



KOMERCIJALNA BANKA AD BEOGRAD

Anti Money Laundering and Terrorism Financing Policy of Komercijalna Banka a.d. Beograd

Introduction

There has been a growing recognition in recent years that an efficient way to fight against crime and terrorism is to prevent criminals, whenever possible, from legitimizing the proceeds of their criminal activities, by concealing the link between an activity and its funding, converting "dirty" funds to "clean" business, or "clean" funds to dirty business in case of terrorism financing.

Recent examples in the sphere of banking operations in the world, have demonstrated that banks handling the proceeds of crime face considerable risks such as credit, fraud and reputational risks that can lead to serious legal and financial difficulties but also have very serious consequences for business operations of banks.

In many countries, legislation and rules have been introduced in the respective banking systems to prevent as far as possible, banks and other financial institutions from becoming involved in money laundering activities.

In other countries where they have not yet been adopted, there are plans to introduce such laws and regulations, usually based on the same international standards.

In this context, Komercijalna Banka a.d. Beograd wishes to be at the forefront in Serbia in the fight against such crime.

Prompted by the desire to minimize the risks to the Bank can be possibly exposed and safeguard its reputation, Komercijalna Banka a.d. Beograd has introduced and implemented internally a set of rules, procedures and guidelines to prevent money laundering and terrorism financing.

The content of these documents is largely guided by generally accepted international principles, legal provisions and by-laws, and instructions which have been adopted by the Government of the Republic of Serbia, the Parliament of the Republic of Serbia and Administration for Preventing Money Laundering of the Republic of Serbia, which are at the same time an example of good international practice in anti-money laundering (AML) guidelines.

These procedures will be consistently applied in accordance with technical and human resources potentials of the Bank and they will be constantly coordinated with and amended to recent professional trends, international standards and legal amendments in order to align the Bank with developments in international banking practice in the prevention of money laundering and terrorism financing.

Section I

1. Definition

Money laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of criminal activities. If undertaken successfully, it also allows them to maintain control over those proceeds and, ultimately, to provide a legitimate cover for their source of income.

Terrorism financing uses the same methods to achieve the opposite outcome: concealing the final destination of funds, hence providing a cover for creating staff and material bases for organizing and executing terrorist activities.

2. Stages of Money Laundering

The requirement to launder the proceeds of criminal activities through the financial system is vital to the success of criminal operations. Those involved must use the facilities of global financial institutions if they are to benefit from the proceeds of their activities. The increased integration of the world's financial systems and the removal of barriers to the free movement of capital have enhanced the ease with which criminal money can be laundered and complicated the tracing process.

There is no single method of laundering money. Initially, however, the proceeds usually take the form of cash which needs to enter the financial system by some means. Despite the variety of methods employed, the laundering process is accomplished in **three stages**, which may comprise numerous transactions by the launderers and could alert a financial institution to criminal activity.

These stages are as follows:

- a) **Placement** - the physical deposit of cash proceeds derived from illegal activity.
- b) **Layering** - separating illicit proceeds from their source by creating sometimes complex layers of financial transactions adapted to disguising trails on the occasion of control or audit and thus provide anonymity.
- c) **Integration** - the provision of apparent legitimacy to criminally derived proceeds. If the layering process has been successful, integration schemes place the laundered proceeds back into the economy in such a way that they re-enter the financial system appearing as normal business funds.

These three basic steps may occur as separate and distinct phases, simultaneously or they may overlap which is more common.

The Table below provides some typical examples:

<i>Placement stage</i>	<i>Layering stage</i>	<i>Integration stage</i>
<ul style="list-style-type: none"> • Cash paid into a bank (sometimes with staff complicity or mixed with proceeds of legitimate business). 	<ul style="list-style-type: none"> • Money transfer abroad (often using shell companies or funds disguised as proceeds of legitimate business). 	<ul style="list-style-type: none"> • False loan repayments, forged invoices used as cover for laundered money.
<ul style="list-style-type: none"> • Cash transfer exported. 	<ul style="list-style-type: none"> • Cash deposited in international banking systems. 	<ul style="list-style-type: none"> • Complex web of transfers both domestic and international which makes tracing original source of funds virtually impossible.
<ul style="list-style-type: none"> • Cash used to buy goods, property or business assets of high value. 	<ul style="list-style-type: none"> • Resale of goods/ assets. 	<ul style="list-style-type: none"> • Income from property or legitimate business assets appears "clean", legal

Certain points of vulnerability have been identified in the money laundering process which the money launderer finds difficult to avoid and where his/her activities are more susceptible to being recognized:

- Entry of cash into the financial system;
- Cross-border flows of cash;
- Transfers within the financial system;
- Transfers out of the financial system.

Following 11 September 2001, general concerns regarding terrorist financing have been enhanced. The measures used to combat terrorist financing are similar to those for money laundering. In this, special attention is devoted to the fulfillment of requirements contained in the “know your customer” procedures.

Section II

Komercijalna Banka a.d. Beograd is aiming to establish and maintain specific Money Laundering Prevention Policies and Procedures (MLP) to safeguard that its business and businesses of its clients are not abused for the purpose of money laundering.

This set of policies, procedures, guidelines and instructions will be applied, develop and implement following the adoption and approval of the Bank’s Executive Board and the Board of Directors.

The Policy, Guidelines and Procedures of the Bank are complied with domestic regulations and international standards. Any subsequent amendments, coordination and revision of these regulations, will take into account the existing legislation of the country in force at the time and to the best possible extent.

These procedures are based on five key principles:

- Building up of internal awareness and responsibility of employees,
- Implementation of procedures “Know-Your Customer”, identification procedures,
- Record keeping,
- Recognition of suspicious transactions and reporting procedures to competent regulatory bodies,
- Getting to know the subject matter, training of employees.

1. Internal Awareness and Responsibility

1.1. Fundamental Principles

Komercijalna Banka a.d. Beograd is forbidden to accept assets which are, or can be suspected of being, the proceeds or funding of or for criminal activities. No anonymous, that is to say so-called numbered accounts are permitted. Komercijalna Banka a.d. Beograd is forbidden to enter into a business relationship with:

- (1) Individuals, groups, or legal entities that are listed on relevant United Nations Security Council lists, other international lists, and the Republic of Serbia’s list;
- (2) Individuals who have been indicted or convicted of crimes including, but not limited, to drugs trafficking, corruption, embezzlement of public funds, or money laundering;
- (3) Individuals for whom it is impossible to implement the Know Your Customer Procedure;
- (4) Individuals who maintain any business relationship with banks or other financial companies that do not maintain a physical business presence in the country in which they are registered (“shell banks”), unless they are subsidiaries of large banking or financial groups which are adequately regulated and supervised on a consolidated basis from a prudential rules and money laundering perspective.

1.2. Responsible and Authorized Person for the Prevention of Money Laundering (Money Laundering Officer - MLO) and Combating Terrorism Financing

Komercijalna Banka a.d. Beograd has appointed appropriate responsible and authorized persons (MLO) on the basis of positive regulations of the Republic of Serbia who are responsible for the proper implementation of these procedures in the whole Bank.

His/her/their responsibilities are particularly focused, among other things, on:

- Maintaining the internal AML procedures.
- Ensuring that Bank employees be informed of the Bank’s AML and anti-terrorism financing policies.
- Following-up on the execution and implementation of AML and anti-terrorism financing procedures and instructions.
- Establishing concrete parameters with which higher risk clients and transactions can be recognized, that is, ensuring that risk assessment and higher risk transactions are recognized properly and acted upon.

- Ensuring that the Procedures are followed in the event of questionable transactions. This includes but is not limited to informing the relevant state organs as necessary and in conformity with the law.
- Conducting all necessary investigations and gathering of all requested materials, in conformity with the Law on Internal Procedures.
- Ensuring that client information and documentation relevant to AML procedures is properly gathered and kept at all times
- Initiates and maintains contact with all relevant regulatory organs, writes and presents reports as required, and fully cooperates with all investigations and requests for information from relevant state organs.
- Regularly reports to the Director of Compliance Division and the Executive Board of the Bank on client relations with which prior agreement was given to proceed.
- Ensures awareness of international AML initiatives and ensures that the Bank pays particular attention to, and conducts itself accordingly, with regards to transactions originating with non-AML cooperative states and territories as defined by relevant watch-lists.
- Plans and supervises AML, anti-terrorism financing and know your customer employee training.
- Examines employee knowledge on AML and know your client procedures at least once per year.

To ensure effective fulfillment of his/her responsibilities, the MLO shall have sufficient number of qualified, competent and morally acceptable employees.

The MLO has an obligation to regularly report to Director of the Compliance Division and to the Executive Board of the Bank. The MLO should at all times act honestly and in good faith.

1.3. Internal Control of Compliance with MLP

The Compliance Division of the Komercijalna Banka a.d. Beograd performs the internal control of compliance with regulatory requirements and internal procedures in the purposes of the money laundering prevention and terrorist financing.

The Internal Audit Division of the Komercijalna Banka a.d. Beograd is responsible for audit and supervision of the implementation of the internal instructions and procedures in respect to the money laundering prevention and terrorist financing. All finding, in compliance with Methodology of the Internal Audit Division, will be reported to the Executive Board and Audit Committee of the Komercijalna Banka a.d. Beograd.

2. “Know Your Customer” Identification Procedures

The basis for effective prevention of money laundering is knowledge of the customers, based on satisfactory evidence of the identity of a customer, regardless of whether the customer is a private person or a business entity. No accounts should be opened or operated without satisfactory evidence of the identity of the customer.

In all cases, the most important priority for the Bank is to have determined a **good profile of its clients**, including accurate knowledge of the client’s business and financial activities, and good records of all information collected on the client in the client’s file. This profile should

be permanently added up and checked in the course of regular contacts and business cooperation.

This allows effective detection of suspicious transactions taking into consideration the fact that depending on the customer profile the same transaction can be perfectly normal for one client but highly suspicious in the case of another.

Opening an Account

2.1 Private Persons

Satisfactory evidence of the identity of a prospective customer must be obtained at all times. The following is necessary to satisfy these requirements:

a. Correctly determined full name and surname of the applicant which is supported by reliable identification documents (for example, personal identity card, passport or any other official document bearing a photograph and which has been issued by a competent authority). The photograph should be checked against the actual individual opening the account. The identity document must contain elements that will enable the issuer to track the relevant data (number and date of issue);

b. Correct permanent address in Serbia or abroad, supported by reliable identification documents (for example, personal identity card, passport or any other official document bearing a photograph and which has been issued by a competent authority).

If the Bank's officer opening the account has any doubts about the veracity of the address given on the identification documents, the Bank's officer will be obliged to also request additional pieces of evidence such as:

- Recent electricity or utility bills
- Tax return or bank statement.

c. Date of birth.

These data must be produced from original documents, and a copy of the original documents and details of such document/documents must be orderly kept on record, preferably in an electronic form but if not, then in hard copy.

2.2. Corporate Customers

In the case of opening an account for corporate customers, it is necessary to undertake all required measures for the purpose of establishing the identity of any person on whose behalf an applicant for establishing business relations is acting.

Before a business relationship is established, measures should be taken to ensure that the applicant has not been blocked, terminated or in the process of being dissolved, blocked or terminated.

Also, it is necessary to determine and precisely identify ownership structure for ownership participation in a company exceeding 10% of the overall ownership.

In addition to that, further checks should be made if changes to the company structure or ownership occur subsequently, or suspicions are aroused due to a change in the profile of payments through a company account.

For the opening of corporate customer accounts the following documents should be obtained:

- Certificate of incorporation or registration, a document issued by the competent government authority;
- Statute (if the corporate client is required to have such a document);
- An authorization of the member of management allowing the client to open an account and an authorization for a person to be in charge of proceeds handling and management;
- Personal data of employees authorized to operate the account.

2.3 Clubs, Societies and Charities

In the case of accounts opened for clubs, societies and charities, Komercijalna Banka a.d. Beograd will have to satisfy itself as to the legitimate purpose of the organization, obtaining evidence of the constitution and personal data of the signatories to the account. When such signatories change, care should be taken that personal data of the new signatories have been obtained in accordance with these procedures.

2.4 Trust Nominee and Fiduciary Accounts

When it is known or suspected that an account has been opened or a transaction has been undertaken on behalf of a third party, without the name of that third party being clearly disclosed and evidenced, sufficient information should be obtained as to the identity of the person on whose behalf the customer is acting. If sufficient information cannot be obtained, the account should not be opened.

2.5 Opening an Account by Post, Telephone or over the Internet (“Non Face-To-Face Verification”)

All accounts in the Bank can be opened only and exclusively with the personal presence and must not be opened without the face-to-face verification.

2.6 Customer Introduced by another Bank.

In accordance with current regulations in Serbia, Komercijalna Banka a.d. Beograd cannot place reliance on anti-money laundering checks performed by any other persons. Accordingly, customers introduced by another bank are subject to the same checks as any other potential customers of Komercijalna Banka a.d. Beograd.

3. Record Keeping

3.1 Financial Activities Subject to the Anti Money Laundering Procedures

The transactions subject to scrutiny for the purpose of money laundering prevention, record keeping and reporting to the regulatory authority if applicable, cover the following financial activities:

- Acceptance of deposits

- Lending which includes consumer loans, mortgage loans, factoring (with or without recourse), financing of commercial transactions (including forfeiting)
- Financial leasing
- Money transmission services
- Issuing and administering means of payment (credit cards, travelers cheques and banker's drafts)
- Guarantees and commitments
- Trading for account of customers in money market instruments (cheques, bills, bonds, etc.)
- Foreign exchange, financial operations: futures and options, exchange and interest rate instruments, transferable securities, foreign bank notes
- Participation in securities issues and the provision of services related to such activities
- Brokerage activities
- Safe keeping and administration of securities;
- Safe custody services.

3.2. Data to be acquired

For the purpose of establishing, maintaining, controlling and auditing transactions which may be identified as those followed by the MLO, and according to the applicable requirements of positive regulations of the Republic of Serbia, Komercijalna Banka a.d. Beograd will establish a register in which all transactions in excess of a counter value of EUR 15,000 will be recorded, whether these transactions are a single one-off or cumulative within a time frame of 30 days.

This Register will contain the following information:

- About the beneficial owner of the account,
- About the volume of proceeds flowing through the account,
- About the origin of proceeds,
- About the form in which the proceeds were offered or withdrawn (for example, cash, cheques, etc.),
- About the identity of the person undertaking the transaction,
- About the destination of the of proceeds,
- About the corresponding documentation and the purpose of transaction,
- About any other information related to the instructions received by the Bank.

If, at any the time during the course of undertaking a transaction, the relevant account officer or teller is concerned that a transaction may be suspicious, that person is obliged to do immediately:

- Contact the MLO or the Anti Money Laundering Department for guidance on additional information to be obtained before undertaking the transaction;
- Request the origin of the proceeds from the client and conduct any additional actions set forth in the procedures or determine real facts which are recommended by the MLO or the Anti Money Laundering Department.

In this situation, the account officer or teller should take care to ensure that the client does not become aware that there is a suspicion regarding the transaction (“tipping off”).

3.3 Time Frame and Responsibility for Record Keeping.

The data identified in 3.2 above must be entered in the appropriate register. The entries will also make reference to the files in which the transaction documents are kept.

All records, including the register must be kept in a fire-proof place for a minimum period of five years in compliance with legal regulations.

Responsibility for the entries in the register and the proper acquisition of supporting documents is vested with the MLO.

This documentation will be made available to the regulatory authorities if they so require, and to the external auditors.

Under no circumstances are the staff and employees allowed to

1. Disclose information regarding data acquired under the MLP,
2. Export outside the premises any document or information regarding transactions entered in the register under the MLP.

These restrictions include any data stored in computerized record format, and micro-film documents.

4. Suspicious Transaction Reporting

In addition to the compulsory reporting which arises as an obligation under the MLP, employees should report to the MLO any transaction perceived as suspicious in terms of potential criminal origins and consequently falling within the MLO responsibilities, irrespective of the amount of the transaction described in point 3.2 above.

The MLO shall enter in the Register all suspicious transaction reports received and review the content of these reports. The MLO should then determine what action, if any, to be taken by the Bank (including reporting to the relevant regulatory authorities) and record their decision in the Register, along with the reason and explanation.

5. Informing Employees with Materials and Training

The effectiveness of above stated AML procedures is clearly dependent on the level of awareness and training of employees regarding the matter. For this reason, each employee who is in charge of clients operations and relevant activities, irrespective of his duties, must be familiarized with these procedures and complied with them.

Some departments in the Bank and specific members of the Bank are potentially more exposed to money laundering attempts and are possibly in a position to uncover such activities. Therefore, it is anticipated that employees working in departments exposed to the risk will receive internal or external training on anti-money laundering operations at least once a year.

Internal or external training will be organized and conducted by the Anti Money Laundering and Terrorism Financing Department.

The training will include the following:

- All new employees in specified categories,
- Cashiers/foreign exchange operators,
- Account opening personnel and current account and deposits administrators,
- Supervisors and managers,
- Money transfer officers,
- Credit officers,
- Payment cards officers,
- Securities officers.

For the purpose of checking acquired knowledge, the Anti Money Laundering and Terrorism Financing Department will organize tests in the form of annual examination of employees in the specified fields.

For the purpose of executing the implementation of relevant regulations, as well as domestic and international standards for this field, in the most successful way, the Bank will establish and develop active cooperation with competent authorities of the Republic of Serbia, correspondent banks and international professional organizations and institutions.

Chairman of the Board of Directors

Vladislav Cvetkovic, M.Sc