

Pursuant to Article 88 of the Anti Money Laundering and Terrorist Financing Law (Official Gazette 87/2008) and Article 43, paragraph 2, item 9 of the Act on the Croatian National Bank (Official Gazette 75/2008), and in connection with Article 29 of the Act on the Croatian National Bank and Article 199, paragraph 1 of the Credit Institutions Act (Official Gazette 117/2008), the Governor of the Croatian National Bank has issued the following

GUIDELINES
for the analysis and assessment of money laundering and terrorist
financing risks
for credit institutions and credit unions

Introductory Provisions

In accordance with the provisions of Article 85 of the Anti Money Laundering and Terrorist Financing Law (Official Gazette 87/2008), (hereinafter the Law), the Croatian National Bank is responsible for the supervision of the implementation of the Law by credit institutions, credit unions and electronic money institutions (hereinafter the institutions).

In accordance with the provisions of Article 7 of the Law, the institutions are obligated to make a risk analysis of money laundering and terrorist financing and apply it to assess risks of individual groups or types of customers, business relationships, products or transactions in respect of possible abuse relative to money laundering and terrorist financing. The institutions are obligated to undertake to align risk analysis and assessment, determined by an internal bylaw, with these guidelines.

In addition to a risk-based approach to assessment within which risk categories related to money laundering and terrorist financing are determined, these guidelines also provide instructions as regards putting in place policies and procedures aimed at diminishing exposure to the risk of money laundering and terrorist financing which may stem from new technologies enabling anonymity (electronic or Internet banking, electronic money, etc.).

The guidelines shall also apply to all activities performed by the institutions on the Internet, including all connected technologies enabling network access and open telecommunications networks which include direct telephone links, the public World Wide Web and virtual private networks.

1. Risk Assessment and the Internal Controls System

In order for the institutions to have effective risk-based approaches, the risk-based process must be imbedded within the internal controls of the institutions. Strong senior management leadership and engagement in anti-money laundering is an important aspect of the application of the risk-based approach. Senior management must create a culture of compliance, ensuring that staff adheres to the institution's policies, procedures and processes designed to limit and control risks.

In addition to other compliance internal controls, the nature and extent of anti-money laundering and counter-terrorist financing controls will depend upon a number of factors, including:

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

The internal controls should:

1. provide increased focus on an institution's operations (products, services, customers and geographic locations) that are more vulnerable to abuse in terms of money laundering and terrorist financing;
2. provide for regular review of the risk assessment and management processes, taking into account the environment which the institution operates and its activity in the market place;
3. provide for appointment of an individual or individuals at management level responsible for monitoring compliance with anti-money laundering and counter-terrorist financing regulations;
4. provide for a compliance function and a review programme relating to anti-money laundering and counter-terrorist financing;
5. ensure that adequate controls are in place before new products are offered;
6. inform senior management of compliance initiatives, identified compliance deficiencies, corrective action taken and suspicious activity reports filed;
7. provide for programme continuity despite changes in management or employee composition or structure;
8. focus on meeting all regulatory record keeping and reporting requirements, recommendations for compliance as regards anti-money laundering and counter-terrorist financing and provide for timely updates in response to changes in regulations;

9. enable the implementation of risk-based customer due diligence policies, procedures and processes;
10. provide for adequate controls for higher risk customers, transactions and products, as necessary, such as transaction limits or management approvals;
11. enable the timely identification of reportable transactions and ensure accurate filing of required reports;
12. provide for adequate supervision of employees that handle currency transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity that forms part of the institution's anti-money laundering and counter-terrorist financing programme;
13. incorporate compliance with anti-money laundering and counter-terrorist financing regulations into job descriptions and performance evaluations of appropriate personnel;
14. provide for appropriate training to be given to all relevant staff.

Senior management will need to have a means of independently validating the development and operation of the risk assessment and management processes and related internal controls, and obtaining appropriate comfort that the adopted risk-based methodology reflects the risk profile of the institution. This independent testing and reporting should be conducted by, for example, the internal audit department, external auditors, specialist consultants or other qualified parties who are not involved in the implementation or operation of the institution's programme for compliance with anti-money laundering and counter-terrorist financing regulations. The testing should be risk-based (focusing attention on higher-risk customers, products and services); should evaluate the adequacy of the institution's overall programme of anti-money laundering and counter-terrorist financing; and the quality of risk management for the institution's operations, departments and subsidiaries, include comprehensive procedures and testing, and cover all activities;

2. Risk-based Approach¹

The risk of money laundering or terrorist financing is defined as the risk of abuse of the financial system by the customer for money laundering or terrorist financing and the risk that some business relation, transaction or product may be used directly or indirectly for money laundering and terrorist financing.

In accordance with the Law, the institutions are responsible for assessing their exposure to the risk of money laundering and terrorist financing. The categories, criteria and elements of risks defined in these Guidelines point to potential risks of money laundering and terrorist financing. The initial assessment of the institutions should be based on risk categories and criteria outlined in these Guidelines, while individual risk

¹ The risk-based approach is dealt with in the FATF document: Guidance on the Risk-based Approach to Combating Money Laundering and Terrorist Financing. <http://www.fatf-gafi.org/dataoecd/43/46/3896057.pdf>

elements may increase or decrease the initial assessment of the exposure.

The purpose of introducing the risk-based approach is to ensure that anti money laundering and terrorist financing measures applied by banks are proportionate to the identified risk. This approach provides for determining potential money laundering and terrorist financing risks and enables the institutions to focus on those customers, business relationships, transactions or products which pose the greatest risk.

The institutions must be able to prove that the level of due diligence measures applied is appropriate in relation to the risk of money laundering and terrorist financing.

2.1 Applicability of the Risk-Based Approach to Terrorist Financing

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 funds that are used to finance terrorist activities may be derived either from criminal activity or from legal sources, so 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. However, as transactions associated with terrorist financing are mainly conducted in very small amounts, these transactions are in applying a risk-based approach to money laundering considered to be of minimal risk.

Where funds for financing terrorist activities are from legal sources then it is even more difficult to determine that they could be used for terrorist purposes. In addition, the actions of terrorists may be overt and outwardly innocent in appearance, such as the purchase of materials and services (*i.e.* commonly held chemicals, a motor vehicle, etc.).

However, as regards the issue of terrorist financing, it is not the responsibility of the financial institution to determine the type of underlying criminal activity, or intended terrorist purpose, rather the institution's role is to report the suspicious activity. The Office for Money Laundering Prevention (hereinafter: the Office) and law enforcement authorities are responsible for examining the matter further and determining if there is a link to terrorist financing.

Given the international character of terrorist financing and the absence of generally accepted typologies, *i.e.* methods and techniques used for terrorist financing, the institutions 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 terrorists are known to operate.

“Credible sources” refers to information that is produced by well-known bodies that generally are regarded as reputable and that make such information publicly and widely available. In addition to the Financial Action Task Force and FATF-style regional

bodies, 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. The information provided by these credible sources does not have the effect of law or regulation and should not be viewed as an automatic determination that something is of higher risk.

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

3. Money Laundering and Terrorist Financing Risk Assessment

3.1 Risk Categories, Criteria and Variables

Risk Categories

When analysing and assessing money laundering and terrorist financing risks, the institutions will classify their customers, business relationships, transactions or products in 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 institution's risk-based approach methodology may take into account risk variables which are specific to a particular customer, business relationship, product or transaction and which may increase or decrease risk. Risk variables include:

- 1. The purpose of an account or business relationship** — accounts opened primarily to facilitate traditional, low-denominated customer transactions may pose a lower risk than an account opened to facilitate large cash transactions from 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 other oversight or governance regime to which a customer is subject — a financial institution regulated 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 minimal money laundering risks. These companies are usually from countries with an adequate, recognised regulatory scheme, and, therefore generally pose less 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 relationships involving frequent customer contact throughout the relationship may present less risk from a money laundering perspective.
5. **Familiarity with the country of a client** — including knowledge of its laws, regulations and rules, as well as the structure and extent of regulatory oversight affects 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 which the institutions have submitted to the Office in the past three years** — in relation with the person in question or its transactions there were reasons for suspicion of money laundering or terrorist financing, which increases the risk.

Equivalent third countries shall be countries which are not Member States of the European Union or signatories of the Agreement on the European Economic Area but meet equal standards in the field of prevention of money laundering and terrorist financing as the Member States of the European Union.

3.2 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, the institutions will determine the due diligence requirements appropriate to each customer. This includes:

1. a standard level of due diligence, to be applied to all categories to which 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 lower 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 level of due diligence in respect of customers identified as higher risk customers, in which case enhanced customer due diligence measures apply; and
 4. exemptions from conducting customer due diligence measures as prescribed by Article 14, paragraph 2 of the Law or an ordinance issued by the Minister of Finance.

Since the setting of parameters by the Law or regulations may limit the discretion in selecting the most appropriate due diligence measures and restrict the institutions from making a free assessment, the institutions are under Article 30 of the Law obligated to apply enhanced due diligence measures, in addition to the measures laid down in Article 8, paragraph 1 of the Law, 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 personally present during the identification and identity verification procedures.

3.3 Entrusting a Third Person with the Conduct of Due Diligence

When establishing a business relationship with a client, the institutions may, under the conditions laid down by the Law and subordinate legislation, entrust a third person with the conduct of the identification and identity verification procedures.

The institutions have to beforehand verify whether the third person they are about to entrust with the conduct of customer due diligence fulfils all the conditions prescribed by the Law.

Customer due diligence conducted for an institution 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.

4. Low Money Laundering or Terrorist Financing Risk

4.1 Customer Risk

A reduced standard level of due diligence can be applied in case of:

1. banks, Member States bank branches, third countries bank branches, and banks from the Member States which are authorised for a direct provision of banking services in the Republic of Croatia, savings banks and housing savings banks;
2. Croatian Post (Hrvatska pošta d.d.);
3. investment funds management companies, business units of third countries investment funds management companies, investment funds management companies from the Member States which have a business unit in the Republic of Croatia, i.e. which are authorised to directly perform funds management business in the territory of the Republic of Croatia, and third parties which may be entrusted, in accordance with the law governing the operations of funds, with the conduct of individual operations by an investment fund management company;
4. pension companies;
5. companies authorised to do business with financial instruments and branches of foreign companies dealing with financial instruments in the Republic of Croatia;
6. insurance companies authorised for the performance of life insurance matters, branches of insurance companies from third countries authorised to perform life insurance matters and insurance companies from the Member States which perform life insurance matters directly or via a branch in the Republic of Croatia, or a similar institution provided it has a seat in a Member State or a third country;
7. state bodies, local and regional self-government bodies, public agencies, public funds, public institutes or chambers;
8. companies whose securities have been accepted and are traded on the stock exchanges or the regulated public market in the Republic of Croatia or in one or several Member States in line with the provisions in force in the European Union, i.e. companies with a seat in a third country whose securities have been accepted and are traded on the stock exchanges or the regulated public market in a Member State or in that third country, under the condition that the third country disclosure requirements in effect are the same as those in effect in the European Union;
9. other financial institutions from equivalent third states.

A reduced standard level of due diligence, i.e. simplified customer due diligence measures are prescribed by Article 36 of the Law.

In addition, customers identified as posing low risk in terms of money laundering and terrorist financing may only include those customers who meet the conditions determined by an ordinance of the Minister of Finance.

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

4.2 Product/Transaction Risk

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

1. credit agreements where credit accounts are used exclusively for loan settlement and loan repayment is executed from an account opened in the name of the customer in a supervised credit institution;
2. transactions involving de minimis amounts for particular types of transactions (e.g. small insurance premiums);
3. savings deposits in housing savings banks.

4.3 Exemptions from the Obligation to Conduct Due Diligence Measures

Electronic money institutions, electronic money institutions from another Member State and business units of foreign electronic money institutions from a third country may be exempted from the obligation to conduct customer due diligence measures in the following instances:

1. when issuing electronic money, if the single amount of payment executed for the issuance of such a 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 performing business with electronic money if the total amount of the 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 cases where the holder of electronic money cashes out a kuna equivalent of EUR 1,000.00 or more during the same calendar year.

The institutions may be exempted from the obligation to conduct customer due diligence measures in the case of other products or transactions associated with them, which pose an insignificant money laundering or terrorist financing risks, provided they meet the conditions prescribed by an ordinance of the Minister of Finance.

By way of exception, the institutions may not be exempted from the obligation to conduct customer due diligence measures when there is reason to suspect that a customer, product or transaction is suspicious of money laundering or terrorist financing activities.

5. Moderate Money Laundering or Terrorist Financing Risk

The institutions shall identify as medium risk category those customers, business relationships, products or transactions which, based on risk analysis and assessment, cannot be identified as posing low or high risk. In such a case, the institutions will act in

accordance with the provisions of the Law which govern the area of standard customer due diligence.

6. High Money Laundering or Terrorist Financing Risk

6.1 Customer Risk

The higher level of standard due diligence shall be applied in case of:

1. politically exposed foreign persons;
2. persons who are not personally present at 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 their registration;
4. customers where the structure or nature of the legal entity makes it difficult or impossible to identify the beneficial owner;
5. customers which are foreign legal persons carrying out the operations referred to in Article 3, item 21 of the Law, and having unknown or hidden owners, secret investors or managers;
6. customers whose beneficial owner is 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 businesses including:
 - (a) remittance houses, authorised exchange offices, money transfer agents and other businesses offering money transfer facilities;
 - (b) casinos, betting and other gambling related activities;
 - (c) businesses that while not normally cash intensive, generate substantial amounts of cash for certain transactions.
8. charities and other “not for profit” organisations, especially those operating on a “cross-border” basis or those seated in a geographical area which poses a higher risk, or its founders or members are natural or legal persons seated or domiciled in a geographical area which poses a higher risk;
9. accountants, lawyers, or tax advisors and others holding accounts at a financial institution, acting on behalf of their clients;
10. customers conducting their business relationship or transactions in unusual circumstances, such as:
 - (a) significant and unexplained geographic distance between the seat of the institution and the location of the customer;
 - (b) frequent and unexplained movement of accounts to different institutions;
 - (c) frequent and unexplained transfer of funds among institutions in different geographical locations;
11. persons in connection with 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 the suspicious transaction;
 - (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 the states 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.)

6.2 Transaction/Business Relationship Risk

Transactions or business relationships carrying a high risk include:

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

6.3 Risk of Business Relationship with other Credit Institution

The establishment of a correspondent relationship with a bank or another credit institution with a seat in a third country poses a high risk.

In accordance with Article 31 of the Law, when establishing a correspondent relationship with a bank or other credit institution with a seat in a third country, the institutions are obliged to conduct measures referred to in Article 8, paragraph 1 of the Law within the framework of enhanced customer due diligence and additionally gather the following data, information and documentation:

1. date of issuance and validity period of license for the performance of banking services, and the name and the seat of the competent third country license issuing body;
2. description of the implementation of internal procedures relating to money laundering and terrorist financing prevention and detection, most notably the procedures of customer identity verification, beneficial owners 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 passed in relation with money laundering and terrorist financing

- prevention and detection;
3. description of the systemic arrangements in the field of money laundering and terrorist financing prevention and detection in effect in the third country in which the bank or other credit institution has its seat or in which it is 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 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 obliged to apply legal and other regulations in the field of money laundering and terrorist financing prevention and detection in accordance with the effective laws of that country.

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

1. a written statement that the bank or other credit institution has verified the identity of the customer and that it conducts ongoing due diligence of customers who have direct access to payable through accounts,
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 with direct access to payable through accounts.

Assessment of exposure to money laundering and terrorist financing risk is carried out in accordance with the risk criteria and elements from the following risk matrix:

Low	Moderate	High
Stable, known customer base.	Customer base increasing due to branching, merger, or acquisition.	A large and growing customer base in a wide and diverse geographic area.
No electronic banking (e-banking) or the web site is informational or non-transactional.	The bank is beginning e-banking and offers limited products and services.	The bank offers a wide array of e-banking products and services (i.e., account transfers, e-bill payment, or accounts opened via the Internet).
There are a few high-risk customers and businesses.	There is a moderate number of high-risk customers and businesses. These may include check cashers, convenience	There is a large number of high risk customers and businesses. These may include check cashers, convenience stores, money

	stores, money transmitters, casas de cambio, import or export companies, offshore corporations and politically exposed persons (PEPs).	transmitters, casas de cambio, import or export companies, offshore corporations and politically exposed persons (PEPs).
No foreign correspondent financial institution accounts. The bank does not engage in pouch activities, offer special-use accounts, or offer special use accounts or payable through accounts (PTAs).	The bank has a few foreign correspondent financial institution accounts, but typically with financial institutions with adequate AML policies and procedures from low-risk countries, and minimal pouch activities, special-use accounts or PTAs.	The bank maintains a large number of foreign correspondent financial institution accounts with financial institutions with inadequate AML policies and procedures, particularly those located in high-risk countries, or offers substantial pouch activities, special-use accounts, or PTAs.
The bank offers limited or no private banking services or trust and asset management products or services.	The bank offers limited domestic private banking services or trust and asset management products or services over which the bank has investment discretion. Strategic plan may be to increase trust business.	The bank offers significant domestic and international private banking or trust and asset management products or services. Private banking or trust and asset management services are growing. Products offered include investment management services, and trust accounts are predominantly nondiscretionary versus where the bank has full investment discretion.
Few international accounts or very low volume of currency activity in the accounts.	Moderate level of international accounts with unexplained currency activity.	Large number of international accounts with unexplained currency activity.
A limited number of funds transfers for customers, non-customers, limited third-party transactions, and no foreign funds transfers.	A moderate number of funds transfers. A few international funds transfers from personal or business accounts with typically low-risk countries.	A large number of non-customer funds transfer transactions payable upon proper identification (PUPID) transactions. Frequent transfers of funds from personal or business accounts to or from high-risk countries, offshore

		financial centres or financial secrecy haven countries.
No transactions with high-risk geographic locations.	Minimal transactions with high-risk geographic locations.	Significant volume of transactions with high-risk geographic locations.
Low turnover of key personnel or frontline personnel (i.e., customer service representatives, tellers, or other branch personnel).	Low turnover of key personnel, but frontline personnel in branches may have changed.	High turnover, especially in key personnel positions.

The employee of the institution who establishes a correspondent relationship with a bank or other credit institution with a seat a third country and who performs an enhanced customer due diligence check is obliged to obtain a written approval of the superior responsible person prior to establishing the business relationship.

Institutions are prohibited from establishing or continuing a correspondent relationship with a bank which operates or could operate as a shell bank or with other similar credit institutions known to enter into agreements on opening and keeping accounts with shell banks. In addition, items (1), (2) and (3) of paragraph (4), Article 31 of the Law shall apply.

6.4 Foreign Politically Exposed Persons

According to Article 32 of the Law, institutions are obliged to apply an adequate procedure to determine whether or not a customer is a foreign politically exposed person. The procedure is defined through internal bylaws, 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 the information from the customer by means of a written form;
2. collect the information from public sources (information that is publicly available in the media - in the press, on TV and on the Internet);
3. collect information by accessing commercial data bases which include lists of politically exposed persons.

6.5 Customer's Absence during the Identification and Identity Verification

According to Article 33 of the Law, when determining and verifying the identity of a

customer who is not physically present, an institution is obliged to perform the following enhanced due diligence measures:

1. collect additional documents, data or information on the basis of which the customer's identity is verified;
2. additionally verify the submitted documents or additionally certify them by a 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 carried out through an account opened in the customer's name with another credit institution.

Additional documents, data or information on the basis of which the customer's identity is verified may be as follows:

1. for residents, evidence of permanent residence obtained from the competent authority that keeps the record or certificate of permanent residence issued by the Police Department; for non residents, evidence obtained from, e.g. credit reference agency;
2. personal references (e.g. from an existing customer of the institution);
3. previous bank references and contact;
4. data on the source of funds and assets which are or will be the subject of the business relationship;
5. certificate of employment or the public function that the person holds.

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

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

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

1. by examining a copy of the latest performance report and financial statements (audited, if available);
2. through an examination performed by the Business Information Centre or a statement of a reputable and well-known attorney or accounting company that verifies 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, that it has not 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 independent verification of information, such as accessing public and private data bases;
- 5. by obtaining prior references of the institution;
- 6. by contacting the company via telephone, mail or e-mail.

In some jurisdictions other equivalent documents may exist which may provide satisfactory evidence on the identity of a customer.

6.6 Country Risk

Customers that represent a high risk shall be customers that have permanent residence or 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 prevention of money laundering and terrorist financing;
 - (b) providing funding or support for terrorist activities and that have designated terrorist organisations operating 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 of the Agreement on the European Economic Area but do not qualify as equivalent third countries;
4. countries which according to the FATF data belong to non-cooperative countries or territories or in case of Offshore Financial Centres are on the list supplied by the Office for Money Laundering Prevention.

As regards information on higher risk countries or non-cooperative countries or territories that do not meet key international standards for the prevention of money laundering or terrorist financing, we advise you to consult the official web sites of:

MONEYVAL, www.coe.int/t/dghl/monitoring/moneyval, and FATF, www.fatf-gafi.org.

6.7 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 being potentially higher risk, including, for example:
 - (a) international services of third-country correspondent bank, including commercial payments for non-customers (for example, acting as an intermediary bank); or

- (b) pouch activities; and
 - (c) international private banking services;
2. services involving banknote and precious metal trading and delivery;
 3. services that inherently provide more anonymity or can readily cross international borders, such as online banking, stored value cards, international wire transfers, private investment companies and trusts, non-government organisations, etc.

6.8 Enhanced Customer Due Diligence Measures

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

With respect to other customers, business relationships and transactions which have been determined to be higher risk, institutions should, within the framework of increased level of standard verification, implement appropriate measures and controls aimed at reducing exposure to identified risks. These measures and controls may include:

1. monitoring of all areas of customers' operations, their business relationships, products and high risk transactions;
2. increased level of determination and verification of customer identity;
3. escalation for approval of the establishment of an account or relationship;
4. increased monitoring of transactions; and
5. increased levels of ongoing controls and frequency of reviews of relationships.

The same measures and controls may address more than one of the risk criteria identified and it is not necessarily expected that a financial institution establish specific controls targeting each risk criteria.

7 New Technologies Providing for Anonymity

When establishing policies and procedures aimed at reducing exposure to the risk of money laundering and terrorist financing stemming from new technologies enabling anonymity (electronic or Internet banking, electronic money, etc), institutions should provide for implementation of technological solutions which ensure:

1. unequivocal identification of customers using electronic banking;
2. credibility of the signed electronic documents;
3. reliable measures against document and signature counterfeiting;
4. systems that are protected from alterations and ensure technical and cryptographic security for electronic banking; and

5. other conditions in accordance with positive regulations governing this area of operation.

Aiming at unequivocal identification of customers using electronic banking, institutions may use different methods to determine identity, including PINs, passwords, smart cards, biometrics and digital certificates.

Final Provisions

Guidelines relating to the prevention of money laundering and terrorist financing for credit institutions and credit unions of 10 January 2008, Decision No. 54-020/01-08/ŽR shall cease to have effect on the date of adoption of these Guidelines.

Decision No. 636-020/07-09/ŽR
Zagreb, 9 July 2009

GOVERNOR
OF THE CROATIAN NATIONAL BANK

Dr Željko Rohatinski