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

1. Scope of Rule

This Rule applies to banks and financial institutions as defined in Regulation 2004/2 operating in Kosovo, including money transfer operators and foreign exchange offices.

This Rule establishes anti-money laundering and combating the financing of terrorism (AML/CFT) requirements regarding customer due diligence, record keeping and retention, monitoring of transactions, reporting of currency and suspicious transactions, internal policies and procedures, and training and screening of staff.

2. Responsibilities of the Governing Board and Management

As an important part of its overall responsibility for governance and management, the Governing Board of the bank or financial institution shall:

a. Adopt effective AML/CFT policies and procedures;
b. Ensure that the AML/CFT policies and procedures are fully implemented in practice;
c. Ensure that its internal AML/CFT compliance function and internal audit are technically equipped and staffed with personnel who have thorough knowledge of the AML/CFT policies and procedures, as well as possessing high ethical standards and relevant expertise;
d. Adopt a policy on establishing and maintaining business relationships, particularly those involving higher risk, including politically exposed persons;
e. Reserve to the Governing Board the role of removing the Head of the AML/CFT compliance function, should circumstances require such removal;
f. Receive and discuss the internal audit reports regarding AML/CFT policies and procedures implementation.
g. Adopt such other measures as may, from time to time, be required by the CBAK.

Management of the bank or financial institution shall be responsible for ensuring effective implementation of all of its AML/CFT policies and procedures on a day-to-day basis.

3. Internal AML/CFT compliance function

Banks and financial institutions shall appoint one or more qualified individuals with relevant expertise and experience to their AML/CFT compliance function and select a senior person as Head of the function, who will act as contact person for the purposes of section 3.16 of Regulation 2004/2. The Head of the function can be removed from his position only with the prior consent of the Governing Board. Should this occur, the bank

or financial institution shall notify their decision immediately to the CBAK, indicating the basis for removal.

The AML/CFT compliance function shall advise and assist the Governing Board and management in implementing the AML/CFT rules and regulations. It shall be responsible, inter alia, for:

a. preparing internal AML/CFT policies and procedures (under section 4 of this Rule) for approval by the Governing Board;
b. monitoring the implementation of internal AML/CFT policies and procedures;
c. liaising with internal and external auditors and management on matters relating to AML/CFT;
d. planning and overseeing AML/CFT training;
e. defining the criteria for business relationships involving higher risk as described in section 6 of this Rule;
f. reporting to the Financial Intelligence Centre (FIC) in accordance with sections 3.9 and 3.10 of Regulation 2004/2;
g. such other tasks assigned by the Governing Board or management to assist in preventing the use of the bank or financial institution for money laundering or terrorist financing purposes.

4. Internal AML/CFT policies and procedures

Banks and financial institutions shall adopt internal AML/CFT policies and procedures and communicate them to all relevant staff.

Such internal policies and procedures shall at a minimum set out:

a. the procedure on customer due diligence in accordance with section 6 of this Rule;
b. a procedure for collecting and maintaining information and records in accordance with Regulation 2004/2, and for preventing unauthorized access thereto;
c. a procedure for reporting to the FIC in accordance with sections 3.9-3.15 of Regulation 2004/2;
d. the criteria to be applied in identifying business relationships which involve higher risk as defined in section 6 of this Rule;
e. the policy on politically exposed persons;
f. the procedures for the development by the bank or financial institution of its own set of indicators of money laundering and terrorist financing activities;
g. the situations in which the internal AML/CFT compliance function must be consulted by staff and cases in which the Governing Board must be notified of events relevant to AML/CFT;
h. the policy on staff vetting, screening and training for AML/CFT purposes;

These internal AML/CFT policies and procedures shall be adopted by resolution of the Governing Board and implemented on a day-to-day basis by management and staff.

5. The role of internal [and external] audit

The internal audit function in banks and other financial institutions shall perform regular checks to ensure that the policies and procedures for AML/CFT prevention are fully implemented and compliant with all requirements of Regulation 2004/2, this Rule and relevant Guidelines. The internal audit function shall report periodically to the Governing Board of the bank or financial institution on its findings and evaluations, including an evaluation of the adequacy of staff training on AML/CFT matters.

The CBAK may require that banks and financial institutions engage their external auditors to evaluate and report on the quality of implementation of AML/CFT measures (including the application of the legal and regulatory requirements, implementation of policies and procedures, internal control systems and performance of internal audit).

6. Customer Due Diligence

Banks and financial institutions shall conduct thorough customer due diligence including:

a. identification of customers, including beneficial owners;
b. gathering of information on customers to create a customer profile;
c. application of acceptance policies for new customers;
d. maintenance of customer information on an ongoing basis;
e. monitoring of customer transactions; and
f. implementing prescribed policies and practices on electronic or wire transfers and correspondent banking.

6.1 Identification of Customers

Banks and financial institutions shall ensure that they know the true identity of the customer and have thorough knowledge of the customer's business before entering into the business relationship, on the basis of the obligations of sections 3.1-3.7 of Regulation 2004/2, as amended, and specifically the identification documents that are specified in sections 3.3 and 3.4 of that Regulation.

Banks and financial institutions shall take additional steps to ensure proper customer identification when doubts have arisen as to the veracity or adequacy of previously-obtained identification data, or where there is a suspicion that the customer is involved in money laundering or terrorist financing.

In the event that banks and financial institutions conduct business or execute transactions with a customer who is not physically present for purposes of identification, banks and financial institutions shall take additional measures to address the specific risk of money laundering and financing of terrorism.

Additional measures for non face-to-face business may include:

a. verification of documents;

b. requisition of additional documents, such as utility bills;
c. development of other means of contact with the customer.

6.2 Determination of the Beneficial Owner

Banks or financial institutions shall take measures to determine if a customer is acting on behalf of one or more beneficial owner(s) in accordance with section 3.2 of Regulation 2004/2. If so, the bank or financial institution shall take reasonable steps to verify the identity of the beneficial owner by using relevant information or data obtained from a reliable source so that the bank or financial institution is satisfied that it knows the identity of the beneficial owner.

For customers that are entities as defined in Regulation 2004/2, the bank or financial institution shall take reasonable measures to understand the ownership and control structure of the entity. This includes identifying the natural person(s) who ultimately owns or controls the entity.

For entities that are non-profit organizations (such as clubs, societies, and charities) the bank or financial institution shall also satisfy itself as to the legitimate purpose of the organization, including by reviewing its charter, constitution, or trust instrument.

Beneficial owner shall mean the natural person who ultimately owns or controls a customer, the person on whose behalf a transaction is being conducted. It includes a person who exercises ultimate effective control over an entity.

6.3 Enhanced Customer Due Diligence for Higher Risk Customers, Business Relationships, and Transactions

Banks and financial institutions shall apply enhanced customer due diligence for customers, business relationships, and transactions that are likely to pose a higher risk of money laundering and terrorist financing. Business relationships with a politically exposed person (PEP) shall always be deemed to involve higher risk.

Enhanced customer due diligence shall be applied at each stage of the customer due diligence process to customers, business relationships, and transactions that the bank or financial institution has determined are of higher risk of money laundering and terrorist financing. This will include scrutiny of the source of wealth and the source of funds of the customer.

A bank or financial institution shall not enter into or maintain a business relationship with a higher risk customer unless a senior member of the management of the bank or financial institution has given approval in writing.

6.4 Establishment of Customer Profile

Banks and financial institutions shall collect information regarding the anticipated purpose and intended nature of the business relationship.

Banks or financial institutions shall create and maintain a customer profile for each customer of sufficient nature and detail to enable the bank or financial institution to monitor the customer's transactions, apply enhanced customer due diligence where necessary, and detect suspicious transactions as required by section 3 of Regulation 2004/2 and this Rule. The level of detail contained in the profile should be consistent with the level of risk expected to be posed by the customer.

A customer profile shall include relevant information as to the normal and reasonable activity for particular types of customers taking into account the nature of the customer's business, as well as a comprehensive understanding of the customer's transactions (including as needed the source and legitimacy of the funds) and the overall relationship with the bank or financial institution.

6.5 Acceptance of New Customers

In cases where a bank or financial institution is unable to verify the identity of a customer in accordance with section 3.7 of Regulation 2004/2, the bank or financial institution shall refuse the transaction and consider filing a suspicious transaction report as provided in section 3.9 of Regulation 2004/2.

Procedures, policies, and controls on acceptance of new customers shall not be so restrictive that they result in a denial of access by members of the general public to financial services, especially for persons who are financially or socially disadvantaged.

6.6 Maintaining Customer Information on an Ongoing Basis

Banks or financial institutions shall gather and maintain customer information on an ongoing basis. Documents, data, or information collected under the customer due diligence process shall be kept up to date and relevant by undertaking periodic reviews of existing records, including transaction records.

6.7 Termination of Customer Relationship

If the bank or financial institution is unable to comply with the customer due diligence required for a customer, it shall terminate the customer relationship and determine if it should file a suspicious transaction report as provided in section 3.9 of Regulation 2004/2.

7. Monitoring of business relationships and transactions

Banks and financial institutions shall conduct ongoing due diligence on the business relationship and scrutinize transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile. Where necessary

for this purpose, information should be sought to confirm the source of funds. Banks and financial institutions shall have systems in place to detect large or complex transactions being carried out outside of expected norms for that type of customer.

Banks and financial institutions shall apply intensified monitoring for higher risk customers. Every bank and financial institution should set key indicators for such accounts taking note of the background of the customer, such as the country of origin and source of funds, the type of transactions involved, and other risk factors as set out in section 6 of this Rule.

8. Record-Keeping and Retention

Banks and financial institutions shall retain all necessary records of transactions, both domestic and international, for at least five years following completion of the transaction (or longer if requested by CBAK, FIC or any other competent authority in specific cases). This requirement applies regardless of whether the business relationship is ongoing or has been terminated.

Transaction records must be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. Necessary components of transaction records include:

a. the name of the customer and the beneficial owner (and holder of a power of attorney, if applicable) and their addresses or other identifying information as normally recorded by the bank or financial institution;
b. the nature and date of the transaction;
c. the type and amount of currency involved; and
d. the type and identifying number of any account involved in the transaction.

Banks and financial institutions shall also retain all necessary records relating to the customer, beneficial owner, or holder of power of attorney, account files, and business correspondence for at least five years following the termination of the business relationship, or in specific cases for a longer period if requested by the CBAK, FIC, or other competent authority. The records shall identify the staff member who carried out the identification of the customer (and beneficial owner, where applicable).

Banks and financial institutions shall establish safeguards to protect the records from damage and to prevent unauthorized access.

Banks and financial institutions shall make available on request to the CBAK, FIC, and other competent authority all records and available information on a customer, beneficial owner, or holder of a power of attorney and all requested transaction records, in a form and manner that is comprehensive, timely, and comprehensible.

Where the bank or financial institution is aware that records relate to on-going investigations, such records should be retained until it is confirmed by the relevant law enforcement agency that the case has been closed.

9. Recognition of suspicious acts and transactions

Banks and financial institutions shall give sufficient guidance and training to staff to enable them to recognize suspicious acts and transactions.

Banks and financial institutions shall ensure that all employees know to which person within the bank or financial institution the staff member should report suspicions and that there is a clear reporting chain under which those suspicions will be passed to the AML/CFT compliance function. The reporting line between the person having the suspicion and the AML/CFT compliance function should be as short as possible.

Once the AML/CFT compliance function has received this initial report, it shall check and analyze the case. Banks and financial institutions shall keep records of such analysis and results. If, on review of the analysis and results, the bank or financial institution concludes that the acts or transactions provide reasonable grounds for suspicion of money laundering, or that there is a link to terrorist or terrorist financing activity, the AML/CFT compliance function shall report the act or transaction to the FIC promptly. All internal enquiries made in relation to the report, and the basis for deciding whether or not to submit the report to the FIC, should be documented. Records of suspicions which were raised internally with the AML/CFT compliance function but not disclosed to the FIC should be retained for five years from the date of the transaction. Records of reported suspicions that assist with investigations should be retained until the bank or financial institution is informed by the relevant law enforcement agency that the records are no longer needed.

10. Reporting of suspicious acts and transactions and cash transactions exceeding 10,000 Euro

Section 3.9 of Regulation 2004/2 requires reporting to the FIC of suspicious acts and transactions and of transactions in currency exceeding 10,000 Euro.

Sufficient information should be disclosed which indicates the nature and the reason for the suspicion and, if a particular offence is suspected, this should be stated. Where the bank or financial institution has additional relevant evidence that could be made available, the nature of this evidence should be clearly indicated when reporting, without delay, to the FIC.

If a bank or financial institution decides not to enter into a business relationship because of suspicion of money laundering or terrorist financing, it shall report the matter to the FIC immediately.

[Banks and financial institutions shall report to the FIC any customer or transaction that they have reasonable grounds to suspect may be linked to the financing of terrorism or to individuals who support terrorism. Attention should be devoted to monitoring and keeping up to date the list of organizations and individuals related to terrorists or terrorism based on information received from the FIC, or other available sources.

Attention shall be paid to non-profit and humanitarian organizations, especially if the activities are not in accordance with the registered activity, if the source of funds is not clear, or if such organizations receive assets from suspicious sources.]

11. Originator information

Banks and financial institutions shall obtain and maintain full originator information for all electronic or wire transfers and verify that the information is accurate and meaningful.

Full originator information includes:

a. the name of the originator;
b. the originator's account number, or a unique reference number if there is no account number; and
c. the originator's official identification number, or another identification number, date and place of birth, and address.

Banks and financial institutions shall include the full originator information in the message or payment form accompanying the transfer, and when they act as intermediaries in a chain of payments, they shall maintain the full originator information with the transfer and transmit it.

In the case of domestic electronic or wire transfers, it is sufficient for the ordering bank or financial institution to include only the originator's account number or, where no account number exists, a unique identifier, within the message or payment form, providing that full originator information can be made available to the beneficiary bank or financial institution and to the CBAK or the FIC within three business days of receiving a request.

Beneficiary banks or financial institutions shall identify and scrutinize wire transfers that are not accompanied by complete originator information. They shall take measures to obtain and verify the missing information from the ordering bank or financial institution or from the beneficiary. Should they not obtain the missing information they should refuse acceptance of the transfer and consider filing a suspicious activity report with the FIC.

12. Cross-border Correspondent Banking and Similar Relationships

Banks shall develop and implement policies and procedures concerning correspondent banking.

A bank should exercise caution and due diligence regarding the potential respondent bank's controls against money laundering and terrorist financing and determine that such controls are adequate and effective, and should document the respective AML/CFT responsibilities of each institution.

A bank shall develop and implement policies and procedures concerning the ongoing monitoring of activities conducted through correspondent accounts. A bank shall obtain approval from senior management before establishing new correspondent relationships.

13. Additional requirements for Foreign Exchange Offices and Money Transfer Operators

Foreign Exchange Offices and Money Transfer Operators shall comply with the general AML/CFT principles of this Rule.

Foreign Exchange Offices and Money Transfer Operators shall develop and implement procedures to pay particular attention to multiple currency transactions that are conducted by or on behalf of one person or entity and that total more than 10,000 Euro in a single day, or series of transactions over a short period of time. When multiple currency transactions are executed at different branches of the Foreign Exchange Office or Money Transfer Operator, they shall be treated as a single transaction.

The procedures shall ensure that as soon as it becomes clear to the Foreign Exchange Office or Money Transfer Operator that a customer is conducting transactions under 10,000 Euro at different locations in a single day, the customer has to be identified and reported to the FIC.

Money Transfer Operators shall ensure identification of a customer (natural or legal person) both on payment and receipt of funds.

14. Vetting, Screening and Training of Staff

The effectiveness of the procedures and recommendations contained in this Rule depends on the extent to which staff in banks and financial institutions appreciate the serious nature of money laundering and terrorist financing. Banks and financial institutions shall make the staff aware of their personal statutory obligations, and inform them that they can be held personally liable for failure to report information in accordance with internal policies and procedures.

Banks and financial institutions shall introduce comprehensive measures to ensure that their employees, especially staff having contact with customers or executing transactions and staff within the AML/CFT compliance function, do not have a criminal record or are not the subject of an ongoing criminal prosecution for financial crime, terrorism, or other serious crime which could call into question their trustworthiness.

Banks and financial institutions shall provide regular training to all relevant staff on AML/CFT prevention. New staff shall undergo AML/CFT training before they may engage in opening business relationships with customers or executing financial transactions.

Employees must be made aware of the internal policies and procedures put in place to prevent money laundering and financing of terrorism, the legal requirements contained in

Regulation 2004/2 and in this Rule, particularly in relation to recognition, monitoring and reporting of suspicious acts or transactions. All staff dealing with customers or executing transactions shall be trained regularly, at least once per year, on current methods and typologies of money laundering and financing of terrorism. The relevant documents published or disseminated by the FIC and/or the CBAK shall be taken into consideration.

Although directors and senior managers may not be involved in the day-to-day procedures, it is important that they understand the statutory duties placed on them, their staff and the business itself. Therefore, they shall participate in training appropriate to their function. This training shall also cover possible sanctions arising from laws and regulations.

The documents on the structure of the training programs, their content and the names and signatures of the participants shall be kept in the files of the bank or financial institution for at least 5 years.

15. Implementation of Rule

15.1 Effective Date and Implementation Measures

The Governing Board of the Central Banking Authority of Kosovo adopted this Rule on April 4, 2007. Previous issuances of this Rule are hereby rescinded.

Banks and financial institutions shall implement the requirements of this Rule within six months of this Rule entering into force.

Banks and financial institutions shall submit an action plan (including timetable) to implement this Rule to the CBAK by July 15, 2007.

15.2 Application of Rule X to existing customers

For all customer relationships in existence at the date on which this Rule comes into effect, banks and financial institutions shall apply the customer due diligence measures as set out in Section 6 by April 30, 2007.

15.3 Administrative Directives and Instructions of the Financial Intelligence Centre

In the event that the Financial Intelligence Centre issues an Administrative Directive or Instruction that is inconsistent with any provision of this Rule, the FIC issuance will supersede that provision.

Michel Svetchine
Managing Director