

UniCredit Bank Czech Republic and Slovakia a. s.,
pobočka zahraničnej banky

AML Program

LOCAL AML PROGRAM:

- adoption of a risk-based approach;
- customer due diligence measures;
- screening of clients and pre-execution screening of payments;
- post-execution monitoring of transactions;
- procedures for internal reporting and investigation of potentially suspicious transactions and, where necessary, the external reporting of suspicious transactions to relevant Authorities;
- record keeping;
- training of Employees;
- tracking of new legal and regulatory AML requirements;
- management information and reporting;
- procedures for monitoring the effectiveness of the above controls; and
- prevention of terrorism financing.

RISK - BASED APPROACH

The risk assessment covers the money laundering risk presented by customers, products and services.

The following factors are used in determining a methodology for risk-classifying customers:

- country risk — including both the customer's nationality, residence, country of operation and country of incorporation and the nationality and/or residence of the beneficial owner(s);
- industry risk – the customer's occupation or the industry in which they are engaged;
- product and services risk – the type of the Group products or services being used by the customer and how those products or services are delivered (e.g. non-face-to-face);
- entity risk – the legal form taken by the customer and its susceptibility to being used for money laundering; and
- PEP and reputation risk – whether the customer or beneficial owner is a Politically Exposed Person (PEP) or where there is negative information concerning the customer that may affect Group's reputation.

CUSTOMER DUE DILIGENCE MEASURES

Program designed to establish:

- that the customer exists;
 - the customer's nationality and usual country of operation;
 - the customer's occupation/business; and
 - the customer's entity type.
- who beneficially owns and controls the customer;

- the customer's (and where applicable, owner's/controller's) general reputation (by screening names against tools provided by reputable commercial organizations such as Dow Jones or WorldCheck);
- what products and services the customer will require; and
- the expected nature and level of activity on the account.

Initial identification and verification:

- before the start-up of a business relationship that, at the time of its establishment, is assumed will have a reasonably long duration; or
- before performing occasional transactions for amounts equal to or exceeding Euro 10,000 or equivalent that entail the transmission or movement of means of payment, regardless of whether they are made in a single transaction or in several transactions that appear to be linked.

Enhanced due-diligence:

- where the client is classified as high risk (or a higher risk classification);
- where the client is a PEP;
- where a PEP is a relevant beneficial owner of a client; and
- for correspondent banking relationships with banks outside the EU or equivalent jurisdictions.

Prohibited business relationships

- establish business relationships with shell banks nor establish or permit transactions on anonymous accounts;
- establish or maintain business relationships where the identity of the customer, or where appropriate its beneficial owner(s), needs to be established in accordance with this Rule and associated procedures but where such identity cannot be established;
- establish relationships with or process transactions connected to individuals or entities named on the EU Financial Sanctions List. Furthermore, a Company shall not establish relationships with or process transactions connected to individuals or entities named on the United States Office of Foreign Assets Control (OFAC) Specially Designated Nationals and Blocked Persons List ('SDN list') unless approval is given by the relevant Local Head of AML. The escalation process described in this Rule may also be relevant. No USD transactions shall be permitted with entities named on the OFAC SDN list;
- establish relationships with unregulated money remittance businesses;
- establish relationships with unregulated providers of digital/virtual currencies;
- establish relationships with individuals or entities where it is known that they are actively involved in criminal, corrupt or terrorist activities.

Ongoing due diligence

- for high risk clients or those with a higher risk classification – every year;
- for medium risk clients – every two years; and
- for low risk clients – every three years.

SCREENING OF CLIENTS AND PAYMENTS**All customers and, where relevant, the directors, beneficial owners and other connected persons are screened against a database that contains:**

- the European Union Financial Sanctions List;
- the OFAC SDN List;
- any applicable locally-issued sanctions lists; and
- a list of PEPs provided by a reputable commercial organization such as Dow Jones or WorldCheck.

All incoming and outgoing payments are screened against a sanctions screening tool which incorporates the EU, OFAC and local sanctions lists.

TRANSACTION MONITORING

- Risk-based framework implemented, that allows for the post-execution monitoring of transactions to identify for further investigation those which may be suspicious. Monitoring is automated.

REPORTING AND INVESTIGATION OF SUSPICIOUS ACTIVITY

- the prompt internal reporting of potentially suspicious activity to the Local Head of AML;
- the assessment and investigation of potentially suspicious activity and the documentation of the results of the investigation;
- the prompt reporting to external Authorities when the Company knows, suspects or has reasonable grounds to suspect that money laundering is being or has been committed or attempted; and
- the prompt response to enquiries from external authorities.

RECORD KEEPING

Procedures ensure the retention of the following, for at least ten years from the execution of an occasional transaction or the termination of the business relationship:

- a copy of or references to the documents used for customer due diligence; and
- the supporting evidence and records pertaining to the business relationship and the transactions, consisting of the original documents or copies admissible in court proceedings under the applicable national legislation.

TRAINING

- all employees trained at least once in a 12 months;
- tailor-made class trainings for specific departments

REGULATORY TRACKING

Procedures implemented to ensure:

- changes to relevant AML laws, regulations and guidance are identified and analyzed for their impact upon the Local AML rules; and
- AML rules and controls are modified to deal with any material impact of those changes.

MANAGEMENT INFORMATION AND REPORTING

Local Heads of AML ensures that they have appropriate internal management information sufficient to allow them to assess and monitor the effectiveness of controls and that regular reports about the AML program are made to the bank's governing bodies.

MONITORING OF CONTROLS

Program for testing of first-level AML controls is sufficient to give reasonable assurance that the controls are working effectively.

FINANCIAL SANCTIONS & PREVENTION OF TERRORIST FINANCING

Procedures implemented that require:

- the restraining of the assets, economic activities and financial resources of persons and entities included in the EU and OFAC blacklists, where legally permissible or required;
- the reporting to the competent Authorities of the restraining measures or the existing relationships with customers not subject to restraining measures but included in the blacklists published by these Authorities;
- the reporting to relevant Authorities of any activity known or suspected (or where there are reasonable grounds to know or suspect) to be connected to terrorist financing; and
- a prohibition against the undertaking of specific commercial activities, as set out by the EU, with countries that threaten international peace and security.