CENTRAL BANKING AUTHORITY OF KOSOVO
AUTORITETI QENDROR BANKAR I KOSOVËS
CENTRALNI BANKARSKI AUTORITET KOSOVA

Advisory Letter 2007-1 **May 2007**

Prevention of Money Laundering and Terrorist Financing

1. PURPOSE

The purpose of this advisory letter is to provide guidelines for additional assistance to banks and financial institutions when implementing certain aspects of the anti-money laundering and combating the financing of terrorism (AML/CFT) requirements of Regulation 2004/2 on the Deterrence of Money Laundering and Related Criminal Offences, as amended, and Amended Rule X on the prevention of money laundering and terrorist financing, authorized under sections 20.1(a), 22, 24, 28.1(f), 32, 33 and 46 of Regulation no. 1999/21 on Bank Licensing, Supervision and Regulation.

2. OVERVIEW OF AML/CFT GUIDELINES

The Central Banking Authority of Kosovo (CBAK) recognizes that the territory of Kosovo could become a target for money laundering. Therefore, there is a need to protect the financial and operational integrity of the local and international markets. Consequently, much emphasis has been made on regulatory requirements for the prevention of money laundering and terrorist financing activities.

GUIDELINE NOTES

Section 22 of Regulation 1999/21 and Amended Rule X provide that banks and financial institutions shall inform the Financial Intelligence Center (FIC) of any evidence of money laundering, and report large currency transactions.

These guidelines are issued by the CBAK pursuant to the provisions of the Regulation and are applicable to all banks and financial institutions licensed by, or registered with, the CBAK.

The scope of these guidelines is to establish best practices according to international standards pursuant to established rules and regulations, and to establish standard procedures of communication between these institutions, the CBAK, and criminal investigation authorities.

These guidelines give an overview of the Prevention of Money Laundering section of the Regulation, and of Amended CBAK Rule X, on Money Laundering.

33 Garibaldi street Prishtina Kosovo UNMIK
Phone: **+381 38 222 055** Fax: **+381 38 243 763** **Web:** www.cbak-kos.org

It must be emphasized, however, that these guidelines are complementary to the Regulation. They should not be construed as a substitute to the Regulation. The responsibility for observing laws and regulations rests entirely with the individual institutions and their employees.

DEFINITIONS

Money laundering is the process through which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities with the ultimate aim of providing a legitimate and legal cover for their sources of income and finance. It is the vehicle through which organizations of serious crime live respectably with no apparent connections with the criminal world.

Criminal activities. The very definition of money laundering calls for an underlying criminal activity which generates the money to be laundered. Different countries have adopted different methods of addressing the underlying criminal activities. Whereas some countries have generalized and included all criminal activities, others have included a list of serious crimes which tend to generate large amounts of money.

PREVENTION OF MONEY LAUNDERING

The international recognition to fight money laundering on a global approach has identified the need to collectively prevent criminals, through all means possible, from legitimizing the proceeds of their criminal activities by converting funds from *dirty* to *clean*.

Although there are various methods of laundering money which can range from the purchase of property or luxury items to complex international networks of apparently legitimate business, the requirement of laundering the proceeds of criminal activity through the financial system is quite often vital to the success of such criminal operations.

The increased integration of the international financial systems, coupled with the free movement of capital through the removal of barriers, have enhanced the ease with which criminal money can be laundered by shifting it from one jurisdiction to another thus complicating the tracing or audit process.

STAGES OF MONEY LAUNDERING

Whatever method is used to launder money, the process is normally accomplished in three stages. These may occur as separate and distinct phases although they may occur simultaneously, at times even overlapping, depending on the criminal organizations involved. The three stages usually comprise numerous transactions by the launderers to try to hide or conceal the tracing process. Such transactions could, however, alert a bank or financial institution to suspect criminal activity through any of these three stages:

- Placement – the physical disposal of cash proceeds derived from illegal activity, e.g., placing it in a bank account;

- Layering – the creation of numerous complex layers of financial transactions being the separation of proceeds from their source aimed to disguise the audit trail thus providing anonymity, e.g., transfers from one account to another, switching currency, changing jurisdiction; and

- Integration – the provision of an apparent legitimate explanation for the illegally derived wealth to be put back into the economic sector, e.g., liquidation of an investment to use proceeds for an apparent legitimate business.

A successful layering process simplifies the integration process schemes to put the laundered proceeds back into the economy in such a way that they re-enter the financial system as normal business funds.

USE OF BANKS AND FINANCIAL INSTITUTIONS

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

- Entry of cash into the financial system;
- Cross-border flow of funds; and
- Transfers within and from the financial system.

It is for this reason that most countries have, to a large extent, concentrated their efforts on the placement stage. Preventing the financial system from being used for money laundering activities has proved to be more effective in making the process of money laundering more difficult. It does not, however, prevent the money launderer from looking for and using other methods to launder his illegal proceeds.

Although most regulations on the prevention of money laundering focus on the placement stage, it is emphasized that banks and financial institutions, as providers of a wide range of servicers, are still vulnerable to being used in the layering and integration stages. Extending credit and the rapid switching of funds between accounts in different names and jurisdictions may be used as that part of the process to create complex layers of transactions.

Banks and financial institutions which become involved in money laundering schemes will risk likely prosecution, loss of their good market reputation and the possible loss of their operation license.

3. GUIDELINES TO BANKS AND FINANCIAL INSTITUTIONS ON THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING

Customer Due Diligence

The following sections provide explanations and additional guidance with respect to some of the terminology used in the Amended Rule X.

In applying enhanced due diligence, banks and financial institutions should take care not to engage in unlawful discrimination on the basis of race, color, religion, or national origin.

CUSTOMERS

Customer includes a person or entity which conducts a transaction with or uses the services of a bank or financial institution, as well as any owner or beneficial owner or other person or entity on whose behalf the transaction is conducted or the services are received.

BUSINESS RELATIONSHIP

A business relationship with a bank or financial institution means to engage the financial services of the bank or financial institution for more than an occasional transaction or transactions. Financial services mean those activities as listed in section 1.12 of Regulation 2004/2, as amended. A business relationship with a bank or financial institution does not include doing business with the bank or financial institution in another capacity, such as providing goods or services to the bank or financial institution or engaging other services from the bank or financial institution.

NON FACE-TO-FACE BUSINESS

Non face-to-face business may include:

a. business relationships concluded over the internet or by other means such as through the post;
b. services and transactions over the internet including trading in securities by retail investors over the internet or other interactive computer services;
c. use of ATM machines;
d. telephone banking;
e. transmission of instructions or applications via facsimile or similar means; and
f. making payments and receiving cash withdrawals as part of electronic point of sale transaction using prepaid, re-loadable or account-linked value cards.

ADDITIONAL GUIDANCE ON IDENTIFICATION DOCUMENTS

For verification of the identity of customers who are natural persons, the bank or financial institution should use reliable, independent source documents, data, or information, such as a government issued ID card or passport. Identification of natural persons and verification of their identity shall include the full name and address, date [and place] of birth.

In the process of obtaining and verifying an entity's identification information (such as corporate name, head office address, identities of directors, proof of incorporation or evidence of legal status, legal form and provisions governing the authority to commit the entity) banks and financial institutions should use documents that prove:

a. the customer's name and legal form, including proof of incorporation or similar evidence of establishment or existence (such as a certificate of incorporation or a trust instrument);
b. the names and addresses of members of the customer's controlling body such as for companies the directors, for trusts the trustees, and for limited partnerships, the general partners, and senior management such as the chief executive officer;
c. the legal provisions that set out the power to bind the customer (such as the memorandum and articles of association or trust instrument);
d. the legal provisions that authorize persons to act on behalf of the customer (such as a resolution of the board of directors or statement of trustees on opening an account and conferring authority on those who may operate the account); and
e. the identity of the physical person purporting to act on behalf of the customer.

ENHANCED CUSTOMER DUE DILIGENCE FOR HIGHER RISK CUSTOMERS

Relevant factors in determining if a customer is higher risk include if the person is:

a. a non-resident, or if the nationality, current residency, or previous residency of the person suggests greater risk of money laundering or terrorist financing;

b. connected with jurisdictions that lack proper standards in the prevention of money laundering or terrorist financing;
c. a politically exposed person (PEP) or linked to a PEP;
d. a very high net worth individual;
e. a private banking customer;
f. engaged in a business that is particularly susceptible to money laundering or terrorist financing;
g. a legal person or arrangement that is a personal asset holding vehicle;
h. a legal person or arrangement whose ownership structure is complex for no apparent reason; and
i. a company with nominee shareholders or shares in bearer form.

This list is not exhaustive and other factors may also be relevant.

In addition to scrutiny of the source of wealth and the source of funds of the customer, enhanced customer due diligence may, among other things, include enhanced:

a. scrutiny of customer identification (including of the beneficial owner and controller);
b. scrutiny of the legitimacy of the recipient of funds;
c. transaction monitoring; and
d. customer profiling.

Politically exposed person means any person who is or has been entrusted with prominent public functions in any country[1], as well as members of such person's family or those closely associated with that person.

Procedures for determining who is a PEP may include:

a. seeking relevant information from the potential customer;
b. referring to publicly available information; and
c. making access to commercial electronic databases of PEPs.

Recognition of Suspicious Acts and Transactions

Certain types of transactions should alert the financial institution to the possibility that the customer is conducting suspicious activities. They may include transactions that do not appear to make economic, lawful or commercial sense, or that involve large amounts of cash movements that are not consistent with the normal and expected transactions of the customer. Very high account turnover, inconsistent with the amount of funds normally held in the account, may indicate that funds are being laundered. Examples of bank-specific suspicious activities can be very helpful to financial institutions and should be included in the training activities.

A suspicious act or transaction will often be one that is inconsistent with a customer's known, legitimate business or personal activities or with the normal business for that type of financial product. The financial institution should gather information to learn about the customer and the customer's business to help them to recognize when a transaction is unusual.

[1 In line with FATF (Financial Action Task Force) Recommendation 6, the CBAK may choose whether to retain this requirement only for foreign PEPs, or to apply it also to domestic PEPs.]

Questions that a financial institution might consider when determining whether an act or transaction might be suspicious are:

- Is the size of the transaction consistent with the normal activities of the customer?
- Is the transaction rational in the context of the customer's business or personal activities?
- Has the pattern of transactions conducted by the customer changed?
- Where the transaction is international in nature, does the customer have any apparent reason for conducting business with the other country involved?

Some indicators of suspicious acts or transactions are given in the Annex.

Action of AML/CFT Compliance Function on Being Notified of a Potential Suspicious Transaction

The AML/CFT compliance function should acknowledge receipt of a report of a staff member and at the same time provide a reminder of the obligation to do nothing that might prejudice enquiries, i.e., 'tipping off' in the sense of section 3.12 of Regulation 2004/2.

After receiving the initial report, the internal AML/CFT compliance function must make certain enquiries, among others (if appropriate):

a. The origin of the assets deposited;
b. The purpose of large withdrawals of assets;
c. The rationale for large deposits;
d. The occupation or business activity of the customer and the beneficial owner;
e. Whether the customer or the beneficial owner is a politically exposed person;
f. In the case of legal entities: who controls such entities.

Depending on the circumstances, the analysis shall include, among others:

a. obtaining information in written or oral form from the customer or beneficial owner;
b. visits to the places of business of the customer and beneficial owner;
c. consulting publicly accessible sources and databases;
d. information from other trustworthy individuals, where necessary.

Additional Guidance on Originator Information for Electronic or Wire Transfers

Electronic or wire transfer means any transaction carried out on behalf of an originator person (both natural and legal) through a financial institution by electronic means with a view to making an amount of money available to a beneficiary person at another financial institution.

The originator is the account holder, or where there is no account, the person (natural or legal) that places the order with the financial institution to perform the electronic or wire transfer.

The policies and procedures on originator information are not intended to cover a) any transfer that flows from a transaction carried out using a credit or debit card so long as the credit or debit card number accompanies all transfers flowing from the transaction; b) transfers and settlements between banks and financial institutions where both the originator and the beneficiary are banks or financial institutions acting on their own behalf.

When credit or debit cards are used as a payment system to effect a transfer, they are covered by Rule X and its Guidelines, and the necessary information should be included in the message.

Beneficiary financial institutions shall have procedures in place to identify and scrutinize wire transfers that are not accompanied by complete originator information. Procedures to address these cases should include the bank first requesting the missing originator information from the financial institution that sent the wire transfer.

If the missing information is not forthcoming, the requesting financial institution should consider whether, in all the circumstances, the absence of complete originator information creates or contributes to suspicion about the transfer. If the transfer is deemed to be suspicious, it should be reported by the beneficiary bank or financial institution to the FIC. In addition, the bank or financial institution may decide not to accept the transfer.

In appropriate circumstances, such as two or more transactions with incomplete or absent originator information, the beneficiary bank or financial institution should consider restricting or terminating business relationships with the bank or financial institution that does not comply with this requirement.

Additional Guidance on Cross-Border Correspondent Banking and Similar Relationships
Correspondent banking is defined as the provision by one bank (the correspondent) to another bank (the respondent) of credit, deposit, collection, clearing or payment services.

To assess the potential respondent bank's controls against money laundering and terrorist financing, the bank should gather sufficient information about the potential respondent bank to understand their business and determine from publicly available information the reputation of the institution, quality of supervision, and whether it has been subject to a money laundering or terrorist financing investigation or regulatory action. The bank should in general establish or continue a correspondent relationship with a foreign respondent bank only if it is satisfied that an authority is effectively supervising the respondent bank. In particular, a bank should not establish or continue a correspondent banking relationship with a non-resident respondent bank incorporated in a jurisdiction in which the bank has no presence and which is unaffiliated with a regulated financial group (i.e., a shell bank).

The information to be collected may include details about the non-resident respondent bank's management, major business activities, where it is located, its money laundering and terrorist financing prevention efforts, the system of bank regulation and supervision in the respondent bank's country, and the purpose of the account.

A bank should pay particular attention when maintaining a correspondent banking relationship with non-resident banks incorporated in jurisdictions that do not meet international standards for the prevention of money laundering and terrorist financing. Enhanced due diligence will generally be required in such cases, including obtaining details of the beneficial ownership of such banks and more extensive information about their policies and procedures to prevent money laundering and terrorist financing.

Particular care should also be exercised where the bank's respondent allows direct use of the correspondent account by third parties to transact business on their own behalf (i.e., payable–through

accounts). The bank has to be satisfied that the respondent bank has performed the customer due diligence for those customers that have direct access to the accounts of the correspondent, and that the respondent is able to provide relevant customer identification information on request of the correspondent.

The banks should document the respective AML/CFT responsibilities of each institution. It is not necessary that the two banks always have to reduce the respective responsibilities into a written form provided there is a clear understanding as to which institution will perform the required measures.

Additional Guidance for Foreign Exchange Offices and Money Transfer Operators

CDD AND MONITORING

Although the identification and verification requirements of section 3.1(d) of Regulation 2004/2 must be complied with, application of full customer due diligence is not necessary when transactions with a client occur occasionally (i.e., a few times per year). In cases where transactions occur more frequently, the business relationship should be perceived as ongoing, requiring further customer identification procedures.

RECORD KEEPING AND RETENTION

Also in the absence of an ongoing business relationship, Foreign Exchange Offices and Money Transfer Operators should keep copies of the identification data and transaction data for a period of five years following a transaction.

ORIGINATOR INFORMATION

Money Transfer Operators sending an electronic or wire transfers under [≤€1,000] do not have to include full originator information with the transfer. They shall however, in accordance with section IV(g) of Rule XVI, be in a position to make the full originator information available to the beneficiary and to the CBAK or the FIC within three business days of receiving a request.]

REPORTING OF TRANSACTIONS

The Foreign Exchange Offices and Money Transfer Operator should consider that the fact that a customer shows a preference to conduct a currency transaction under the €10,000 threshold, presumably to avoid reporting, creates or contributes to a suspicion about the transaction. They should also consider that multiple currency transactions that are conducted by or on behalf of one person or entity and that total more than €10,000 over a period of time creates or contributes to suspicion about the transactions.

Annex to Guidelines
Indicators of Potential Money Laundering and Financing of Terrorism

The indicators of potential money laundering and terrorist financing activity set out below are primarily intended to raise awareness among the staff of banks and financial institutions.

These indicators are not intended to be exhaustive and provide examples only of the most basic ways by which money may be laundered or terrorism may be financed. However, identification of any of the types of transactions listed here should prompt further analysis.

GENERAL INDICATORS

Transactions where the structure indicates some illegal purpose, their commercial purpose is unclear or appears absurd from a commercial point of view.

Transactions where the customer's reason for selecting this particular financial institution or branch to carry out its transactions is unclear.

Transactions which are inconsistent with the financial intermediary's knowledge and experience of the customer and the stated purpose of the business relationship.

Customers who supply false or misleading information to the financial institution, or refuse for no credible reason to provide information and documents which are required and routinely supplied in relation to the relevant business activity.

Transactions with a country or jurisdiction deemed to be uncooperative by the Financial Action Task Force (FATF), or business relationships with counterparts domiciled in these countries.

The execution of multiple cash transactions just below the threshold for which customer identification or transaction reporting is required.

The structure of the customer's business relationship with the financial institution lacks a logical rationale (large number of accounts at the same institution, frequent transfers between accounts, excessive liquidity, excessive use of cash where the type of business usually is non-cash etc.).

Transfers of large amounts, or frequent transfers, to or from countries producing illegal drugs or known for terrorist activities.

Customer tries to evade attempts by the financial intermediary to establish personal contact.

Customer requests business relationships to be closed and to open new relationship in his own name, or in the name of a family member, without leaving a paper trail.

Customer has been prosecuted for a criminal offence, including corruption or misuse of public funds.

Transactions that unexpectedly result in zero customer's balance.

Application for business from a potential client in a distant place where comparable service could be provided closer to home.

Application for business outside the financial institution's normal pattern of business.

Any want of information or delay in the provision of information to enable verification to be completed.

Any proposed transaction involving an undisclosed party.

Unusually large introductory commissions.

SPECIFIC INDICATORS FOR BANKS AND FINANCIAL INSTITUTIONS

Transactions involving a withdrawal of assets shortly after funds have been deposited with the bank (pass-through accounts).

Transactions resulting in significant, but unexplained, activity on an account which was previously mostly dormant.

The exchange of a large amount of small-denomination banknotes (EUR or foreign) for large-denomination banknotes.

The exchange of large amounts of money without crediting a customer account or outside the normal course of business for the customer.

Cashing cheques for large sums, including travellers' cheques outside the normal course of business for the customer.

The purchase or sale of large amounts of precious metals outside the normal course of business for the customer.

The purchase of banker's drafts for large amounts outside the normal course of business for the customer.

Instructions to make a transfer abroad by occasional customers, without apparent legitimate reason.

The acquisition of bearer instruments by means of physical delivery.

Frequent deposits or withdrawals of large amounts of cash which cannot be explained by reason of the customer's business.

Use of loan facilities that, while normal in international trade, is inconsistent with the known activity of the customer.

Accounts through which a large number of transactions are routed, though such accounts are not normally used, or only used to a limited extent.

Provision of security (pledges, guarantees) by third parties unknown to the financial institution, who have no obvious affiliation to the customer and who have no credible and apparent reasons to provide such guaranties.

Accepting funds transferred from other financial institutions when the name or account number of the beneficiary or remitter has not been supplied.

Transfers of large amounts of money with instructions that the sum be paid to the beneficiary in cash.

A large number of different individuals make cash deposits into a single account.

Unexpected repayment of a non-performing loan without any credible explanation.

Withdrawal of funds shortly after these have been credited to the account (pass-through account).

Fiduciary loans (back-to-back loans) for which there is no obvious legal purpose.

Customer requests receipts for cash withdrawals or deliveries of securities which in effect never took place, followed by the immediate deposit of such assets at the same bank.

Customer requests payment orders to be executed with incorrect remitter's details.

Customer requests that certain payment be routed through nostro accounts held by the financial intermediary or sundry accounts instead of its own account.

Request by the customer to accept or record in the accounts loan collateral which is inconsistent with commercial reality, or grant fiduciary loans for which notional collateral is recorded in the accounts.

Customers has several accounts in different branches of the same bank which cannot be explained by reason of the customer's business.

A customer makes a lot of cash deposits for a company that normally does not deal with cash.

Frequent unusual transactions between a customer's personal and business accounts

Introduction of business by an agent/intermediary in an unregulated or loosely regulated jurisdiction or where criminal activity is prevalent.

SPECIFIC INDICATORS FOR SECURITIES DEALERS

Business relationships that have been inactive suddenly experience large investments that are inconsistent with the normal investment practice of the customer or their financial ability.

Customer wishes to purchase securities, where the transaction is inconsistent with the normal investment practice of the customer or their financial ability.

Customer uses securities or brokerage firm as a place to hold funds that are not being used in trading of securities for an extended period of time and such activity is inconsistent with the normal investment practice of the customer or their financial ability.

Customer makes large or unusual settlements of securities in cash.

Transfers of funds or securities between accounts not known to be related to the customer.