Anti-Money Laundering and Counter Terrorist Financing Policy

2019

Credit EuropeBank

Table of Contents

Purpose of the Policy

Money Laundering can be defined as concealment of the true nature or origin of funds derived from illegal activities. Predicate offences* for money laundering are defined by local legislation in specific jurisdictions, but most commonly those include fraud, drugs smuggling, corruption, bribery, organized crime, terrorism, tax crime and many other types of crime.

In everyday business a financial institution faces the risk that through providing services to its customers, for instance through processing a payment, or accepting a deposit or granting a loan, it performs an act that apparently gives a legitimate 'face' to an otherwise unlawful money flow. Money launderers seek to ensure flows of unlawful funds by disguising them as legitimate financial transactions. As a result, almost every transaction may appear 'clean' on the face of it.

Terrorist financing can be defined as providing financial support to terrorist organisations, whose aim is to intimidate a population or to compel a government or an international organization to do or abstain from doing any act. Unlike in case of money laundering, terrorist financing may use funds that have a legitimate source. Terrorists move money or transfer value through the use of the financial system, physically, or through international trade system.

There is still a resemblance between money laundering and terrorist financing: in both situations, there is a need to conceal the connection between the criminal organisation and the source of funds. Therefore, both use similar methods to move money or transfer value through the financial system.

The harm caused by money laundering to the financial sector, economy and the society on the whole is enormous: it incites crime, undermines fair competition, diminishes tax revenue, diminishes economic growth and weakens morale. Terrorist financing leads to the loss of lives and endangers peace.

Therefore, in an absolute majority of jurisdictions money laundering and terrorist financing are criminal offences. Financial institutions all over the world are legally obliged to counter money laundering and terrorist financing – not only through spotting and reporting the (attempted) acts of misusing and abusing financials services for the sake of money laundering and financing of terrorism, but also through having systems in place which prevent money laundering and terrorist financing from taking place.

To assist the banking industry in this task various international organizations have published standards (i) providing a set of counter-measures against money laundering and terrorist financing covering the criminal justice system and law enforcement, the financial system and its regulation, and international co-operation, and (ii) to detect, prevent and suppress terrorist financing.

The purpose of this policy is to establish a general framework for CEB to counter the risk of involvement in money laundering and terrorist financing. The basic principle for CEB is to be vigilant in both assessing the suitability of its (prospect) customers and handling the customers' transactions.

Adherence to this policy is absolutely fundamental for ensuring that all offices of CEB, regardless of geographic location, fully comply with applicable AML/CTF legislation. In this respect, CEB also endorses:

- the FATF standards on money laundering and terrorist financing,
- publications by the Basel Committee on customer due diligence, and
- the AML principles of the Wolfsberg Group,

---

* Actions that provides the underlying resources for another criminal act

as setting solely or jointly the benchmark for best industry practices in banking.

Some terms as used within this policy are defined (see "Definitions").

Applicability

In response to the international community's growing concern about the problem of money laundering and terrorist financing, many countries around the world are continuously enacting or strengthening their laws and regulations regarding this subject.

CEB must ensure that the statutory duties resulting from the different applicable laws and regulations on money laundering and terrorist financing are fulfilled by its branch offices and subsidiaries. In any country/jurisdiction where the requirements of applicable AML laws and regulations establish a higher standard than described in this document, the respective office of CEB must meet those standards.

All offices of CEB have detailed AML procedures and subordinated AML/CTF Programmes, which implement the provisions of this AML/CTF Policy, CEB's KYC policy and the norms of the local AML legislation.

Local AML procedures meet (i) the applicable AML laws and regulations of the relevant jurisdiction and (ii) the provisions set out in this policy whereas local KYC procedure meet (i) the respective local regulatory requirements, as well as (ii) the provisions set out in CEB's KYC policy.

If any applicable laws and regulations are in conflict with this policy, the relevant office of CEB must consult with local Compliance or the Country AML Officer where applicable, to resolve the conflict.
Compliance with the CEB's AML/CTF requirements and cooperation in detecting attempts of ML/TF is the responsibility of each and every staff member. Therefore, all staff members must be aware of:

- ML/TF risks relevant to CEB and the ways these risks may be revealed in the customer's features, business structures and individual transactions – known as ML/TF risk indicators or "red flags".
- The obligation to file internal reporting to the designated service within CEB (usually Compliance) in all instances where there are grounds to suspect that customers, business structures used by the customers and individual transactions pose ML/TF risk or if customers demonstrate unusual behaviour, particularly the behaviour which is questionable from the point of view of economic rationally.
- The obligation to keep information about internal investigations or reports (to be) submitted to the regulatory bodies/local financial intelligence units confidential. Specifically, this information may not be shared with the customer whose behaviour/transactions are subject to an internal investigation.

Three Lines of Defense

CEB applies the three lines of defense model to manage risks, including ML/TF risks. The ownership and operational accountability for CEB's AML/CTF program primarily rests with the business lines (i.e. first line of defense). The second line of defense is formed by the risk management functions – including the compliance function that supports the business lines with the implementation and maintenance of the entire AML/CTF program and the monitoring thereof. The audit function is the third line of defense, which independently assesses the overall effectiveness of CEB's risk management activities, including CEB's AML/CTF program.

Each of the three lines play a distinct role within CEB's wider governance framework.

Detailed Policy

Sound AML/CTF standards constitute a key component of CEB's efforts to prevent CEB from being misused for money laundering, terrorist financing or other fraudulent transactions.

CEB establishes and maintains relationships exclusively with those customers whose source of and funds and wealth, as well as the purpose and nature of business activities undertaken with CEB, are well understood and can be reasonably established as legitimate.

To ensure the above, CEB exercises customer due diligence ("CDD") with regard to each prospective customer before entering into business relations with it and continuously monitors the legitimacy of customer's business while providing banking services.

The CEB CDD standards are determined in the KYC Policy and further explained in the local KYC Procedures. The following standards are to be understood as minimum requirements for CEB based on either legal and regulatory requirements or directive guidelines and best practices.

Risk identification

The continuing threat of money laundering through financial institutions is most effectively managed by understanding and addressing the potential money laundering risks associated with customers and transactions.

In measuring a potential money laundering risk it is recommended to consider and assess its following components: country risk, customer risk and services risk.

To minimize the money laundering risk CEB needs to make sure that it carries out appropriate CDD when entering into a business relationship with a customer, and monitoring of transactions throughout the course of the relationship.
Local AML and KYC procedures shall provide guidance on the way of identification of the customer's money laundering risk, including the proportional weight of each risk on the risk components in the overall risk assessment and on the way of measuring thereof.

Risks posed by some customers may only become evident once the customer has commenced transacting through the account, making monitoring of customer transactions a fundamental component of the local AML procedures.

Country risk

Country risk, in conjunction with other risk factors, provides useful information as to potential money laundering and terrorist financing risks. There is no universally agreed definition by either governments or institutions that prescribes whether a particular country represents a higher risk.

Factors that may result in a determination that a country poses a higher risk include:

- Countries identified by the FATF as:
    - non-cooperative in the fight against money laundering;
    - lacking appropriate money laundering laws and regulations;
    - providing funding or support for terrorist activities;
    - having significant levels of corruption, or other criminal activity;
    - lacking financial and fiscal transparency.

Countries subject to sanctions, embargoes or similar measures issued by, for example, United Nations, European Union.

Customer Risk

Determining the potential money laundering risks posed by a customer will provide significant input into the overall money laundering/terrorist financing risk assessment. CEB needs to assess, based on its own criteria, whether a particular customer poses a higher risk of money laundering/terrorist financing and whether mitigating factors may lead to a determination that customers engaged in such activities do not pose a higher risk of money laundering. Application of the different risk variables plays an important part in this determination.

There is no universal consensus as to which customers pose a higher risk, but the below listed, non-exhaustive, characteristics of customers are recommended to be viewed as associated with potentially higher money laundering risks:

- Customers which are established in offshore, obscure or apparently unconnected jurisdictions (in which respect attention shall be paid to the FATF's 'black-list' of jurisdictions with strategic deficiencies in AML/CTF measures, and other similar databases or freeze-lists carrying similar precautionary advice issued by competent authorities).

- Customers in high risk businesses (e.g. cash-intensive businesses, some types of investment and wealth management, professional services specialising in accounting and legal support, etc).

- The use or involvement of intermediaries within the relationship. However, the involvement of an intermediary that is subjected to adequate AML regulation and is supervised for compliance with such regulation or otherwise employs adequate AML procedures generally poses reduced money laundering risks.

- Customers that are Politically Exposed Persons and customers in whose ownership and control structures Politically Exposed Persons are present.

- Customers with complex and non-transparent ownership structure.

- Charity institutions and other non-profit entities that are not subject to any type of supervision.

Services Risk

Determining the potential money laundering risks presented by services offered to a customer by CEB may also assist in the overall risk assessment. Services that pose a higher risk of money laundering should be included in a determination of the overall money laundering risks posed. Determining the money laundering risks from the services should include a consideration of such factors as services identified by regulators, governmental authorities or other credible sources as being potentially high risk for money laundering including, for example:

- International Correspondent Banking services.
- Services involving the trade and delivery of precious metals.
- Financing international trade whenever trade contains unusual and high risk features.
- Non-standard business i.e. a service or product which the customer specifically describes to CEB as wishing to receive; and in all cases, banking business of a nature which CEB has not provided in the past.

For the avoidance of doubt, services intended to render the customer deliberately anonymous to CEB, to avoid identification and detection, may not be offered and thus are not offered.

Establishment of customer identity

CEB should neither carry out, nor solicit business with customers which pose an unacceptable integrity risk and therefore put or can potentially put CEB's reputation at stake.
Before starting the business relations, CEB exercises CDD on each prospective customer. No relationships can be launched before the CDD is completed with satisfactory results that confirm the customer's legitimacy and good repute. In the course of the relationships, CEB continuously monitors the customer, as well as the customer's business, in order to ensure its legitimacy and good repute.

In the process of customer acceptance, CEB establishes and verifies the prospective customer's identity.

Prudent identification and verification is achieved through the use of official information from independent sources.

- For corporations: through reliance on official incorporation documentation (e.g. commercial registry extract, certificates of incorporation, good-standing and incumbency, articles and/or memorandum of association).
- For natural persons: by reliance upon valid official identity documentation (i.e. valid passports or valid identity cards).
- For trusts: by reliance upon satisfactory evidence of the creation, establishment and valid existence of the trust (e.g. trust deed, licence).

As a mandatory part of the CDD process, CEB performs screening of the parties involved against internal and external restricted and black lists. This screening can be performed with the use of external intelligence data bases, as well as with the help of internal applications.

The CDD process includes amongst other a review of public information on a customer, with a view to avoid getting into/continuing relations with the customer whose reputation is blemished.

Identification of ultimate beneficiary owner(s)

Whenever CEB is required to establish the identity of a corporate customer or a financial institution to which it provides services, the ultimate beneficial owner(s) must also be properly identified and if applicable verified, as the ultimate beneficial owner(s) are frequently defining the purpose of the business enterprise. Besides that ultimate beneficiary owners, may use corporate vehicles to conceal criminal financial behaviour of their own.

Identification of the beneficial owner(s) consists of determination through proper documentation of the ultimate beneficial shareholding in corporate customers or financial institutions (e.g. share certificates, certificates of incumbency).

Establishment of the source of funds, purpose and nature of relationship

CEB strives to have a clear picture of the customer's (business) activities in orders to identify the plausibility and legitimacy of the source of funds which are used in the relationships or are involved in transactions.

CEB has understanding of the purpose and nature of relationships with its customers and will not accept customers whose source of funds cannot be reasonably established to be legitimate. The customer's business activities must be in agreement with the products/services provided to the customer by CEB.

Monitoring

CEB ensures that ongoing account and transaction monitoring is conducted to detect unusual or suspicious activities.

CEB applies a risk-based approach to the monitoring activities. The specific money laundering and terrorist financing risks are defined on the basis of systematic risk assessment undertaken by CEB and are derived from assessment of ML/TF risks posed by specific groups of customers and different types pf products.

CEB monitors its customers and their financial/transactional behaviour in order to recognise non-standard customer features and activities – for instance, overly complex ownership structures, uncommonly large or frequent transactions, which, if not explained from the point of view of economic rationality, may be raising suspicion about their legitimacy.

Monitoring of customers

Customer monitoring includes the monitoring of changes in the customer ownership and governance structure, as well as changes to its business and/or occupation, CEB products and services it uses, and assessing these changes from the point of view of the reputational risk they can pose to CEB.

Periodic reviews over the customer transactions and KYC are part of the customers' monitoring undertaken by CEB. The periodic reviews are made with certain periodicity depending on the risk assigned to the customer, in line with local KYC procedures.

Monitoring of transactions

Monitoring of a customer's activity is the process that starts from the time of customer acceptance and continues until termination of the business relationship.

CEB applies different methods and techniques of transaction monitoring, adapted for the customers' profile and risk.

The specific modes and methods of transaction monitoring are defined by every CEB office and detailed in their AML/CTF Procedures and programmes. While the post-transaction monitoring is mandatory, it can be complemented by pre-transaction monitoring with regard to higher risk customers/transactions. Depending on business volumes and customer/transaction types, the monitoring can be exercised in automated and manual fashion.

All the relevant stakeholders in transaction monitoring activity have their roles and responsibilities explicitly described in the relevant procedures.
They have to be aware and recognise the indicators of unusual or suspicious activities ("red flags") associated with the transactions' types in their specific business line. The most common red flags for ML/TF include:

- account transactions or other activities which are not consistent with the profile of the customer or its group members;
- transactions over a certain amount, inconsistent with the customer's turnover;
- breaking up amounts before transfer or receipt without a logical explanation or clear business purpose (e.g. ' smurfing');
- transfer of company funds to private accounts or vice-versa;
- offering or acceptance of irregular transaction conditions.

An extensive list of the red flags should be part of the relevant procedures.

An unusual or a suspicious activity is a processed transaction or (prospect) transaction presented for processing which presents at least one red flag for ML/TF and cannot be explained the economic rationale of the transaction in any logical way (whether objectively or by the customer).

Reporting of unusual or suspicious transactions

Applicable laws and regulations of respective jurisdictions require CEB to report unusual or suspicious transactions to the local FIU.

To help institutions in determining whether a transaction is unusual or suspicious the competent authorities have listed a number of 'objective' indicators whereby criteria are defined under which a reporting is mandatory. In addition, it may also refer to some 'subjective' indicators, whereby CEB is obliged to do some further investigation if it feels that it is or can be relevant.

If, after thorough investigation, CEB comes to the conclusion that the transaction is still unusual or suspicious, an external reporting to the local FIU will be made, under the provisions of the local applicable law.

Record keeping

Records must be kept of:

- all transaction data,
- data obtained for the purpose of identification,
- all documents related to money laundering and terrorist financing.

The local relevant procedures must stipulate the specific record keeping requirements according to the relevant laws and regulations of the respective jurisdiction.

However, the record keeping has to be done in such a manner that:

- ✓ the competent authorities are able to assess the Bank's compliance with relevant legislation;
- ✓ any customer or third party acting on behalf of the customer can be identified;
- ✓ all the reports filed with FIU-NL, together with the related documents and information on the transactions, can be easily retrieved and identified; and
- ✓ the Bank can satisfy, within an appropriate time, any regulatory enquiry or court order to disclose information.

Responding to requests for information

CEB may receive requests from competent authorities for personal data from customers to use on behalf of their investigative tasks. Amongst others the inquiries can be received from the National Police, Public Prosecution Services, Tax Authorities, National FIUs and special investigative services. If there are no grounds for providing the requested information, CEB takes all appropriate measures to comply with the national laws on a timely and complete basis.

When receiving such an inquiry CEB will also conduct its own investigation towards customers involved in the inquiry. Investigations initiated as a result of inquiries are clearly documented and designed to ensure that all aspects of the findings are addressed within the set time-frame (if any) provided by the issuing body. CEB ensures that all staff is aware of their legal obligation of secrecy and the prohibition to share information regarding the investigation with its customers.

Training

All staff with direct customer contact, staff who are authorized to execute cash and non-cash financial transactions, and staff in essential support functions for the processing of financial transactions (e.g. Compliance, Internal Audit, or data processing centres) must be trained on the duties derived from the applicable legal and regulatory AML requirements initially upon commencement of employment with follow-up training on a regular basis.

Distribution

This policy is published using a form that can only be changed by the owner of this document. Any changes to this document require the approval from the Managing Board of Credit Europe Bank N.V.

Enforcement

Governments and regulators have taken money laundering seriously for a long time. Even so, recent events have made everyone, especially the authorities, more sensitive. Previously money laundering was strictly a matter of regulation and criminal statutes. The regulations and criminal laws still apply, of course, but money laundering has now become more a political issue than ever before. Countries all over the world have adopted new laws. Enforcement of existing laws is more aggressive than ever before. As a practical matter, this makes potential reputation damage much more immediate. Even an allegation of the lack of prevention of money laundering can result in catastrophic damage to CEB's ability to do business.

CEB is therefore committed to high standards of AML compliance and requires local management and all other staff of every CEB office to adhere to these standards in preventing the use of its products and services for money laundering purposes.

Getting Help

Any queries related to the content and interpretation of this policy can be addressed to local Compliance or the Country AML Officer where applicable.

Policy Authority

This policy is approved by the Managing Board of Credit Europe Bank N.V. and valid as per effective date. As a minimum, this policy will be reviewed and updated every two years.

Definitions

AML	Anti-Money Laundering
CEB	Credit Europe Bank Group, consisting of Credit Europe Bank N.V. (Head Office, branches, overseas liaison offices) and its subsidiaries
FATF	Financial Action Task Force
KYC	Know Your Customer
ML/TF	Money Laundering/Terrorist Financing
Wolfsberg Group	An association of global banks which aims to develop frameworks and guidance for the management of financial crime risks
Basel Committee	Basel Committee on Banking Supervision, the primary global standard setter for the prudential regulation of banks

***