armenia, including through token-based digital wallets, clearing and settlement must take place in Armenia (point 29.1).

Resolution

The Law on Bank Resolution (HO-363-N) `Adopted, effective 1 Jan 2027` gives the CBA tools to resolve failing banks, including bridge banks and asset separation, and adds a minimum requirement for total capital and subordinated liabilities available for resolution to the Law on Banks and Banking (Law HO-366-N).

8 Risk indicators and red flags

INDICATORS FROM THE CBA GUIDELINE RELEVANT TO DIGITAL BANKING

- **Doubtful identity data**: data whose authenticity needs extra inquiry, or copies offered with excuses for missing originals.
- **Altered documents**: identity documents showing signs of alteration or falsification, or different documents presented on different occasions.
- **Shared devices**: several customers accessing online banking from the same electronic system, or with identical contact details.
- **Structuring**: fragmented transactions kept below reporting or CDD thresholds, or amounts reduced to avoid CDD.
- **Dormant reactivation**: accounts or payment instruments unexpectedly reactivated after long inactivity.
- **Risky IP locations**: online transactions with parties whose IP address is in a non-compliant country.
- **Gambling flows**: large numbers or amounts of transactions through accounts of internet betting companies.
- **Crypto-asset obfuscation**: funds presented as crypto-asset conversion proceeds, or use of mixers, tumblers and cross-chain bridges.

MONEYVAL identified fraud, corruption, tax crimes, drug trafficking and cybercrime among Armenia's main money laundering threats.

9 Enforcement and penalties

AML breaches by banks are sanctioned under the Law on Banks and Banking (AML law, article 30(2)). For each breach the CBA may impose, alone or together, a warning with an order to remedy, a fine, withdrawal of managers' qualification certificates, or revocation of the licence (article 61). Fines are set per violation (article 63(3)):

- up to 5% of the CBA's minimum charter capital for each breach of a prudential standard or late reporting to the CBA;
- up to 1% of the minimum charter capital, currently AMD 10 million, for each other breach of banking legislation.

A fine must not push the bank into serious financial difficulty, and if the bank contests it, the CBA collects it through the courts (article 63(1) and (4)). MONEYVAL notes that the CBA's sanctioning methodology has no quantitative fine formula and that published sanction information is brief.

Action	Detail	Source
AML sanctions on banks, 2020 to Q3 2025	38 warnings, 35 fines totalling about EUR 1.49 million, one removal of an AML compliance officer; about a third of the fines imposed in Q3 2025	MONEYVAL 2026 report, Table 3.6 and para. 215
VTB-Armenia Bank, 5 January 2022	Warning with remedial orders for breaches of banking and AML legislation	CBA Chairman's Decision 1/01BG-A
Inecobank, 21 October 2025	AMD 10 million fine: domestic tokenised Visa and Mastercard transactions not cleared in Armenia	CBA statement of 24 October 2025

10 Recent changes and what to watch

- **17 November 2026:** `Proposed, comments close 17 Nov 2026` Public consultation ends on the draft Law on Electronic Identification and Trust Services, which would introduce eID assurance levels and an Armenian digital identity wallet.
- **1 January 2027:** `Adopted, effective 1 Jan 2027` The Law on Bank Resolution and related amendments to the Law on Banks and Banking and the deposit guarantee law take effect, adding a loss-absorbing liabilities standard and a new creditor ranking.
- **21 August 2026:** `In force` CBA rules on managing the risk of circumventing international sanctions (Decision 25-N, published 20 February 2026) apply to money transfer and e-money institutions, not to banks.
- **17 July 2026:** `In force` CBA Decision 176-N of 30 June 2026 amended the card security rules, adding issuer limits for stand-in authorisation and updating alert and incident duties.
- **9 July 2026:** `Published` MONEYVAL published Armenia's sixth-round report, adopted at its 71st Plenary (26 to 29 May 2026), and placed Armenia in enhanced follow-up, calling for better suspicious activity reporting and beneficial ownership accuracy.
- **18 May 2026:** `In force` Amendments to the Law on Banks and Banking (HO-150-N) move statutory publications online.

- **30 January 2026:** `In force` CBA Decision 11-N of 22 January 2026 redrafted the high-risk and low-risk criteria in Regulation 279-N, keeping non-face-to-face relationships as high risk.
- **24 September 2025:** `In force` The CBA amended its guideline on high-risk criteria and suspicious activity indicators; the current version includes online banking and crypto-asset indicators.
- **8 August 2025:** `In force` AML law reform (HO-261-N): seven-day delayed verification with a pre-verification policy, PEP checks extended to life insurance beneficiaries, and a rewritten targeted financial sanctions freezing regime.

11 What this means for identity verification

- **Documents.** Capture every article 16(4) data element, including place of birth, document issue date and place of residence.
- **Remote methods.** No approved list exists; the bank's non-face-to-face policy is what supervisors will test.
- **Risk engine.** Fully remote customers default to high risk, with senior management approval in the flow and six-monthly reviews (three-monthly for PEPs), unless a documented analysis filed with the CBA supports a medium rating or only listed low-risk payments are involved.
- **Payments.** Match the first incoming payment to an account in the customer's name at a regulated institution.
- **Biometrics.** Capture consent in a form article 9(7) accepts before face matching or liveness, and file the mandatory notification with the Agency first.
- **Re-verification.** Refresh identification and verification data at least once a year (art. 17(2)), separately from the point 38 schedule for other CDD data; keep evidence for five 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 KYC onboarding with ID document capture and verification, face match and biometric liveness, configured to your non-face-to-face risk policy.
- KYB and beneficial owner verification for corporate customers against the 20% ownership test.
- AML screening against terrorism and proliferation lists, PEP lists and adverse media at onboarding and on an ongoing basis.
- Configurable risk-based workflows in a no-code builder, including enhanced due diligence steps and KYC questionnaires, 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), official incorporation in force since 8 August 2025, articles 3, 6 to 9, 15 to 20, 22, 26 to 28 and 30, ARLIS, arlis.am
- **Law HO-261-N of 3 July 2025 amending the AML law** (published 29 July 2025), transitional provisions, ARLIS, arlis.am
- **Law on Banks and Banking** («Բանկերի և բանկային գործունեության մասին», HO-68, 30 June 1996), incorporation in force since 18 May 2026, articles 6, 9, 18, 23 to 29, 34 and 60 to 63, ARLIS, arlis.am

- **Law HO-366-N of 3 July 2026 amending the Law on Banks and Banking** (effective 1 January 2027), ARLIS, arlis.am
- **Law HO-150-N of 16 April 2026 amending the Law on Banks and Banking**, ARLIS, arlis.am
- **Law on Bank Resolution** («Բանկերի վերակառուցման մասին», HO-363-N, 3 July 2026, effective 1 January 2027), ARLIS, arlis.am
- **Law on Guaranteeing Compensation of Bank Deposits of Natural Persons** (HO-142-N, 24 November 2004), incorporation in force since 1 July 2022, articles 3 and 13, ARLIS, arlis.am
- **Law on Minimum Monthly Wage** («Նվազագույն ամսական աշխատավարձի մասին», HO-66-N), article 3, ARLIS, arlis.am
- **Law on Protection of Personal Data** («Անձնական տվյալների պաշտպանության մասին», HO-49-N, 18 May 2015), articles 9(7), 13, 23(3) and 24(2), ARLIS; official English title from the ARLIS translation (acts/117034), arlis.am
- **Law on Electronic Document and Electronic Digital Signature** (HO-40-N, 14 December 2004), article 14, ARLIS, arlis.am
- **CBA Board Decision 279-N of 7 October 2014, Regulation on Minimum Requirements to Reporting Entities in the Field of Preventing Money Laundering and Terrorism Financing**, as amended by Decision 11-N of 22 January 2026 (in force 30 January 2026), points 22.1, 23 to 28, 35 to 38, 40, 41, 41.1, 43 and 51, ARLIS, arlis.am
- **CBA Board Decision 75-N of 8 May 2020 on the form and procedure of banks' threshold and suspicious transaction reports**, points 11 and 12, ARLIS, arlis.am
- **CBA Board Decision 39-N of 9 February 2007, Regulation 2 on the regulation of banks and prudential standards**, points 15 to 17, ARLIS, arlis.am
- **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, sections 1.3.2 and 2, cba.am
- **Financial Monitoring Center, About FMC**, Central Bank of Armenia, cba.am
- **CBA statement on the measure applied to Inecobank** (24 October 2025; decision of 21 October 2025), cba.am
- **CBA summary of Chairman's Decision 1/01BG-A of 5 January 2022 on VTB-Armenia Bank**, cba.am
- **Law HO-368-N of 3 July 2026 amending the Law on Guaranteeing Compensation of Bank Deposits of Natural Persons** (effective 1 January 2027), ARLIS, arlis.am
- **CBA Board Decision 118-N of 20 July 2018 on prior consent to outsourcing by banks**, points 6 and 7, ARLIS, arlis.am
- **CBA Board Decision 173-N of 9 July 2013 on minimum requirements for information security**, point 94, ARLIS, arlis.am
- **CBA Board Decision 300-N of 4 November 2014 on card security rules**, as amended by Decision 176-N of 30 June 2026, points 18 to 21 and 29.1, ARLIS, arlis.am

- **CBA Board Decision 25-N of 30 January 2026 on managing the risk of circumventing international sanctions by payment and settlement organisations** (published 20 February 2026, in force 21 August 2026), ARLIS, arlis.am
- **CBA Guidance on Determining the Beneficial Owner**, 22 October 2024, points 39 to 42, cba.am
- **Government Decision 734-N of 2 July 2015 establishing the Personal Data Protection Agency of the Ministry of Justice**, ARLIS, arlis.am; Agency page, Ministry of Justice, moj.am
- **Law on Identity Document** («Անձը հաստատող փաստաթղթի մասին», HO-210-N, 11 May 2026, in force 30 October 2026), article 11, ARLIS, arlis.am; **Government Decision 1581-N of 29 October 2026** on the passport and identification card (annex, ID card chip functions), ARLIS, arlis.am
- **What is the "YesEm" Identification Platform and How to Log in?**, National Services Gateway, english.hartak.am
- **Draft Law on Electronic Identification and Trust Services and related drafts**, Ministry of High-Tech Industry and Artificial Intelligence, public consultation 2 to 17 November 2026, e-draft.am, e-draft.am
- **MONEYVAL, Anti-money laundering and counter-terrorist financing measures: Armenia, Sixth Round Mutual Evaluation Report**, MONEYVAL(2026)8, adopted at the 71st Plenary (26 to 29 May 2026), published 9 July 2026, paras 128, 169, 175, 214 to 218, Table 3.6 and Technical Compliance Annex, criterion 15.9, rm.coe.int; executive summary, rm.coe.int; "Outcome of MONEYVAL 71st Plenary Meeting", coe.int
- **MONEYVAL, "Armenia: Council of Europe's MONEYVAL highlights robust targeted financial sanctions regime, calls for improvements in money-laundering prosecutions and asset recovery"**, 9 July 2026, coe.int