

KYC/AML Procedure – Consumer Lending

Document owner: Head of Retail Operations

Version: 1.3

Date: 12/10/2026

Bank: Demo Bank d.d. (fictional Slovenian bank)

Scope: Customer due diligence (CDD) for natural persons applying for unsecured consumer loans in branches and online

Related documents: KYC/AML Policy (KB-INT-0003); Records Retention Policy (KB-INT-0008); Consumer Loan Approval Process

1. Purpose

This procedure sets out the steps that branch and online staff follow to know the customer before a consumer loan is granted, so that the bank meets its obligations under the Slovenian Act on the Prevention of Money Laundering and Terrorist Financing (ZPPDFT-2) and the bank's KYC/AML Policy.

2. Roles

Role	Responsibility
Relationship manager (RM)	Performs identification in the branch, collects CDD information, assigns the initial risk rating.
Digital Onboarding team	Operates the online application journey and reviews online identification exceptions.
AML Compliance	Maintains the risk-rating methodology, reviews unusual activity, files reports to the Office for Money Laundering Prevention.
Operations	Archives CDD records and deletes them at the end of the retention period.

3. When CDD is performed

CDD is performed when the customer enters into a business relationship with the bank, i.e. for every loan application. CDD must be completed before the credit decision and before the contract is signed. If CDD cannot be completed, the application is rejected and no business relationship is established.

4. Identification and verification – branch channel

- The RM identifies the customer in person on the basis of a valid official photo identity document (identity card or passport) presented in original.
- The RM checks that the document is valid, that the photo matches the customer and that the document shows no signs of tampering.
- The RM records name, address, date and place of birth, tax number, document type, number, issuer and validity in the core system and stores a copy of the document.
- The customer signs a statement confirming that he or she acts on his or her own behalf and is the beneficial owner of the loan.

5. Identification and verification – online channel

To keep the online journey short, the following simplified steps apply:

- The customer uploads a photo or scan of the front and back of the identity card and a selfie.
- The system reads the document data automatically (OCR) and pre-fills the application.
- The Digital Onboarding team checks only cases where the OCR confidence score is below 80%. Other cases are accepted automatically.
- Video identification or a qualified electronic identity is not used, because it lowers the conversion rate.

- The online application does not include the statement on acting on own behalf (beneficial ownership); this question is asked only in the branch.
- Customers onboarded online are monitored in the same way as all other customers.

6. Purpose and intended nature of the business relationship

For every loan, the RM or the online form records the purpose of the loan (e.g. car, home furnishing, education, refinancing), the expected source of repayment (salary, pension, other income) and the expected pattern of repayments. Unusual purposes or a mismatch between declared income and requested amount are referred to AML Compliance.

7. Customer risk rating

Every customer receives a risk rating of low, medium or high in the core system. The rating takes into account the customer's occupation, the channel, the loan amount and the product. Customers rated high risk are referred to AML Compliance, which decides whether to proceed.

Customers resident in, or with nationality of, a country on the EU list of high-risk third countries are treated under standard CDD, because consumer loans are low-value domestic products and the loan is repaid from a Slovenian account. No additional measures are applied for these customers.

8. Politically exposed persons (PEPs)

PEP status is not checked in the consumer lending process. PEP checks are performed by the Payments department when a customer opens a current account. Lending staff may rely on that check even if it was performed several years ago or if the customer has no current account with the bank.

9. Sanctions screening

Sanctions screening is not part of loan onboarding. Instead, the full customer base is screened against the EU consolidated sanctions list in a monthly batch run performed by IT. Potential matches from the batch run are sent to AML Compliance.

10. Ongoing monitoring

Loan accounts are monitored throughout the business relationship. The transaction monitoring system generates alerts for unusual repayment patterns (for example large early repayments from third-party accounts or cash). Alerts are reviewed by AML Compliance. Customer data are updated at least every 3 years for low-risk, every 2 years for medium-risk and every year for high-risk customers, and whenever the bank becomes aware of a change.

11. Suspicious transactions

Staff who suspect money laundering or terrorist financing report immediately to AML Compliance using the internal form. Staff must not inform the customer about the report (no tipping-off). AML Compliance decides on reporting to the Office for Money Laundering Prevention.

12. Record keeping

Copies of identity documents and all CDD information are kept for 5 years after the loan is disbursed and are then deleted by Operations.

13. Training

All RMs and Digital Onboarding staff complete AML training on joining and annually afterwards. Completion is tracked by HR.

14. Version history

Version	Date	Change
1.0	02/02/2023	First version
1.2	14/05/2025	Online channel added
1.3	12/10/2026	Simplified online identification to improve conversion