Guidelines for the implementation of the Anti Money Laundering and Terrorist Financing Law with respect to credit institutions, credit unions and electronic money institutions

Zagreb, June 2015

CONTENTS

Pursuant to Article 88 of the Anti Money Laundering and Terrorist Financing Law (Official Gazette 87/2008 and 25/2012) and Article 43, paragraph (2), item (9) of the Act on the Croatian National Bank (Official Gazette 75/2008 and 54/2103), the Governor of the Croatian National Bank has issued Guidelines for the implementation of the Anti Money Laundering and Terrorist Financing Law with respect to credit institutions, credit unions and electronic money institutions.

1 Introductory provisions

1.1 Purpose and applicability of the Guidelines

For the purpose of a uniform application of the provisions of the Anti Money Laundering and Terrorist Financing Law (hereinafter: the Law) and pursuant to the regulations adopted on the basis thereof, the Croatian National Bank (hereinafter: the CNB), as the competent supervisory authority, hereby issues these Guidelines for the implementation of the Anti Money Laundering and Terrorist Financing Law with respect to credit institutions, credit unions and electronic money institutions (hereinafter: the Guidelines).

The Guidelines shall apply to the following obligated persons referred to in Article 4 of the Law (hereinafter: obligated persons), supervised by the CNB:

1. banks, Member States' bank branches, branches of third-country banks, and banks from Members States which are authorised for a direct provision of banking services in the Republic of Croatia;
2. savings banks;
3. housing savings banks;
4. credit unions; and
5. electronic money institutions, branches of Member States' electronic money institutions, branches of third-country electronic money institutions and electronic money institutions from Member States which are authorised for a direct provision of electronic money issuance services in the Republic of Croatia.

Being a part of the financial system which may be used for illegal purposes and through which money laundering and terrorist financing activities may be carried out, obligated persons are exposed to various kinds of risk (reputation[1], legal[2] and operational risks[3]) that can threaten their stability.

[1] Reputation risk is defined as the risk of a loss of trust in the integrity of an obligated person, caused by adverse public opinion on the obligated person's business practices and connections, regardless of whether there are any grounds for such a public opinion or not.

In order to reduce the exposure to the reputation, legal and operational risks, and particularly the risk of the financial system abuse by using various money laundering and terrorist financing methods and techniques, obligated persons should effectively apply the measures laid down in these Guidelines.

1.2 Money laundering

1.2.1 Money laundering definition

Money laundering means the undertaking of actions aimed at concealing the true source of money or other property suspected to have been obtained in an illegal manner in the country or abroad, including:

1. the conversion or any other transfer of money or other such property;
2. the concealment of the true nature, source, location, disposition, movement, ownership or rights with respect to money or other such property; and
3. the acquisition, possession or use of money or other such property.

1.2.2 Money laundering stages

The process of money laundering generally involves the following three stages:

1. Placement stage

Illicitly acquired funds are initially entered into the financial system. At this stage, the "dirty" money is most visible and easy to detect.

2. Layering stage

At this stage, the funds are entered into financial flows, where a number of complex transactions are used to disguise the origins or owners of illicitly acquired funds. The detection of the "dirty" money becomes more difficult.

3. Integration stage

At this stage, the "dirty" money is re-entered into the legal financial flows and included into other financial system assets of a country, which makes its detection almost impossible.

---

[2] Legal risk relates to the possibility that a legal action instituted against an obligated person, and contracts concluded or business decisions taken by that obligated person, which are found to be unenforceable, might adversely affect the obligated person's business or financial position.

[3] Operational risk is defined as the risk of loss resulting from inadequate or failed internal processes, people or systems, or external events, including a legal risk.

1.2.3 Money laundering methods

Due to technological progress, an increased number of sophisticated and complex methods are used to conceal the origins of illicitly acquired funds.

Of a large number of methods, only a few most commonly used ones are described, aimed at circumventing the money laundering detection and prevention system:

1. Structuring – the breaking of larger amounts of cash over a reporting limit into cash transactions of smaller amounts and their placement into the financial system. The smaller cash amounts are most commonly deposited by a rather large number of persons, in order to avoid detection, or evade the obligation to report on cash transactions above a certain amount and the customer identification obligation.
2. Multiple transactions – the same person carries out two or more transactions in one day, where the total amount of transactions in a day exceeds the prescribed limit for customer identification and identity verification, or notification of the Anti-Money Laundering Office (hereinafter: the Office).
3. Purchase/sale of foreign currency – illicitly acquired funds are used for the purchase of foreign currency which is then transferred to bank accounts held with off-shore financial centres.
4. Using nominal representatives – the most commonly used method at the placement stage. A person intending to enter dirty money into the financial system can try to conceal the origin of the illicit funds, by including a nominal representative, such as a family member, a friend or a business acquaintance enjoying the trust of the community.

The most common methods of laundering money acquired through some of the so-called predicate offences are the following:

1. the use of various forms of companies and foundations, particularly shell companies, established in countries with no strict regulations on the prevention of money laundering and identification of its true owners;

2. the use of the services of various legal and/or financial experts, particularly lawyers, who establish companies, open bank accounts, make cash transfers, buy assets and perform other tasks on behalf of their clients.

3. the use of domestic credit/financial institutions: enhanced due diligence is conducted only in the case of politically exposed foreign persons; for that reason, politically exposed persons use accounts in banks having their seat in a country of their residence, either at the layering stage or by returning the cash to a "domestic" bank after it has been "laundered" abroad;

4. the use of foreign/offshore jurisdictions, particularly the use of several foreign/offshore jurisdictions in a way that, for example, a bank account in one country

is owned by a company with a seat in another country, where the "owner" of that company has a seat in a third country, etc.; an increased number of foreign/offshore jurisdictions involved in the scheme, hinders the performance of legal actions for identifying the offence and its perpetrators by the criminal prosecution authorities in the country where the predicate offence has been committed;

5. the use of trustees – the use of family members, friends or close business associates, carrying out transactions in their own name, but for the account of a politically exposed person;

6. the use of cash – given its anonymous character, i.e. given no written record of its transfer, cash is attractive to money "launderers"; in the case of politically exposed persons, another advantage is the exemption of "diplomatic baggage" from customs control and its use for the transfer of cash across the border.

1.3 Terrorist financing

1.3.1 Terrorist financing definition

In the broadest sense, the term terrorism includes any use of violence for the purpose of achieving political goals. The term 'terrorist financing" means the provision or collection of, as well as an attempt to provide or collect legal or illegal funds by any means, directly or indirectly, with the intention to be used, or in the knowledge that they are to be used, in full or in part, for the commitment of a terrorism offence by a terrorist or by a terrorist organisation.

A terrorist financing risk is the risk that the financial system might be abused for terrorist financing purposes, or that a legal relationship, a transaction or a product might be directly or indirectly used for terrorist financing purposes.

In contrast to money laundering, which is always preceded by an unlawful act, terrorism may be financed from revenues generated through legal activities (of humanitarian organisations or various associations, or from donations, etc.). This circumstance greatly complicates the detection of terrorist financing, particularly as the amounts of transactions used for terrorist financing are often lower than the prescribed limit for reporting to the Office. The measures taken to prevent money laundering are insufficient to combat terrorist financing and have to be supplemented by special measures prescribed by competent international bodies.

1.3.2 Terrorist financing methods

The characteristics of terrorist financing differ from those of money laundering, so it is

difficult to assess the associated risk without a complex set of indicators of the methods and techniques that are used for terrorist financing.
As the funds used to finance terrorist activities may be derived either from criminal activities or from legal sources, the nature of the funding sources may vary according to the type of terrorist organisation. Where funds are derived from criminal activity, then the risk-based approach used to identify money laundering may also be appropriate for terrorist financing.

Where the funds used for financing terrorist activities are from legal sources, it is more difficult to establish that they are used for terrorist purposes. Moreover, preparations for terrorist activities can be public and overt, such as the purchase of materials and services (e.g. common chemical products, motor vehicles, etc.).

However, in the context of terrorist financing, the responsibility of obligated persons is not to identify a criminal offence, or intended terrorist financing, but to report suspicious activities. The Office and criminal prosecution authorities are responsible for a further investigation into the matter and for establishing a potential connection with terrorism.

Given the international character of terrorist financing and the lack of generally accepted typologies, i.e. methods and techniques used for terrorist financing, obligated persons are instructed to monitor and report to the Office transactions with countries identified by credible sources as countries that finance or support terrorist activities and in which identified terrorist organisations are known to operate.
The term “credible sources” refers to information provided by well-known bodies, that are generally regarded as reputable and that make such information publicly and widely available. In addition to the Financial Action Task Force and regional bodies operating in accordance with the FATF, such sources may include, but are not limited to, international bodies such as the International Monetary Fund, the World Bank and the EGMONT Group, as well as relevant national government bodies and non-governmental organisations. Information provided by these credible sources does not have the force of law or regulation and should not be viewed as an automatic determination that something poses a higher risk.

The method of monitoring and reporting such transactions is defined in Articles 42 and 43 of the Law.

As the prevention of money laundering and the prevention of terrorist financing have similar objectives, the basic features of both approaches produce synergistic effects. In both cases, efforts are made to conceal funds and financial transactions by hiding the sender and the recipient of the funds and concealing their mutual connection.

2 Legislative framework for the prevention of money laundering and terrorist financing

2.1 The Law and subordinate legislation

The legislative framework for the prevention of ML/TF in the Republic of Croatia comprises the Law, which is fully in line with the Directive 2005/60/EC of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Official Journal of the European Union L 309/15), the so-called Third Directive, and ordinances of the Ministry of Finance of the Republic of Croatia, enacted in accordance with the Law. In addition to the Law and the ordinances, currently in effect in the Republic of Croatia is Regulation (EC) No. 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds.

2.2 Criminalisation of money laundering and terrorist financing activities

Money laundering offences are criminalised under Article 265 of the Criminal Code (Official Gazette 125/2011, 144/2012, 56/2015 and 61/2015), which provides that whoever invests, takes over, converts, transfers or exchanges pecuniary gains acquired through a criminal offence with the intention of concealing their illicit origin shall be punished by imprisonment for six months to five years.

Terrorist financing is criminalized as a specific criminal offence under Article 98 which provides that whoever directly or indirectly, provides or raises funds with the intention of using them, or knowing that they are to be used, entirely or in part, for the perpetration of one or several criminal offences referred to in Article 97 (terrorism), Articles 99 (public incitement to terrorism) to 101 (training for terrorism), Article 137 (abduction), Article 216, paragraphs (1) to (3) (destruction or damage of public utility installations), Article 219 (abuse of radioactive substances), Article 223 (attack on an aircraft, a ship or an immovable device), Article 224 (endangering the safety of traffic by a dangerous act or means), Article 352 (murdering a person under international protection) and Article 355 (threatening a person under international protection) of that Code, or other criminal offences aimed at causing death or inflicting a serious bodily injury to a civilian or another person not actively participating in the armed conflict, provided that the purpose of such an act is to intimidate the population or coerce a state or an international organisation into doing or not doing something, shall be punished by imprisonment for one to ten years. The same punishment shall be inflicted on whoever provides or raises funds with the intention that they are used, or knowing that they are to be used, entirely or in part, by a terrorist or a terrorist association.

3 Measures to be carried out by obligated persons for the purpose of the ML/TF prevention

3.1 Organisation of an obligated person's AML/TF system

3.1.1 Appointment of an authorised person

Pursuant to Article 44 of the Law, an obligated person shall appoint an authorised person and one or several deputies to the authorised person. The authorised person and his/her deputies are persons authorised and responsible for carrying out the measures and actions aimed at preventing and detecting ML/TF within the obligated person. The authorised person's deputy replaces the authorised person during his/her absence in the performance of the activities prescribed by Article 46, paragraph (1) of the Law, and carries out other tasks under the Law, if so provided by an internal bylaw.

Pursuant to Article 45 of the Law, an obligated person shall ensure that the tasks of the authorised person or the authorised person's deputy can only be carried out by a person who meets the following requirements:

1. that the person is employed at a position within the obligated person's organisational scheme, which enables the person to carry out the tasks prescribed by the Law and regulations adopted on the basis thereof in a quick, efficient and timely manner, to be independent in his/her work and to communicate directly with the management board;

2. that the person is not undergoing criminal proceedings, i.e. the person was not convicted of a crime against the values protected by international law, safety of payment operations and arrangements, credibility of documents, against property and the official duty for a period of 5 years from the finality of the judgement by which the person had been convicted, excluding the time of serving a sentence;

3. that the person is adequately professionally trained to carry out tasks in the field of the ML/TF prevention and detection, and has the abilities and experience necessary to perform the functions of an authorised person; and

4. that the person is well familiarised with the nature of the obligated person's operation in the fields exposed to the ML/TF risk.

In addition, pursuant to Article 47 of the Law, an obligated person shall ensure the following conditions to the authorised person and the deputy:

1. unrestricted access to all data, information and documentation necessary for the ML/TF prevention and detection;
2. adequate authorisation for an efficient performance of the authorised person's tasks prescribed by the Law;

3. adequate personnel-related, material and other working conditions;
4. adequate premises and technical conditions, which will guarantee an appropriate level of protection for confidential data and information available to the authorised person and the deputy under the Law;
5. adequate IT- support enabling ongoing and safe monitoring of the activities in the field of the ML/TF prevention and detection;
6. regular professional training and development in the ML/TF prevention and detection;
7. replacement of the authorised person during his/her absence.

Equally, pursuant to Article 47, paragraph (3) of the Law, an obligated person shall ensure that the persons performing the function of the authorised person or the deputy carries out his/her work and tasks as an exclusive full-time work duty, where the volume of tasks in the field of the ML/TF prevention and detection is permanently increased due to a large number of employees, the nature or scope of the obligated person's operations or for other justified reasons.

In such cases, the obligated person shall enable the authorised person to carry out his/her tasks as an autonomous organisational unit, directly accountable to the management board and organisationally segregated from other organisational units of the obligated person.

Those obligated persons who, on the basis of the number of their employees, the nature or scope of their operations or for other justified reasons, assess that the volume of their tasks in the field of the ML/TF prevention and detection has not permanently increased, may include the authorised person into another organisational unit, or may organise the carrying out of the authorised person's tasks in a way other than as an exclusive full-time work duty.

In any case, however, obligated persons shall ensure that the authorised person is employed at a position within the obligated person's organisational scheme, which enables the person to carry out the tasks prescribed by the Law and regulations adopted on the basis thereof in a quick, efficient and timely manner, to be independent in his/her work and to communicate directly with the management board;

Pursuant to Article 46 of the Law, the authorised person and the deputy shall be authorised to carry out all the measures and actions prescribed in this Law, notably as follows:
1. taking care of the establishment, operation and development of the ML/TF prevention and detection system within the obligated person;

2. taking care of the regular and timely provision of data to the Office, in accordance with the Law and the regulations adopted on the basis thereof;

3. taking part in the preparation of operational procedures and amendments thereto,

and in the drafting of the obligated person's internal bylaws applicable to the ML/TF prevention and detection;

4. taking part in drawing up guidelines for conducting internal audits with respect to the ML/TF prevention and detection;

5. monitoring and coordinating the activities of the obligated person in the field of the ML/TF prevention and detection;

6. taking part in the establishment and development of IT support for carrying out the activities in the field of the ML/TF prevention and detection within the obligated person;

7. providing incentives and making suggestions to the management board for improvements in the ML/TF prevention and detection system;

8. taking part in the preparation of the professional training and development program for the obligated person's staff members in the field of the ML/TF prevention and detection.

An obligated person shall notify the Office of the appointment of an authorised person and the deputy immediately, but no later than 7 days from the appointment, or from a change of the authorised person's data. The notification submitted to the Office must contain the names and surnames of the authorized person and his/her deputy, telephone and telefax numbers and e-mail address.

3.1.2 Organisation of an AML/TF system

Pursuant to Article 46, paragraph (1), item (1) of the Law, an authorised person and the deputy shall, among other tasks, take care of the establishment, operation and development of the ML/TF prevention and detection system within the obligated person.

Moreover, Article 47, paragraph (2) of the Law prescribes that internal organisational units and the management board are obliged to ensure that the authorised person and the deputy have assistance and support during the performance of the tasks prescribed by the Law and regulations adopted on the basis thereof, and to inform them permanently of all the activities which were, or might be related to ML/TF. The manner of submitting the notifications and the course of cooperation between the authorised person and employees within other organisational units shall be prescribed in detail in the obligated person's internal bylaws.

In the process of establishing an AML/TF system, obligated persons should take account of the following:

1. the nature, scope and complexity of the obligated person's operations;
2. the diversity of the obligated person's operations, including geographical distribution;
3. the obligated person's customer, product and activity profiles;
4. the distribution channels used;
5. the volume and size of transactions;
6. the degree of risk associated with each area of the institution's operation;
7. the extent to which the institution is dealing with the customer directly or through intermediaries, third parties, correspondents, or using a non-face-to-face approach.

Based on the analysis of the above mentioned elements, obligated persons assess their own exposure to the ML/TF risk, in order to determine the level of complexity of the AML/TF system. The system complexity will be manifested in the manner in which an obligated person ensures the application of the provisions of the Law concerning: the authorised person and his/her deputy, internal bylaws, staff training and education, the obligation to conduct regular annual internal audits, data keeping, record keeping and the information system.

In order to ensure maximum efficiency of the established AML/TF system and the compliance of an obligated person's operations with the provisions of the Law, the system has to comply with the basic principles of the internal control system, and to ensure the following:

1. the application of an approach based on customer/product/transaction/country risks - an AML/TF system relying on the risk-based approach enables increased focus on an obligated person's customers/products/transactions that are perceived as more vulnerable to abuse in terms of ML/TF. Increased focus involves the application of more complex and intensive customer due diligence procedures, monitoring of customers' business relationships and implementation of other measures and activities provided by the Law, for the establishment or continuation of a particular relationship or for conducting transactions;
2. adequate professional training and education for all staff members involved in the AML/TF system - the continuous professional training and development ensures the compliance of an obligated person's operations with the provisions of the Law, enables staff members to be clearly familiarised with their powers, roles and responsibilities in the AML/TF system, and improves the obligated person's organisational culture;

3. adequate inclusion of the internal audit function (for some obligated persons, also external audit or external experts) - regular annual internal audits provide for a regular review of the risk assessment and management processes relating to ML/TF , and efficiency of the established AML/TF system;
4. adequate inclusion of the compliance function into the AML/TF system - the inclusion of the compliance function enables continuous monitoring of the compliance of the obligated person's operations with the provisions of the Law and regulations adopted on the basis thereof, the estimation of effects of the relevant regulation changes on the obligated person's operations, and verification of the compliance of new products or procedures with the relevant laws and regulations;
5. adequate senior management involvement in the AML/TF system - strong senior management leadership in AML/TF is an important aspect of an efficient AML/TF system. Senior management must promote compliance with the regulations and ensure consistent application of the obligated persons' internal policies, procedures and other internal bylaws by all staff members within their responsibility;
6. an adequate reporting system - apart from the direct accountability of the authorised person to the obligated person's management board, it is necessary to establish the appropriate reporting lines, i.e. the way of communication between the authorised person and control functions, between the authorised person and senior management, between the authorised person and responsible persons in individual organisational units, e.g. offices, etc. The reporting system should, in addition to regular reporting, provide for timely notification of all relevant lines of responsibility of identified deficiencies in the AML/TF system, corrective actions taken and the persons determined and time limits set for their correction;
7. an adequate information system - the obligated person's information system must provide for prompt, timely and full reporting to the Office on the persons and transactions prescribed by the Law. Furthermore, the information system should be permanently improved and upgraded, in order to enable the consistent an simpler application of the legal regulations, by both the authorised person and his/her deputy and all staff members involved in the operational implementation of the Law.

3.1.3 Internal bylaw

Pursuant to Article 48 of the Law, obligated persons shall adopt internal bylaws prescribing measures, actions and procedures for the ML/TF prevention and detection in accordance with the Law and regulations adopted on the basis thereof.

The measures, actions and procedures to be prescribed by each obligated person in an internal bylaw, which arise from the provisions of Articles 7, 8, 32, 34, 41, 47 and 48 of the Law are the following:

1. An analysis, i.e. assessment of risk to rate the risks of:
   a) an individual group or type of customers;
   b) a business relationship; and
   c) a product or transaction;
2. Procedures for the implementation of customer due diligence measures:
   a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a credible, reliable and independent source;
   b) identifying the beneficial owner of the customer and verifying the beneficial owner's identity;
   c) methods and procedures for obtaining information on the purpose and intended nature of the business relationship or transaction;
   d) methods and procedures for ongoing monitoring of the business relationship;
3. Procedures to determine whether a customer is a politically exposed person or not;
4. Policies and procedures for risks involved in a business relationship or transaction with customers who are not physically present:
5. A list of indicators for the detection of suspicious transactions and customers, in relation to which there are grounds for suspicion of ML/TF;
6. The manner of sending notifications and the course of cooperation between the authorised person and employees in other organisational units;
7. The responsibility of authorised persons in charge of the implementation of the Law in the case of the non-observance of the provisions of the Law and regulations adopted on the basis thereof, as well as the responsibility of all other obligated person's staff members taking part in the implementation of the Law and regulations adopted on the basis thereof.

In addition to the above mentioned, obligated persons should prescribe in their internal bylaws, according to their size and the nature and scope of their operations, the following measures, actions and procedures:

1. Monitoring procedures for customers or business relationships according to the established level of risk;
2. Enhanced customer due diligence procedures, i.e. procedures in the case:
   a) of establishing as correspondent relationship with a bank or other similar credit institution with a seat in a third country;
   b) of establishing a business relationship with a customer that is a politically exposed person; and
   c) when a customer is not physically present during the identification and identity verification procedures.
3. The manner of identifying and monitoring suspicious transactions and procedures applied by staff members upon detection of suspicious transactions;
4. The manner and dynamics of and responsibility of the authorised person and his/her deputy in reporting to the Office on the prescribed transactions and in the provision of other information and data to the Office;

5. The manner of and time limits for preparing a staff training and education program and the method of its implementation;
6. Record keeping: the manner of keeping data, retention periods, the content of records and data protection.

Staff members must be familiar with the provisions of internal bylaws and their impact on daily operations, in order to ensure consistent application of these provisions in practice and maximum efficiency of the staff members.

Obligated persons should ensure that the internal bylaws are easily accessible to the staff members e.g. at the obligated person's internal portal, and that the staff members are regularly informed of any amendments to these bylaws.

3.1.4 Producing a list of indicators

Pursuant to Article 41 of the Law, obligated persons are required to produce a list of indicators for the detection of suspicious transactions and customers in relation to which there are grounds for suspicion of ML/TF. When producing the list of indicators, obligated persons are required to take account of the specific features of their respective operations and characteristics of suspicious transactions referred to in Article 42, paragraph (7) of the Law. In the compilation of the list of indicators, obligated persons cooperate with the CNB.

When establishing the grounds for suspicion of ML/TF, obligated persons are required to use the list of indicators. Obligated persons must amend the list of indicators, which is an integral part of an obligated person's internal bylaw, and adapt it to the money laundering trends and typologies known to them, as well as to the circumstances stemming from the obligated person's operation.

3.1.5 Staff training and education

Pursuant to Article 49 of the Law, obligated persons are required to ensure regular training and education of all staff members involved in the tasks related to the ML/TF prevention and detection. Furthermore, the Law provides that the staff training and education should include the familiarisation with the provisions of the Law and regulations adopted on the basis thereof, with the obligated person's internal bylaws, and with international standards stemming from international AML/TF conventions, with guidelines and the list of suspicious transactions detection indicators, and with other tasks prescribed by the Law.

During the preparation of an annual staff training and education program, obligated persons should ensure that the program is appropriate to the type and scope of their operations and to the obligated persons' exposure to the ML/TF risk. In any case, the

annual staff training and education program must enable the staff members to better understand their obligations with respect to AML/TF and their roles in the established AML/TF system, and with respect to the exposure of their operations to the ML/TF risk.

Obligated persons should educate their staff members on most of these topics through internally organised workshops, and should establish an efficient reporting and education system at the internal web portal, in the form of brief information, written materials and on-line education programs. Moreover, obligated persons should, in accordance with their abilities, refer the staff members to seminars organised by other domestic and foreign institutions for the purpose of acquiring new knowledge and experience.

The annual staff training and education program must cover all the staff members involved in the tasks related to the ML/TF prevention and detection. It is particularly important that the program should cover new staff members before they start interacting with customers. Hence, the ML/TF prevention and detection training should be an integral part of initial training and guidance programs for new staff members.

Obligated persons are required to prepare the annual staff training and education programs in the field of the ML/TF prevention and detection for the next calendar year by the end of the current year. The programs should be documented and must show which staff members will take part in a particular training program and in which time period.

Pursuant to Article 46, paragraph (1), item (8) of the Law, both the authorised person and his/her deputy shall take part in the preparation of a program. Moreover, the annual staff training and education program should be included in the audit program and evaluated within the regular annual internal audit procedure.

3.1.6 Internal audit

Pursuant to Article 50 of the Law, obligated persons are required to ensure that a regular internal audit of the performance of AML/TF tasks is carried out at least once a year and to inform the Office accordingly at request. The purpose of the regular internal audit is to detect and prevent irregularities in the implementation of the Law and to improve the internal system for detecting suspicious transactions and persons.

The regular internal audit obligation for credit institutions and electronic money institutions should be discharged by the internal audit function. As the said institutions are required to adopt audit programs for each area of internal audit, including the audit of the AML/TF system, they should ensure that this program is consistent with the size and volume of a given institution's operation, its risk profile and exposure to the ML/TF

risk and that it is tailored to the specific characteristic of the ML/TF prevention system established within the institution.

The internal audit function is obliged to prepare a report on each completed audit, including the audit of the AML/TF system. Should the internal audit function, during the performance of internal audits, detect deficiencies, irregularities or illegalities in the AML/TF system, it shall impose measures and set deadlines for their correction. The internal audit function shall submit the report to the Audit Committee, a member of the Management Board responsible for the audited areas of operation, the authorised person and the responsible persons of the organisational units competent for the audited areas of operation.

Credit unions are not legally obliged to establish an internal audit function and should therefore entrust the conduct of the regular annual audit of the performance of the AML/TF tasks to an audit firm that will carry out the audit of the annual financial statements in accordance with the legislation governing accounting and auditing, or, where appropriate, to a person with the title of an auditor, obtained in accordance with the law governing auditing.

3.1.7 Data retention and records keeping

3.1.7.1 Data retention

Pursuant to Article 78 of the Law, obligated persons are required to retain the data collected in accordance with the Law and regulations adopted on the basis thereof and the pertaining documentation for a period of ten years after the execution of a transaction, termination of a business relationship or a customer's access to a safe deposit box.

Furthermore, obligated persons are required to retain data and the pertaining documentation on an authorised person and the authorised person’s deputy, the staff training and development and on the conduct of a compulsory internal audit for a period of four years after the appointment of an authorised person and the authorised person’s deputy, the delivery of the staff training and education or the completion of the internal audit.

Obligated persons should additionally regulate the stated time limits prescribed by the Law in their internal bylaws. Obligated persons should also regulate in their internal bylaws the manner, form and place of retaining the data collected pursuant to the Law, data protection measures and procedures for data handling after the expiry of the retention period.

3.1.7.2 Secrecy of collected data and procedures

Pursuant to Article 75 of the Law, obligated persons and their staff members may not disclose the following information to a customer or a third party:

1. that the Office was, or will be supplied with a piece of data, information or documentation on the customer or a transaction referred to in Article 42, Article 54, paragraphs (1) and (2) and Article 59 of the Law;
2. that the Office has temporarily suspended the execution of a suspicious transaction, or has given instructions to this effect to the obligated person pursuant to Article 60 of the Law;
3. that the Office requested ongoing monitoring of a customer's financial operations pursuant to Article 62 of the Law; and
4. that pre-investigatory proceeding have been initiated, or might be initiated against a customer or a third party due to suspicion of money laundering or terrorist financing.

The data submitted in accordance with Article 42 of the Law are labelled as classified data for which an adequate secrecy degree is determined in accordance with Article 9 of the Data Secrecy Act (OG 79/2007). The secrecy degree RESTRICTED is assigned to information the unauthorised disclosure of which would be damaging to the functioning of state authorities and performance of their tasks which are of security interest to the Republic of Croatia.

The exchange of information collected in accordance with the Law between credit and financial institutions belonging to the same group in the country and abroad may only include statistical data, e.g. the number of reported suspicious cash transactions, number of applications received by the Office, etc., but without indicating the identification data on persons or transactions.

3.1.7.3 Records keeping

Pursuant to Article 81, obligated persons are required to keep the following records:

1. records of customers, business relationships and transactions amounting to HRK 105,000.00 or more, regardless of whether the transaction is a single one or there are several, obviously interrelated transactions, amounting to a total of HRK 105,000.00 or more;
2. records of the data submitted to the Office on each cash transaction amounting to HRK 200,000.00 or more
3. records of transactions which the obligated person has not executed because the obligated person knew or suspected that the transactions were related to ML/TF, and which have been reported to the Office;

4. records of the supervisory bodies' inspections of classified data, with the indication of the name of the supervisory body, the name and surname of the authorised person who carried out the inspection and the date and time of the data inspection.

In addition, pursuant to Article 43 of the Law, obligated persons are required to analyse the background and purpose of complex and unusual transactions and to make a written record of the analysis results in order to make them available at the request of the Office and other supervisory bodies. Obligated persons should regulate in their internal bylaws the manner and form of keeping and accessing the records made in accordance with the Law.

3.1.8 Establishing an information system

Pursuant to Article 6, obligated persons are required to establish an information system adequate to their respective organisational schemes, in order to provide the Office with prompt, timely and complete information as to whether or not they maintain or have maintained a business relationship with a given natural or legal person, as well as to the nature of such a relationship.

Furthermore, pursuant to Article 47 of the Law, obligated persons are required to provide the authorised person and his/her deputy with adequate IT support to enable ongoing and safe monitoring of the activities in the field of the ML/TF prevention and detection;

In addition, pursuant to Article 46 of the Law, the authorised person and his/her deputy are authorised to take part in the establishment and development of IT support for carrying out the AML/TF activities.

In order to be able to provide the Office with prompt, timely and complete information as to whether or not they maintain, or have maintained a business relationship with a given natural or legal person, as well as to the nature of such a relationship, obligated persons should continuously improve their current information systems, so that they enable the staff to keep records of customers and to monitor the relationships with customers in a quick and efficient way, i.e. that the possibilities of updating, monitoring and searching customer data within the system are adequate for the processing and searching of high quantities of data in a short time. Consequently, obligated persons are encouraged to upgrade their information systems to include, e.g. differentiation between cash and cashless transactions, easier detection of suspicious transactions, monitoring of interrelated cash transactions, etc.

3.2 Risk assessment

Pursuant to Article 7 of the Law, obligated persons are required to carry out an analysis of the ML/TF risk and to use it for the assessment of the risks of a particular group or type of customers, business relationships, products or transactions with respect to a possible abuse related to money laundering and terrorist financing. Obligated persons are required to align the risk analysis and assessment, regulated by internal bylaws, with these Guidelines.

In addition to the risk-based approach, within which risk categories related to money laundering and terrorist financing are determined, these Guidelines also provide instructions for establishing policies and procedures aimed at reducing exposure to the money laundering and terrorist financing risks which may stem from new technologies enabling anonymity (electronic or Internet banking, electronic money, etc.).

The Guidelines also apply to all activities performed by obligated persons on the Internet, including all connected technologies enabling network access and open telecommunications networks, including direct telephone links, the World Wide Web and virtual private networks.

3.2.1 Risk-based approach[4]

The ML/TF risk is defined as the risk of abuse of the financial system by the customer for ML/TF and the risk that some business relationship, transaction or product may be used directly or indirectly for ML/TF.

In accordance with the Law, obligated persons independently assess the exposure of their customers or business relationships, transactions and products to the ML/TF risk. The categories, criteria and elements of risks defined in these Guidelines indicate potential ML/TF risks. The initial assessment of a customer made by an obligated person should be based on these risk categories and criteria, while individual risk elements may increase or decrease the initial assessment of the exposure.

The purpose of introducing the risk-based approach is to ensure that the AML/TF measures applied by obligated persons are proportionate to the identified risk. This approach provides for determining potential ML/TF risks and enables obligated persons to focus on those customers, business relationships, transactions or products that pose the highest potential risk.

[4]The FATF has published detailed guidelines on the risk-based approach in relation to various sectors: http://www.fatf-gafi.org/documents/riskbasedapproach/.

Obligated persons must be able to prove that the level of due diligence measures applied is appropriate with respect to the ML/TF risk.

3.2.2 The ML/TF risk assessment

3.2.2.1 Risk categories, criteria and variables

Risk categories
When analysing and assessing the ML/TF risks, obligated persons classify their customers, business relationships, transactions or products into the following categories:

1. **low risk;**
2. **moderate risk; and**
3. **high risk.**

Risk criteria
The most commonly used risk criteria are:

1. country or geographic risk;
2. customer risk; and
3. product/transaction/business relationship risk.

Risk variables
An obligated person's methodology based on risk analysis and assessment may take into account risk variables which are specific to a particular customer, business relationship, product or transaction and which may increase or decrease the risk. The risk variables include:

1. **The purpose of an account or a business relationship** — accounts opened to carry out common, low-value customer transactions may pose a lower risk than accounts opened to carry out large cash transactions by a previously unknown customer.
2. **The level of assets or the size of transactions** — unusually high levels of assets or unusually large transactions compared to what might reasonably be expected of customers with a similar profile may indicate that a customer, not otherwise seen as higher risk, should be treated as such.
3. **The level of regulation** or another oversight or governance regime to which a customer is subject — a legally regulated financial institution in a country with a satisfactory anti-money laundering regime poses less risk than a customer that is unregulated or subject only to minimal anti-money laundering regulation. Companies and their wholly owned subsidiaries that are publicly owned and traded on a recognised exchange generally pose a minimal money laundering risk. These companies usually have their seat in equivalent third countries with adequate, recognised regulatory schemes, and therefore pose a lower risk due to

the type of business they conduct and the wider governance regime to which they are subject.

4. **Duration of the business relationship** — long-standing business relationships involving frequent customer contacts may present less risk of money laundering.
5. **Familiarity with the client's country**— including knowledge of its laws, regulations and rules, as well as the structure and extent of regulatory oversight influences risk assessment.
6. **The use of intermediate corporate vehicles** or other structures that have no apparent commercial or other rationale or that unnecessarily increase the complexity of transactions, or otherwise result in a lack of transparency, without an acceptable explanation, increases the risk.
7. **Data on persons submitted to the Office by obligated persons in the past three years** — in relation to such a person or his/her transactions there were grounds for suspicion of money laundering or terrorist financing, which increases the risk.

Equivalent third countries are countries other than the Member States of the European Union or signatories of the Agreement on the European Economic Area, which meet the same standards in the field of money laundering and terrorist financing prevention as the EU Member States. A list of equivalent third countries shall be assembled by the Inter-institutional Working Group for Preventing Money Laundering and Terrorist Financing and shall be published by the Office.

3.2.2.2 Level of customer due diligence measures

The level of due diligence must be appropriate in relation to identified risk categories. Depending on the identified money laundering or terrorist financing risk categories, and following analysis and assessment of the risk of money laundering or terrorist financing, obligated persons determine the due diligence requirements which include:

1. a standard level of due diligence to be applied to all categories to which the customer due diligence measures referred to in Article 8, paragraph (1) of the Law apply;
2. a reduced standard level of due diligence for categories in recognized low risk scenarios, where simplified customer due diligence measures apply, as prescribed by an ordinance issued by the Minister of Finance in accordance with Article 7, paragraph (5) of the Law;
3. an increased standard level of due diligence for customers identified as high risk customers, in which case enhanced customer due diligence measures apply; and
4. exemption from conducting customer due diligence measures as prescribed by Article 14, paragraph (2) of the Law or by an ordinance issued by the Minister of Finance.

Pursuant to Article 30 of the Law, obligated persons are required to apply enhanced due

diligence measures in the following cases:

1. when establishing a correspondent relationship with a bank or other credit institution with a seat in a third country;
2. when establishing a business relationship with a customer that is a politically exposed person; and
3. when a customer is not physically present during the identification and identity verification procedures.

3.2.3 Low ML/TF risk

3.2.3.1 Customer Risk

A reduced standard level of due diligence can be applied to the customers referred to in Article 35, paragraph (1) of the Law, and to customers who meet the conditions determined by the Ordinance on the determination of conditions under which obligated persons identify customers as customers who pose a negligible risk in terms of money laundering or terrorist financing. A reduced standard level of due diligence or simplified customer due diligence measures are prescribed by Article 36 of the Law.

By way of exception, when establishing a correspondent relationship with a bank or another credit institution with a seat in a third country, obligated persons have to apply enhanced customer due diligence.

3.2.3.2 Product/transaction risk

A reduced standard level of due diligence may also be applied to the following products and transactions:

1. credit agreements, where credit accounts are used exclusively for loan settlement, and loan repayment is made from an account opened in the name of a customer with a supervised credit institution;
2. transactions involving de minimis amounts for particular types of transactions (e.g. small insurance premiums, children's savings up to HRK 1,000.00 per month, deposits and withdrawals of pensions, social benefits, etc.);
3. savings deposits in housing savings banks;
4. electronic payment of certain services (e.g. the payment of parking fees or public city transportation tickets), involving de minimis amounts (HR 1,125). By way of exception, if the transaction issuer is unknown, the verification of the issuer's identity can be omitted.

3.2.4 Moderate ML/TF risk

Obligated persons shall identify as medium risk category those customers, business relationships, products or transactions that, based on the risk analysis and assessment, cannot be identified as posing a high or a low risk. In such cases, the obligated persons will act in accordance with the provisions of the Law governing the area of standard customer due diligence.

3.2.5 High ML/TF risk

3.2.5.1 Customer risk

An increased level of standard due diligence is applied where the customers are:

1. politically exposed foreign persons;
2. persons who are not physically present at the identification and identity verification during the conduct of due diligence;
3. foreign legal persons who do not, or may not, conduct trading, manufacturing or other activities in the country of registration;
4. customers, the organisational structure or nature of the legal personality of which makes it difficult or impossible to identify the beneficial owner;
5. foreign legal persons carrying out the operations referred to in Article 3, item (21) of the Law, and having unknown or hidden owners and secret investors or managers;
6. customers whose beneficial owners are subject to sanctions imposed in the interest of international peace and security in accordance with the legal acts of the EU and resolutions of the UN Security Council;
7. cash intensive business entities including:
    (a) remittance houses, authorised exchange offices, money transfer agents and other companies offering money transfer services;
    (b) casinos, betting houses and other activities related to games of chance; and
    (c) companies that, while not normally cash intensive, use substantial amounts of cash for certain transactions;
8. charity and other non-profit organisations, especially those operating on a "cross-border" basis, or those seated in a high-risk geographic area, or some of their founders or members are natural or legal persons seated or domiciled in a higher-risk geographic area;
9. accountants, lawyers, or tax advisors and others, holding accounts with a particular financial institution, and acting on behalf of their clients;
10. customers conducting their business relationships or transactions in unusual circumstances, such as:
    (a) a considerable and unexplained geographic distance between the seat of the obligated person and the location of the customer;

(b) frequent and unexplained movements of accounts to different obligated persons;
(c) frequent and unexplained transfer of funds among obligated persons at different geographic locations;

11. persons in relation to which the Office has, in the past three years:
(a) requested from the obligated person to supply data due to suspicion of money laundering or terrorist financing;
(b) ordered the obligated person to suspend the execution of a suspicious transaction; or
(c) ordered the obligated person to monitor the customer's financial operations on an ongoing basis;

12. natural or legal person and other entities included in the list of persons subject to measures issued by the UN Security Council or by the EU — the relevant measures include financial sanctions requiring the freezing of the funds in the account and/or the prohibition of free disposal of assets, a military embargo on the arms trade with the entity, etc.;

13. natural or legal persons having their residence or seat in entities which are not subject to international law, i.e., which are not internationally recognised (due to their facilitating the fictitious registration of legal persons, issuance of fictitious identification documents, etc.);

3.2.5.2 Transaction/business relationship risk

Transactions or business relationships posing a high risk include:

1. transactions intended for persons or entities that have been subjected to measures issued by the UN Security Council or EU;
2. transactions a customer might carry out in the name and for the account of a person or an entity that has been subjected to measures issued by the UN Security Council or EU; and
3. business relationships that might be established to the benefit of a person or an entity included in the list of persons or entities that have been subjected to measures issued by the UN Security Council or EU.

3.2.5.3 Risk of a business relationship with another credit institution

The establishment of a correspondent relationship with a bank or another credit institution with a seat in a third country, other than the equivalent third country referred to in item 3.2.2.1 of these Guidelines poses a high risk.

Pursuant to Article 31 of the Law, when establishing a correspondent relationship with a bank or another credit institution with a seat in a third country, obligated persons are required to carry out the measures referred to in Article 8, paragraph (1) of the Law

within the framework of enhanced customer due diligence and additionally collect the following data, information and documentation:

1. the date of issuance and validity period of authorisation to provide banking services, and the name and seat of a competent third-country authority that issued the authorisation;
2. a description of the implementation of internal procedures relating to money laundering and terrorist financing prevention and detection, particularly the procedures of customer identity verification, beneficial hidden identification, reporting to the competent bodies on suspicious transactions and customers, record keeping, internal audit and other procedures that the bank or other credit institution adopted in relation to money laundering and terrorist financing prevention and detection;
3. a description of systemic arrangements in the field of the ML/TF prevention and detection in effect in a third country in which the bank or other credit institution has its seat or in which it has been registered;
4. a written statement confirming that the bank or other credit institution does not operate as a shell bank;
5. a written statement confirming that the bank or other credit institution neither has business relationships with shell banks established, nor does it establish business relationships or conduct transactions with shell banks;
6. a written statement confirming that the bank or other credit institution falls under the scope of legal supervision in the country of its seat or registration, and that it is required to apply legal and other regulations in the field of the ML/TF prevention and detection in accordance with that country's effective laws.

In the context of enhanced due diligence, when establishing a correspondent relationship with a bank or another credit institution having its seat in a third country, obligated persons should provide the following additional documentation:

1. a written statement that the bank or other credit institution has verified the identity of a customer and that it conducts ongoing due diligence of customers who have direct access to payable-through accounts, and
2. a written statement that the bank or other credit institution can provide, upon request, relevant data obtained on the basis of due diligence of customers having direct access to payable-through accounts.

The obligated person's staff member who establishes a correspondent relationship with a bank or another credit institution with a seat a third country and who performs enhanced customer due diligence is required to obtain a written approval of the superior responsible person prior to establishing the business relationship.

Obligated persons are not allowed to establish or continue a correspondent relationship with a bank which operates or might operate as a shell bank (the description and features of a shell bank are available at:

http://www.bis.org/publ/bcbs95.pdf). Obligated persons are not allowed to establish or continue a correspondent relationship with a bank or with another similar credit institution known to enter into agreements on opening and keeping accounts with shell banks. In addition, Article 31, paragraph (4), items (1), (2) and (3) of the Law shall apply.

3.2.5.4 Foreign politically exposed persons

Pursuant to Article 32 of the Law, obligated persons are required to apply an adequate procedure to determine whether or not a customer is a foreign politically exposed person. The procedure is defined by an internal bylaw, taking into account these Guidelines.

When determining whether or not a person is a politically exposed person, institutions may proceed in one of the following ways:

1. request information directly from a customer by means of a written form;
2. collect information from public sources (information that is publicly available through the media - press, TV or Internet);
3. collect information by accessing commercial data bases which include lists of politically exposed persons.

3.2.5.5 Country risk

Customers that pose a high risk may be customers having permanent residence or a seat in the following countries:

1. countries subject to sanctions, embargoes or similar measures issued by the United Nations;
2. countries identified by credible sources as:
   (a) lacking appropriate laws, regulations and other measures for the prevention of money laundering and terrorist financing;
   (b) providing funding or support for terrorist activities and having designated terrorist organisations which operate within them;
   (c) having significant levels of corruption, or other criminal activity;
3. countries which are not Member States of the European Union or signatories to the Treaty Establishing the European Economic Area, and do not qualify as equivalent third countries;
4. countries which, according to the FATF data, belong to non-cooperative countries or territories or, in the case of an Offshore Financial Centre from the list supplied by the Office.

As regards information on high-risk countries or non-cooperative countries or territories that do not meet key international standards for the ML/TF prevention, you are advised to visit the official web sites of the following international bodies: MONEYVAL[5], **www.coe.int/t/dghl/monitoring/moneyval**, and FATF[6], **www.fatf-gafi.org**.

[5] MONEYVAL is a regional body within the Council of Europe, established in 1997, which consists of the members of the Council (including the RC); its objective is to assess the status of the fight against money laundering and terrorist financing in the Council of Europe member countries. The assessment is based on the FATF and EU standards, as well as conventions of the Council of Europe and UN.

[6] FATF (Financial Action Task Force) is an international body, established in 1989, which has developed 40 recommendations outlining measures for the prevention of money laundering and terrorist financing, recognised as a standard for fighting money laundering and terrorist financing,

3.2.5.6 Product risk

The increased level of standard verification should be applied to the following products or services:

1. services identified by competent authorities or other credible sources as potentially posing an enhanced risk, for example, establishing correspondent relationships with credit institutions having their seats in third countries;
2. services involving banknote and precious metal trading and delivery;
3. services that provide more anonymity or that can be readily provided across international borders, such as online banking, stored value cards, international wire transfers, the services of private investment companies and trusts, non-government organisations, etc.

3.2.5.7 Enhanced customer due diligence measures

Articles 31, 32 and 33 of the Law prescribe enhanced customer due diligence that obligated persons are required to perform when establishing correspondent relationships with third-country credit institutions, or business relationships with politically exposed persons, as well as in the cases of customer absence.

With respect to other customers, business relationships and transactions identified as posing a high risk, obligated persons should, within the framework of increased level of standard verification, implement appropriate measures and controls aimed at reducing the exposure to identified ML risks. These measures and controls may include:

1. the monitoring of all areas of customers' operation, their business relationships, products and high risk transactions;
2. an increased level of determination and verification of customer identity;
3. imposing stricter requirements for approvals to open accounts or establish business relationships;
4. closer transaction monitoring; and
5. increased levels of ongoing controls and frequency of business relationship reviews.

The same measures and controls may address more than one of the risk criteria identified, and obligated persons are not necessarily expected to introduce specific controls with respect to each of the risk criteria.

3.2.6 New technologies providing for anonymity

Pursuant to Article 34 of the Law, obligated persons are required to pay special attention to any ML/TF risk which may stem from new technologies enabling anonymity and to put in place policies and take measures aimed at preventing the use of such new technologies for ML/TF purposes.

Obligated persons must put in place policies and procedures for the risk involved in business relationships or transactions with customers who are not physically present, and apply them when establishing a business relationship with a customer, and during the performance of the customer due diligence, while taking into account the provisions of Article 33 of the Law, governing the procedures to be followed by an obligated person when establishing a business relationship without the presence of the customer.

In the process of defining the said policies and procedures for the risk involved in business relationships or transactions with customers who are not physically present, or in the process of defining policies and applying measures for the prevention of the use of new technologies for ML/TF purposes, obligated persons are recommended to apply the obligations, principles and rights governed by the Credit Institutions Act (Official Gazette 159/2013 and 19/2015) and the bylaws pertaining thereto, notably the Decision on Adequate Information System Management (Official Gazette 37/2010), the Guidelines on the Security of Internet Payments released by the European Banking Authority (EBA), which will become mandatory as of 1 August 2015, and the Guidelines for Information System Management Aimed at Reducing Operational Risk.

3.3 Customer due diligence measures

Pursuant to Article 8 of the Law, obligated persons are required to carry out the following customer due diligence measures:

1. identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a credible, reliable and independent source;
2. identifying the beneficial owner of the customer and verifying the beneficial owner's identity;
3. collecting data on the purpose and intended nature of a business relationship or transaction and other data in accordance with the Law; and
4. ongoing monitoring of the business relationship, including close scrutiny of transactions carried out during that relationship, in order to ensure that these transactions are consistent with the obligated person's knowledge of the customer, the type of his/her business and risk, including, where necessary, information on the source of funds; the documents and data available to the obligated person must be up-to-date.

Obligated persons which are unable to carry out the customer due diligence measures referred to in Article 8, paragraph (1), items (1), (2) and (3) of the Law, may not establish a business relationship or carry out a transaction, or must terminate an existing business relationship and send a notification thereof to the Office, accompanied by all previously collected data on the customer or transaction, in accordance with Article 42 of the Law.

Obligated persons which are unable to carry out the measure of updating the collected data on a customer with which they have already established a business relationship are not required to terminate such a business relationship. Obligated persons should, in line with their own risk analysis referred to in Article 7, paragraph (2) of the Law, re-evaluate the risk stemming from such a business relationship with a customer and take measures they deem necessary to mitigate the risks they are exposed to based on this business relationship until the measure of updating the data is carried out.

Pursuant to Article 13, paragraph (1) of the Law, obligated persons are required to terminate a business relationship with a customer when there are doubts about the credibility and veracity of the previously obtained customer or customer beneficial owner information and in all instances when there are reasons for suspicion of money laundering or terrorist financing in relation to a transaction or customer as referred to in Article 9, paragraph (1), items (3) and (4) of the Law and when they were unable to obtain the data required under Article 16, paragraph (1) of the Law within the customer due diligence.

3.3.1 Obligation to identify a customer and verify the customer's identity; exemptions

Pursuant to Article 9 of the Law, obligated persons must carry out customer due diligence in the following cases:

1. when establishing a business relationship with a customer; a business relationship is any business or other contractual relationship established or concluded by a customer with an obligated person, which is of a relatively long duration, which enables ongoing monitoring;
2. when carrying out a transaction amounting to HRK 105,000.00 or more, whether the transaction is a single one or it includes several interrelated transactions totalling HRK 105,000.00 or more. In contrast to a business relationship, in the case of a transaction the emphasis is on a one-off nature of the activity.
3. when there are doubts about the credibility and veracity of the previously obtained information on a customer or the customer's beneficial owner;
4. in all instances when there are grounds for suspicion of ML/TF in relation to a transaction or a customer, regardless of the transaction value.

Exemptions from the obligation to carry out due diligence measures for certain products

Electronic money institutions, electronic money institutions from another Member State and branches of third-country electronic money institutions may be exempted from the obligation to carry out customer due diligence measures in the following cases:

1. when issuing electronic money, if a single amount of a payment executed for the issuance of such money, on an electronic data carrier which may not be recharged, does not exceed the kuna equivalent of EUR 150.00;

2. when issuing electronic money and dealing with electronic money, if the total amount of executed payments, stored on an electronic data carrier which may be recharged, does not exceed the kuna equivalent of EUR 2,500.00 during a calendar year, except in the cases where the electronic money holder cashes the kuna equivalent of EUR 1,000.00 or more during the same calendar year.

Obligated persons may be exempted from the obligation to carry out the customer due diligence measures in the case of other products or transactions associated with them, which pose negligible ML/TF risks, provided they meet the conditions prescribed by an ordinance of the Minister of Finance.

By way of exception, obligated persons may not be exempted from the obligation to carry out customer due diligence measures when there are grounds for suspicion of ML/TF with respect to a customer, product or transaction.

Bearing in mind the activity of electronic money institutions - mobile network operators which, in addition to their primary activity, provide the services of executing payment transactions where the consent of the payer to execute a payment transaction is given by means of a telecommunication, digital or IT device and the payment is made to a telecommunication, a network or an IT system operator, acting exclusively as an intermediary between the payment service user and the supplier of goods and services, electronic money means only that part of the stored monetary value which has been used for the payment of certain goods and services.

The amounts paid by prepaid users to their accounts for the purpose of recharging them where these accounts are used for telecommunication services provided by a mobile network operator, are not considered as electronic money. The measures and actions against ML/TF are only applied in the part relating to payment services connected with electronic money.

3.3.2 Identification of the beneficial owner

Obligated persons are required to identify a customer's beneficial owner in accordance with Article 23 of the Law.

3.3.2.1 Identification of the beneficial owners of associations, endowments, foundations, political parties and religious communities

1. Where the customer is a non-profit organisation, such as an association, attention should be focused on activities through which the statutory goals are achieved, reasonable measures should be taken to identify the founder, and the identity of one and/or more persons controlling or managing the customer's activities, including the members of the governing and representative bodies, should be established.

These data are obtained from publicly available registers (a register of associations) or directly from the non-profit organisations concerned. Given that associations do not have capital divided into shares or stakes, the customer is not required to provide data on the natural person directly or indirectly holding more than 25% of shares, stakes or votes in the legal person.

2. Where the customer is a non-profit organisation which administers and distributes monies, such as an endowment or a foundation, or where it conducts legal transactions, such as trust dealings, the beneficial owner is a legal person holding 25% or more of the

property rights of a particular legal transaction, if future beneficial owners have already been identified.

Where future beneficial owners have not yet been identified, the beneficial owner shall be the person in whose main interest the legal transaction is conducted, i.e. in whose main interest the business is done, or in whose main interest the legal person has been established. A natural person who controls 25% or more of the property rights of a particular legal transaction is considered to be the beneficial owner.

The data necessary to identify the beneficial owner are obtained directly from the customer or from publicly available registers. Obligated persons obtain data from an endowment or foundation administrator, or from a trustee who manages certain property, relating to one or more natural and/or legal persons who have established the endowment or the foundation, or relating to persons on whose behalf the trustee decides on the property management. The registers (endowment book, foundation book, etc.) are public registers offering free access to every interested party that can request excerpts from such registers or copies of documents from a file (articles of association, a statute, a decision approving the establishment of an endowment or other documents on the basis of which an entry in the book or a change in the data has been made.

3. Political parties, trade unions and religious communities do not have beneficial owners.

4. Where the customer is an embassy, obligated persons conduct the simplified customer due diligence referred to in Article 35 of the Law, which excludes the identification of the beneficial owner.

3.3.2.2 A natural person exercising control over a legal person's management board without ownership of shares/stakes

Pursuant to Article 23, item (1), second indent of the Law, in the case of legal persons, branches, representative offices and other entities subject to domestic and foreign law and equated to a legal person, the beneficial owner shall be a natural person who otherwise exercises control over the legal person.

This provision applies, for example, to limited liability companies, whose articles of incorporation provide that the company's management board is appointed by an individual company member. According to the Companies Act, members of a limited liability company's management board are appointed by the company's assembly, but, subject to the articles of incorporation, this right may be transferred to somebody else, e.g. the supervisory board, one of the company's bodies or even a company member. Hence, a natural person who is a company member determined by the articles of incorporation as a person to appoint the members of the management board, can be

considered as the beneficial owner in terms of Article 23, item (1), second indent of the Law.

3.3.3 Identification and identity verification of a customer who is not physically present

Pursuant to Article 33 of the Law, if the customer is not physically present during the identification and identity verification, the obligated person shall be required to apply the following enhanced customer due diligence measures:

1. collect additional documents, data or information on the basis of which the customer's identity is to be verified;
2. additionally verify the submitted documents or additionally certify them by the foreign credit or financial institution referred to in Article 3, items (12) and (13) of the Law;
3. apply a measure whereby the first payment within the business activity is made through an account opened in the customer's name with another credit institution.

The additional documents, data or information on the basis of which the customer's identity is verified may include the following:

1. for residents, proof of permanent residence obtained from the competent authority that keeps civil status records, or certificate of permanent residence issued by the competent Police Department; for non residents, proof obtained from, e.g. a credit reference agency;
2. personal references (e.g. from an existing obligated person's customer);
3. previous bank references and bank contacts with respect to the customer;
4. data on the source of funds and assets which are or will be the subject of the business relationship;
5. a certificate of employment or of a public office held by the person.

For natural persons, obligated persons may additionally verify the submitted documents in at least one of the following ways:

1. by verifying the date of birth on the basis of an official document (e.g. a birth certificate, a passport, an ID card or social security records);
2. by verifying the permanent address (e.g. through utility bills, tax apportionment, bank statements or letters from public authorities);
3. by contacting the client by telephone, letter or e-mail for the purpose of verifying the supplied information after the account has been opened (e.g. a disconnected telephone line, a returned letter or an inaccurate e-mail address should indicate a need for further checks); or
4. by checking the validity of official documentation by means of a certificate issued by an authorised person (e.g. an embassy officer or a public notary).

For legal persons, obligated persons may additionally verify the submitted documents in at least one of the following ways:

1. by examining the copies of the latest business report and financial statements (audited, if available);
2. through an examination carried out by the Business Information Centre or on the basis of a statement given by a reputable and well-known attorney or an accounting company that verifies the submitted documents;
3. by examining the company or carrying out some other type of review in order to verify that the company has not ceased operating, or been removed from the register or liquidated, or that it is not in the process of terminating its operation, removal from the register or liquidation;
4. by an independent verification of information, e.g. through an access to public and private data bases;
5. by obtaining prior references of the obligated person; and
6. by contacting the company via telephone, mail or e-mail.

In some jurisdictions, there may be other equivalent documents to provide satisfactory proof of a customer's identity.

3.3.4. Data on the payer in the case of electronic funds transfer

The main determinants of electronic funds transfer, i.e. of the obligation to collect data on the payer and the procedure to be followed by payment service providers are specified in Article 15 of the Law.

The rules on information on the payer accompanying transfers of funds laid down for the purposes of prevention, investigation and detection of money laundering and terrorist financing are regulated by Regulation (EC) No. 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds.

3.3.5 Entrusting a third party with the conduct of customer due diligence

When establishing a business relationship with a customer, obligated persons may, under the conditions laid down by the Law and subordinate legislation, entrust a third party with the conduct of the identification and identity verification procedures.

Obligated persons must check upfront whether the third party they are about to entrust with the conduct of customer due diligence meets all the conditions prescribed by the Law.

The customer due diligence conducted for an obligated person by a third party may not be accepted if the third party conducted the identification and identity verification

procedures without the presence of the customer.

3.4 Monitoring a customer's business activities and notifying the Office

3.4.1 Business relationship monitoring measures

Obligated persons must closely monitor transactions carried out during the business relationship, in order to ensure that the transactions are consistent with the obligated person's knowledge of the customer, type of business, source of funds and the purpose and intended nature of the business relationship or a transaction. They are required to ensure that the volume and frequency of the business relationship monitoring measures are in line with the ML/TF risk to which they are exposed in running a business or dealing with a customer, pursuant to Article 7 of the Law.

Obligated persons are required to conduct a repeated annual due diligence of a foreign legal person, regularly once a year, but no later than after the expiry of one year since the last customer due diligence has been conducted.

The annual customer due diligence is also obligatory for a customer which is a legal person with a seat in the RC, conducting transactions in the amount of HRK 105,000.00 or more, and which is 25% or more owned by:
1. a foreign legal person which does not or may not engage in trading, manufacturing or other activities in the country of registration; or
2. a fiduciary or another similar company subject to foreign law, having unknown or hidden owners and secret investors or managers;

3.4.2 Notifying transactions to the Office

3.4.2.1 Obligation to notify the Office of cash transactions and notification deadlines

Obligated persons are required to notify the Office immediately of each cash transaction in the amount of HRK 200,000 or more, but no later than three days from the date of execution of such a transaction. The cash transaction notification form comprises the data prescribed by the Ordinance on the obligation to report cash transactions in the amount of HRK 200,000.00 or more to the Anti-Money Laundering Office, and on conditions under which obligated persons are not required to report cash transactions of certain customers to the Anti-Money Laundering Office.

3.4.2.2 Obligation to notify the Office of suspicious transactions and persons and notification deadlines

Obligated persons are required to notify the Office immediately of a suspicious transaction prior to its execution, and to indicate, among other things, the grounds for suspicion of ML/TF. By way of exception, where an obligated person has been unable to notify the Office in the prescribed manner of a suspicious transaction prior to its execution, due to the nature of the transaction, or the fact that the transaction had not been executed, or for other justified reasons, the obligated person is required to notify the Office subsequently, but no later than the next business day. The suspicious transaction report must be accompanied by documents to substantiate the reasons for not acting in the prescribed manner.
The Office should be notified of suspicious transactions prior to their execution by telephone, fax or in another adequate manner, and after their execution in the manner prescribed by the Ordinance on the notification of the Anti-Money Laundering Office of suspicious transactions and persons.

Obligated persons are required to refrain from executing transactions which they know or suspect to be related to ML/TF. Obligated persons are required to notify the Office, immediately and in the prescribed manner, of such transactions prior to their execution, to explain the grounds for suspicion of ML/TF, which clearly indicate that a transaction or person is suspicious, and to specify indicators on the basis of which such an assessment has been made.

When establishing the grounds for suspicion of ML/TF, obligated persons are required to use the list of indicators for the detection of suspicious transactions and persons. The assessment that a transaction or person is suspicious is based on the criteria specified in the list of indicators for the detection of suspicious transactions and persons. Obligated persons are required to amend the list of indicators and adapt it to the money

laundering trends and typologies known to them, as well as to the circumstances stemming from the obligated person's operation.

Where a transaction or person complies with one of the indicators, this does not necessarily mean that the transaction or person is suspicious. However, it points to a need for additional analysis prescribed in Article 43 of the Law. A broader view should be taken, being aware that obligated persons best know their clients and ensuring that the measure of ongoing monitoring of the business relationship is carried out, which includes a close scrutiny of transactions executed during that business relationship in order that these transactions are consistent with the obligated person's knowledge of the purpose and intended use of the transaction, the knowledge of the customer and of the type of business relationship and risk, including the source of funds. Should the obligated person assess, based on the analysis made, that there are grounds for suspicion that a transaction or person is related to money laundering, the obligated person is required to notify the Office in a prescribed manner of such a transaction prior to its execution.

3.4.2.3 Complex and unusual transactions

Obligated persons must pay special attention to complex and unusually large transactions, as well as to each form of transaction having no apparent economic or visible lawful purpose, even if grounds for suspicion of ML/TF with respect to such a transaction have not yet been established.

In addition, obligated persons must analyse the background and purpose of such transactions and make a written record of the analysis results, in order to make them available at the request of the Office or another supervisory body. The purpose of the report on the analysis results is to explain the reasons for not reporting a particular transaction as suspicious.

An analysis of complex and unusual transactions should cover the data on:

1. the intended nature and purpose of a business relationship;
2. the customer's activities;
3. funds kept on transaction accounts;
4. the purpose and intended use of a transaction;
5. cash transaction inflow and outflow;
6. transactions with countries from enhanced-risk geographic areas;
7. persons authorised to use the accounts;
8. frequency of transactions involving a certain legal or natural person as the transaction issuer;
9. the source of funds;
10. information obtained from the media; and
11. information obtained from publicly accessible databases, etc.

Should the analysis demonstrate that there are grounds for suspicion of ML/TF, the Office should be notified accordingly. The report on a suspicious transaction or person should comprise all data obtained during the analysis, as well as the data prescribed by Article 42 of the Law.

4 AML/TF measures in business units and companies in majority ownership, having their seat in a third country

Pursuant to Article 5 of the Law, obligated persons are required to ensure that the ML/TF prevention and detection measures are applied to the same extent in their business units and in companies in which they have a majority holding or a majority of the voting rights, and which have their seat in a third country, unless this is expressly contrary to the third country's legislation.

For this purpose, business units and companies in which the obligated person has a majority holding or a majority of voting rights should be regularly informed of the obligated person's internal procedures relating to the ML/TF prevention and detection, particularly as concerns customer due diligence, data supply, record keeping, internal controls, etc.

Where the legislation of a third country does not permit the application of the ML/TF measures to the extent prescribed by the Law, the obligated person is required to notify the Office thereof and to introduce the appropriate measures for eliminating the ML/TF risk.

5 Final provisions

On the date of adoption of these Guidelines, the Guidelines for the analysis and assessment of money laundering and terrorist financing risks for credit institutions and credit unions of 18 June 2012 No: 138-020/06-12/ŽR, shall cease to have effect.

Dec. No:

Zagreb,

CROATIAN NATIONAL BANK

GOVERNOR

Boris Vujčić