

# Money laundering: correlation between risk assessment and suspicious transactions

SONJA CINDORI, PhD\*

Review article\*\*

JEL: K42

doi: 10.3326/fintp.37.2.3

---

\*The author would like to thank two anonymous referees for their useful comments and suggestions.

\*\* Received: January 31, 2012

Accepted: December 18, 2012

---

Sonja CINDORI

University of Zagreb, Faculty of Law, Ćirilometodska 4, 10000 Zagreb, Croatia

e-mail: scindori@pravo.hr

## Abstract

*The risk assessment system was introduced in the Republic of Croatia in 2009, as a result of harmonization with international standards, especially the Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. Risk assessment is an extensive concept which requires not only a legislative framework, but also the application of numerous criteria for its effective implementation in practice. Among these criteria are suspicious transactions, closely related to the assessment of the customer, transaction, product or service.*

*The undeniable contribution of suspicious transactions to the quality of the risk assessment system will be confirmed by a statistical analysis of a number of West and East European countries. A combination of strict, but sufficiently flexible legal provisions governing the system for prevention of money laundering and terrorist financing and a statistical analysis of reported suspicious transactions will lead to conclusions that either support or represent criticism of the efficiency of application of the risk assessment system in practice.*

*The aforementioned statistical analysis will show whether suspicious transactions are a reliable criterion for the risk assessment analysis, and whether they can be considered the only such criterion. There is a possibility that the findings of the analysis will be contradictory to those of some international studies.*

*Keywords: money laundering, suspicion, transaction, risk, risk assessment, statistics, analysis*

## 1 INTRODUCTION

The variety of possibilities to convert illegal into apparently legal money suggests that money laundering is a complex activity. Without prejudice to the unbounded sophistication, inventiveness and imagination of money launderers in finding perfect way to launder money, preventive measures to this effect include the detection of cash and suspicious transactions through risk assessment, i.e. the application of a risk-based system<sup>1</sup>.

This raises the issues of implementation of the idea of money laundering prevention through risk assessment, the legality of its practical consequences and logicity of its realisation. Resolving these issues requires understanding of the definition and nature of risk assessment. In this context, suspicious transactions represent the backbone of any money laundering prevention system, the analysis of which will show how the risk assessment operates in practice.

<sup>1</sup> The “risk-based system” is a money laundering prevention system based on risk assessment, as opposed to a “rule-based system” which relies on strictly defined rules.

## 2 MEANING OF THE “RISK-BASED APPROACH” SYSTEM

The primary characteristic of the money laundering prevention system based on risk assessment is that it is complex and necessarily resilient. While on the one hand the financial and non-financial sectors are required to apply some basic prevention rules, on the other hand they are supposed to have their own approaches to risk assessment, and hence to the reporting of suspicious transactions.

The main principle underlying any system for the prevention of money laundering and terrorist financing is that the higher the risk of money laundering the closer the attention needed from all competent institutions. Yet, following this principle is far from simple. Unlike with the rule-based system<sup>2</sup> applied so far, the logic behind the risk-based system is entirely different.

A system based on rules initially requires from all those responsible for the prevention to apply clear and rigid rules in legally prescribed situations. Within such a system, financial and non-financial institutions, being the chief agents of prevention, are focused on meeting the precisely defined legal conditions (treating them equally) rather than on “taking the pulse” of potential money launderers.

A much greater effort is required to change the perception of the importance and scope of money laundering prevention, from the routine fact-finding prescribed by law to the assessment of each client through a sophisticated risk assessment filter. Unavoidable in this context is the appropriate application of the legislation as well as guidelines and indicators to be adjusted to each particular case and then used in practice.

Accordingly, the risk assessment system requires not only the assessment, but also classification of risks and their materialisation in the form of suspicious transactions. While suspicious transactions constitute the backbone of the risk, it is clear that there are no universally accepted methodologies to describe the nature and scope of such transactions. They appear through the identification and classification of the money laundering and terrorist financing risks, which results in the establishment of control mechanisms tailored to the detected risk.

This statement does not mean the absence of any principled rules applying to the customer and the customer’s business. The imposed rules only represent a framework for action, with a certain degree of flexibility of implementation, in accordance with the risk assessment for each category of customers, transactions, products or services rendered.

---

<sup>2</sup> The “rule based system”, i.e. a system based on rules was presented in the first two EU directives on prevention of the use of the financial system for money laundering purposes (Directive 91/308/EEC and Directive 2001/97/EC amending the Directive 91/308/EEC).

## 2.1 RISK CATEGORISATION

The FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing indicates three steps in an effective implementation of the risk-based approach, namely the risk detection, risk assessment and development of strategies to manage and mitigate the risks (Financial Action Task Force, 2007). The risk, as the basic concept, is closely related to the customer, product of service, including the manner of conducting transactions and geographic location of the country assessing the risk.

The said FATF Guidance recognises three risk categories: low risk, high risk and innovation (new technologies to ensure anonymity). The fourth category comprises mechanisms for the analysis of applied procedures for deciding on the level of risk, the way of acting upon identified risks and the evaluation of such actions. Risk assessment should be tailored to each customer, product or service, by employing a measure corresponding to the degree of identified risk. However, it is not unthinkable that two financial institutions could take different decisions on the basis of similar parameters.

This reaffirms the fact that the risk assessment method is not easy to apply. The sharper the deviation from the risk assessment principle the stronger is the possibility of negative consequences. While the overestimation of risk is impossible due to limited time, personnel and information sources, its underestimation is an unacceptable alternative. A good risk assessment system should primarily be balanced. To this effect, an efficient application of the risk-based approach should include the undertaking of customer due diligence, as well as effective supervision and information exchange between the financial intelligence unit (hereinafter: FIU) and all institutions participating in the prevention of money laundering and terrorist financing.

## 3 SUSPICIOUS TRANSACTIONS

The money laundering risk assessment by its nature consists in the filtering of all available information in order to identify suspicious transactions or customers. Given the complexity of the money laundering process, it is clear that the detection of suspicious transactions involves a set of different preventive measures.

If the money laundering stages are viewed from the perspective of implementation of the money laundering risk assessment, the placement and layering stages are the most relevant in the process of transforming money into a more convenient form of assets (Cindori, 2010). Despite the differences in the money laundering modalities with respect to the amount of money to be laundered, relevant legislation, economic situation, financial market, chosen method of operation (through the financial or non-financial sector), as well as the actual (stages of the) process through which the dirty money goes, the money laundering risk can be most easily

assessed during these two stages, because they offer unlimited opportunities to carry out due diligence of the customer, a product or a transaction.

At the first stage, by placing money into the financial system or converting it into another form of assets, money launderers are already subject to customer due diligence, i.e. the application of the risk-based system. At the second stage, cash is deposited in one or several accounts (held by one or more persons) with a view to fragmenting large amounts of money and channelling them to various natural or legal persons and changing the form of money. The activities subsequently carried out by legislators for prevention purposes, i.e. the detection of suspicious or illogical transactions, most frequently constitute *modus operandi* at the layering stage. From this perspective, it is easy to conclude that suspicious transactions are very difficult to detect at the third money laundering stage (integration stage).

### 3.1 SUSPICIOUS TRANSACTIONS IN THE EUROPEAN UNION

The EU directives on prevention of the use of the financial system for money laundering purposes very clearly show the evolution of the definition of suspicious transaction. By setting up the fundamentals of a prevention strategy to combat money laundering, these directives impose the need for harmonization and adjustment of national legislations. In this context, the need is emphasized to set up an anti-money laundering system relying on “a risk-based approach”, which will increase the importance of suspicious transactions and their treatment.

The first attempts to set up a framework for preventive measures in the area of anti-money laundering were made in the Directive 91/308/EEC (hereinafter: First Directive), which was the first to define, although very elastically, the term “suspicious transaction”. As this definition required from credit and financial institutions to check *each transaction that might be connected with money laundering*, the content of the term was obviously vague and it should necessarily undergo legislative revision at the national level. Taking into account that the First Directive was only guidance for action at the national level, despite the very elastic definition of suspicious transactions it provided (Graham, Bell and Elliott, 2006), it in a way created a basis for preventive action.

The Directive 2001/97/EC (hereinafter: Second Directive) does not go much further in developing the definition of suspicious transactions, but it identifies independent professions and occupations that are exempt from the obligation to report suspicious transactions in certain cases<sup>3</sup>.

In contrast to the first two directives, the Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (hereinafter: Third Directive) is based on risk assessment and hence it

<sup>3</sup> For more information, see Article 1, item 5 of the Second Directive.

deals with the issue of detecting suspicious transaction in an entirely different way.

The Third Directive assigns a new role to suspicious transactions, seeing them (indirectly) as the backbone of money laundering prevention through a risk-based system. In the Directive, the term “suspicious transaction” is not explained in the form of a definition, but is “hidden” in Article 20 (Reporting Obligations). While it, to some extent, repeats the definition from the First Directive, this Article expands the concept of suspicious transactions to include complex and unusual transactions, specifying and elaborating on the concept of “being suspicious”<sup>4</sup>. All this said, there is no doubt that suspicious transactions are important for setting up a money laundering prevention system, as reflected in the obligation of all institutions and persons covered by the Third Directive to carry out customer due diligence, which is a signal of a new, risk-based approach to suspicious transactions.

The implementation of customer due diligence measures and their content clearly suggest that the perception of money laundering goes far beyond the disposing of cash, and the suspicion of money laundering exists from the customer identification at the moment of (or before) establishing a business relationship to the verification of data. Suspicion also exists when carrying out other due diligence activities which require an ongoing gathering of information on the purpose and envisaged nature of the business relationship and its continuous monitoring, with a view to creating the customer, business and risk profiles and identifying the source of the customer’s funds.

Similar development logic of suspicious transactions can be found in the FATF Recommendations. Significant changes towards risk assessment can be observed in the latest revised FATF Recommendations 2012. Both financial and non-financial sectors are increasingly focused on higher-risk areas, while the measures applicable to lower-risk areas become simpler and more elastic.<sup>5</sup>

#### 4 RISK ASSESSMENT SYSTEM IN THE REPUBLIC OF CROATIA

The legislation of the Republic of Croatia has been developed in accordance with the three aforementioned directives.

The first anti-money laundering law was passed in 1997. The definition of suspicious transactions was not given separately, but it arose from the content of customer identification procedures<sup>6</sup>, which did not specify the characteristics of a suspicious transaction, but a suspicious transaction was considered to be “any cash or non-cash transaction for which there is suspicion of money laundering”.

<sup>4</sup> For more information, see Article 22 of the Third Directive.

<sup>5</sup> The Revised Recommendations are available at: [<http://www.fatf-gafi.org/topics/fatfrecommendations/documents/internationalstandardscombatingmoneylaunderingandthefinancingofterrorismproliferation-thefatfrecommendations.html>].

<sup>6</sup> For more information, see Article 4 of the Anti-Money Laundering Act (Croatian version, OG 69/97).

By introducing amendments to the Anti-Money Laundering Act<sup>7</sup> (hereinafter: AMLA) considerable progress was made in this respect, but without any substantial changes in the operation of the Anti-Money Laundering Office (hereinafter: Office). There was still no definition of suspicious transactions, although the term was used in the general provisions on the activities of the Office in “detecting *suspicious transactions*, concealing the true source of money, property or a right suspected to have been obtained illegally in the country or abroad”<sup>8</sup>. While this undoubtedly emphasized the importance of suspicious transactions, it was quite certain that the Office’s activities were still focused on cash transactions<sup>9</sup>.

By following the Third Directive, the Republic of Croatia introduced a new Anti-Money Laundering and Terrorist Financing Act<sup>10</sup> (hereinafter: AMLTFA), thereby adopting the risk assessment system. In other words, the necessity to carry out customer due diligence and risk assessment as crucial measures has been mentioned throughout the AMLTFA. Consequently, suspicious transactions play a leading role in the detection of money laundering and terrorist financing. This is reflected in the obligation of the Office to carry out analytical data processing exactly on the basis of substantiated reasons for suspicion of money laundering or terrorist financing.

Besides suspicious transactions, the AMLTFA also recognizes complex and unusual transactions. In contrast to suspicious transactions that arouse a certain degree of suspicion sufficient for establishing a criminal offence, an unusual transaction is considered to be any illogical transaction in relation to which no criminal offence has yet been established. Given these criteria, it is beyond doubt that a large number of reported suspicious transactions actually constitute unusual or illogical transactions (Savona, 2004).

This is exactly why the legislator emphasized the need to pay close attention to all complex and unusual transaction, as well as to any other unusual form of transaction having no obvious economic or legal purpose<sup>11</sup>. The risk assessment system definitely requires that such transactions be monitored, even in situations when no reasons for suspicion of money laundering or terrorist financing have yet been identified.

<sup>7</sup> Amendments to the Anti-Money Laundering Act (Croatian version, OG 117/03).

<sup>8</sup> The amendments to the existing Act were in accordance with the international standards then in force, i.e. Article 3, paragraph (8) of the Second Directive, and FATF Recommendations Nos 13 and 11.

<sup>9</sup> For more information, see the Ministry of Finance Annual Reports 2005-2008: [<http://www.mfin.hr/hr/godisnjaci-ministarstva>] and Moneyval reports: [[http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/Evaluation\\_reports\\_en.asp](http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/Evaluation_reports_en.asp)].

<sup>10</sup> Anti-Money Laundering and Terrorist Financing Act (Croatian version, OG 87/08).

<sup>11</sup> For more information, see Article 43 of the AMLTFA.

#### 4.1 DEFINITION AND ASSESSMENT OF RISK

The guiding principle of the AMLTFA arises from the risk assessment, as shown in Article 7 of the Act, providing a definition of the money laundering and terrorist financing risks. The focus is principally on the risk that a customer might misuse the financial system for money laundering or terrorist financing, or that a business relationship, a transaction or a product might be directly or indirectly used for money laundering or terrorist financing purposes.

In order to reduce the risk, reporting entities are obliged to undertake a risk analysis and use it for assessing the risk of a group or type of customers, a business relationship, a product or a transaction with respect to their potential misuse for money laundering or terrorist financing purposes. In this context, reporting entities may include in the group of customers representing a negligible risk only the customers determined by a rulebook laid down by the finance minister. The limitation regarding risk assessment arises from the reporting entity's obligation to comply with the guidelines issued by competent supervisory authorities. In other words, during the risk analysis and assessment both the reporting entity and supervisory authority are obliged to consider the specific characteristics of the reporting entity and its business, while taking into account the size and organisational structure of the reporting entity, the type of customers it deals with and the type of products it offers.

#### 4.2 DEFINITION OF SUSPICIOUS TRANSACTIONS

The risk assessment procedure inevitably entails the definition of the concept of "suspicious transactions". Treating risk assessment as the guiding principle, the AMLTF treats suspicious transactions with equal care, surpassing the criteria set in accordance with international standards.

In light of this, according to the Act, a suspicious transaction is any attempted or executed cash or non-cash transaction, regardless of its value and the manner of its execution. Already in the first part of the definition the legislator emphasizes the active role of a reporting entity in the detection of (innovative) money laundering or terrorist financing attempts. The definition further indicates three characteristics a transaction may (but not necessarily must) have in order to be considered as suspicious:

- a) it must be connected with illegal sources or funds or with terrorist financing;
- b) it must deviate from a customer's normal operation, taking into account the set indicators; and
- c) there must be an attempt to find loopholes in the law.

Besides these possible reasons for suspicion of money laundering, established on the basis of categorisation, considered as suspicious is also any transaction or cu-



stomer for which/whom the reporting entity deems that there are reasons for suspicion of money laundering or terrorist financing<sup>12</sup>.

As suspicious transactions, by their very nature, pose high money laundering and terrorist financing risks, each reporting entity is obliged to detect them within its activity, taking into account the specificities of the business. This confirms that the AMNLTA is founded on risk assessment, the monitoring of the customer's operations and collection of information on the purpose and envisaged nature of the business relationship. This is why the compilation of a list of indicators for the detection of suspicious transactions and persons in relation to which there are reasons for suspicion of money laundering or terrorist financing is within the competence of the reporting entity<sup>13</sup>.

### 4.3 TREATMENT OF SUSPICIOUS TRANSACTIONS

Besides the aforementioned definition of a suspicious transaction, the AMLTFA, in its very introduction, defines a suspicious transaction as any transaction for which a reporting entity and/or a competent authority deems that there are reasons for suspicion of money laundering or terrorist financing in relation to that transaction or a person conducting the transaction, or a transaction suspected to involve funds derived from illegal activities. While it is emphasized that a competent authority can also assess a transaction a suspicious, based on a subsequently conducted strategic analysis, the focus is also on the importance of such transactions for the prevention of money laundering and terrorist financing.

In order to be classified as suspicious, transactions must be previously passed through the risk assessment filter, i.e. subjected to customer due diligence measures. The customer due diligence measures comprise identifying the customer and the beneficial owner and verifying their identities, as well as collecting information on the purpose and intended nature of the business relationship or a transaction. Besides these due diligence measures, it is particularly important to conduct ongoing monitoring of the business relationship to ensure the implementation of the risk assessment system in the way that the transaction analysis is consistent with the reporting entity's knowledge about the customer, type of business and risk, including, where applicable, information on the sources of funds<sup>14</sup>.

The same reasoning applies to the supervision of reporting entities. The Financial Inspectorate supervises compliance with the AMLTFA of all reporting entities exclusively on the basis of the assessment of money laundering and terrorist financing risks. In this context, should the Inspectorate establish that a legal person, a

<sup>12</sup> A definition of suspicious transactions is given in Article 42 of the AMLTFA.

<sup>13</sup> For a full and comprehensive overview, the supervisory authorities cooperate with reporting entities in the compilation of the list of indicators. Similarly, the minister of finance may, in a special rulebook, prescribe mandatory inclusion of particular indicators in the list of indicators for the detection of suspicious transactions and persons in respect of which there are reasons for suspicion of money laundering or terrorist financing. For more information, see Article 41, paragraphs (5) and (6) of the AMLTFA.

<sup>14</sup> Article 8 of the AMLTFA.

member of the management board (or another responsible person of the legal person), or a natural person has failed to make a risk analysis, or risk assessment for a particular group or type of customers, business relationships, products or transactions, or if such persons have failed to align the risk analysis and assessment with the guidelines issued by a competent supervisory authority, it can impose a fine on such persons for the committed violations<sup>15</sup>.

#### 4.4 ACTING UPON SUSPICIOUS TRANSACTIONS

The treatment of suspicious transactions is also reflected in the manner of reporting suspicious transactions and of how the Office acts upon them. Should a reporting entity, after the risk analysis, know or suspect that a transaction is connected with money laundering or terrorist financing, it should notify the Office of such a transaction without delay<sup>16</sup> prior to the execution of the transaction. The notification should be sent by telephone, fax or in another appropriate way, indicating all reasons for the suspicion of money laundering or terrorist financing and the deadline for the execution of the transaction<sup>17</sup>. Particularly important is the submission of information on the intention and planning to carry out a suspicious transaction, regardless of whether the transaction has subsequently been executed or not<sup>18</sup>.

By following the same line of logic, the commencement of the analytical processing by the Office is closely related to the transactions or persons in respect of which a reporting entity or a competent authority “submits substantiated reasons for suspicion of money laundering or terrorist financing”<sup>19</sup>. Thus, the legislator has placed emphasis on the fact that the Office should act upon transactions for which the risk analysis has been made, and has limited any action based on strict compliance with the rules. As a consequence of this, the number of “formally”

<sup>15</sup> A legal person will be fined between HRK 50,000 and HRK 700,000 and a member of the management board or another responsible person of the legal person will be fined between HRK 6,000 and HRK 30,000. A natural person who is a craftsman or a natural person engaged in another independent activity will be fined between HRK 35,000 and HRK 450,000 for the same violation. For more information, see Article 90 of the AMLTFA.

<sup>16</sup> Exempt from the obligation to report suspicious transactions is a group of professions and occupations, such as lawyers, notaries public, auditors and natural and legal persons providing accounting and tax consulting services, with respect to the information obtained from customers or about customers during the determination of the legal status of a customer or its representation in the court proceedings (including counselling the customer to propose or avoid legal proceedings), regardless of whether the information was obtained or collected before, during or after the proceedings. For more information, see Article 55 of the AMLTFA.

<sup>17</sup> We are talking here about an “active” role of the reporting entities based on their initiative, as opposed to a “passive” obligation to submit data additionally requested by the Office (Mitsilegas, 2003).

<sup>18</sup> Should it be necessary to take urgent action to verify data on a suspicious transaction or person, or should the Office deem that there are reasons for suspicion that a transaction or a person is connected with money laundering or terrorist financing, the Office may issue a written order instructing the reporting entity to temporarily suspend the execution of the suspicious transaction for a maximum of 72 hours. The Office will notify the State Attorney’s Office and/or the competent State Attorney’s Branch Office without delay of the issued orders. For more information, see Article 60 of the AMLTFA.

<sup>19</sup> Exceptionally, the Office may commence the analytical processing of suspicious transactions at a substantiated written proposal of the competent authorities, but only if such activities might be connected with money laundering or terrorist financing. For more information, see Article 64 of the AMLTFA.

open cases, encouraged under the old AMLA, was now reduced, which released additional resources for the Office<sup>20</sup>.

#### 4.5 COMPLEXITY OF THE SCOPE OF “SUBSTANTIATED REASONS FOR SUSPICION”

The way the Office acts upon “submission of substantiated reasons for suspicion of money laundering or terrorist financing” shows that the Office does not consider only suspicious transactions, but also all other transactions, either cash or linked transactions, for which it receives *substantiated reasons for suspicion of money laundering or terrorist financing* from a reporting entity.

The money laundering methods and typologies used by natural persons support the need for such an approach, but also for a more flexible, risk-based procedure. For example, depositing unusually large cash amounts, as a money laundering typology used by natural persons, includes cash deposits in all types of accounts which deviate from the normal customer’s account turnover. These are usually considerable amounts derived from illegal activities and representing illegal income of the customer. Most transactions of this type are not consistent with the business and economic criteria.

The very name of this money laundering method suggests that it deals with cash deposits, i.e. cash transactions. However, as the content of the term “unusually” (large amounts) varies from customer to customer, and is determined, e.g. by a customer’s business background, the values of such suspicious or illogical transactions very often remain below the legally prescribed limit for “cash transactions” subject to reporting to the Office. In assessing the risk of such transactions and identifying the character of their dubiousness, the first thing to do is to organise training for employees of financial and non-financial institutions who should be able, based on the indicators of suspicious transactions and information on the customer’s business, to detect a suspicious transaction and establish whether a business is really illegal.

As unusual or large cash deposits are conspicuous and open up further possibilities of a quick detection of money laundering cases, the so-called “linked transactions” are usually used in practice. They imply breaking down a large amount into several smaller amounts (to evade the reporting threshold for cash transactions), because smaller cash amounts apparently represent a better way of money laundering.

The breaking down of a transaction into smaller amounts and creation of “linked transactions” in order to evade the reporting requirements is referred to in English

<sup>20</sup> The legislative changes led to a restructuring of the Office, i.e. the establishment, among other departments, of a Prevention and Customer Supervision Department and a Strategic Analysis and IT System Department. For more information, see Regulation on the Internal Organisation of the Ministry of Finance (Croatian version, OG 29/09).

literature as “structuring”. Richards uses the same term explaining it as follows: “a person structures a transaction if that person, acting alone, or in conjunction with, or on behalf of other persons, conducts, or intends to conduct, one or more transactions in currency, in any amount, at one or more financial institutions, on one or more days and in any manner, for the purpose of evading the reporting requirements...” (Richards, 1998)<sup>21</sup>. Given this definition of the term “structuring”, it is beneficial to use the suspicious transaction indicators in order to facilitate the detection of linked transactions which are in themselves defined elastically, due to the complexity of their execution and impossibility of their strict regulation.

Consequently, it is obvious that, like cash and suspicious transactions, linked transactions can also be the subject of consideration for the Office, provided that there are “substantiated reasons for suspicion of money laundering or terrorist financing” with respect to such transactions. They will be considered as suspicious transaction and recorded in the Office’s statistics. Concrete analyses of suspicious transactions will show why this is important and what we can learn about the risk-based system from the statistics on reported suspicious transactions.

## 5 AN ANALYSIS OF SUSPICIOUS TRANSACTIONS AS RISK ASSESSMENT SYSTEM ANALYSIS

The application of a risk-based based system is far from being simple, from the perspectives of both legislative regulation and practical implementation efficiency. The complexity of the system is due to suspicious transactions, the content of which is indeterminable while their scope must not be limited. It is exactly this legislative philosophy that the risk assessment system is based on.

In order to prove the efficiency of application of such a system in the Republic of Croatia, we compared the statistics on suspicious transactions reported in the period 2005-2010 across ten countries of different sizes and at different levels of development and compliance with international standards.

### 5.1 IMPACT OF THE RISK-BASED APPROACH ON THE NUMBER OF REPORTED SUSPICIOUS TRANSACTIONS

According to the Final Study on the Application of the Third EU Directive on the prevention of the use of the financial system for the purpose of money laundering (hereinafter: Final Study)<sup>22</sup>, a risk-based system has a positive influence on reporting on suspicious transactions, in terms of the number of reported suspicious or unusual transactions, quality of such reports and their effects on the detection of suspicious transactions.

<sup>21</sup> There have been similar considerations in the Republic of Croatia long before the introduction of the legislation prescribing anti-money laundering measures. Hršak wrote about linked transactions as far back as 1993, as “large-scale financial operations broken down into a series of smaller transactions in small amounts of money” (Heršak, 1993).

<sup>22</sup> Available at: [[http://ec.europa.eu/internal\\_market/company/docs/financial-crime/20110124\\_study\\_amld\\_en.pdf](http://ec.europa.eu/internal_market/company/docs/financial-crime/20110124_study_amld_en.pdf)].

In the discussion on the “number of reported suspicious transactions” criterion and its relationship to the “quality of the reports” criterion in the said Final Study, it is emphasized that these two criteria are interdependent, i.e. that there is an increase in both the number of reported suspicious transactions and the quality of the reports, as a consequence of the application of the risk-based approach (as opposed to the previously applied rule-based approach).

As the application of the risk-based approach in the Republic of Croatia shows a completely opposite trend, i.e. a fall in the number of reported transactions, this problem demands closer attention in order to establish the real correlation between the number of reported suspicious transactions and the achievement of the main goals of the risk assessment system.

**TABLE 1**

*Reported suspicious transactions related to money laundering, 2005-2010*

Country	2005	2006	2007	2008	2009	2010
Bulgaria	680	374	431	591	883	1,460
France	11,553	12,047	12,481	14,565	17,310	19,208
Croatia	2,908	2,891	2,857	2,323	629	602
Liechtenstein	192	161	205	157*	235	261*
Germany	8,241	10,051	9,080	7,349	9,046	11,042
Romania	3,858	3,195	2,574	2,332	2,259	2,925
Slovenia	116	165	192	248	199	233
Serbia	138	622	1,432	2,884	3,957	4,537
Switzerland	729	619	795	851	896	1,159
Ukraine	350,507	313,074	322,966	290,418	227,192	96,221**

\* Reports on suspicious transactions received by 1 October 2008/2010.

\*\* Reports on suspicious transactions received by 1 August 2010.

Source: MONEYYVAL<sup>23</sup> Reports and Annual Reports of the stated countries.

### 5.1.1 A fall in the number of reported suspicious transactions

In order to understand the real nature of the risk assessment system and its correlation with the number of reported suspicious transactions, an analysis will be made of a fall in the number of reported suspicious transactions, observed in the Republic of Croatia, Slovenia and Ukraine.

#### 5.1.1.1 Croatia

The data on suspicious transactions related to money laundering, reported to the Office in the period 2005-2008 clearly show that their number was constant. With the entry into force of the AMLTFA in 2009, under which the risk-based approach was used in the detection and reporting of suspicious transactions, the number of suspicious transaction reports decreased up to five times (in 2009 and 2010). A comparison between the four-year period of application of the AMLA (2005-

<sup>23</sup> Available at: [[http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/Evaluation\\_reports\\_en.asp](http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/Evaluation_reports_en.asp)].

2008) and the two years of application of the AMLTFA (2009-2010) clearly shows that half as many suspicious transactions (on average) were reported in the two-year period of applying the risk-based approach as in one year of application of the rule-based approach.

The established decline in reported suspicious transactions was due to the application of the AMLTFA, which provides a very detailed description of the nature of suspicious transactions. Besides in the AMLTFA, suspicious transactions are also dealt with in the Regulations on the Notification of the Anti-Money Laundering Office of Suspicious Transactions and Persons<sup>24</sup>, with a detailed specification of the manner of and deadlines for reporting, as well as additional information to be submitted to the Office, and the electronic data delivery.

As a result of a detailed prescription of the content of a suspicious transaction and of assigning an active role to reporting entities<sup>25</sup> in setting up indicators for the detection of suspicious transactions, as well as their frequent participation in the training measures (in 2009 and 2010)<sup>26</sup>, the statistics only confirm an improvement in the quality of reports on suspicious transactions to the detriment of their quantity. Reporting entities have thus shown their maturity in the assessment of risks and detection of suspicious, unusual or illogical transactions. This mainly applies to the financial sector, i.e. banks, because they accounted for 90% of total suspicious transactions reported in the period 2005-2008, while this share dropped to 50% in the period 2009-2010. Nevertheless, the number of suspicious transaction reports coming from the non-banking and non-financial sectors remained unchanged, leaving a plenty of room for improvement and the overall system development.

Another reason for the expected evolution of the risk assessment system in terms of the number of open cases and forwarded notifications of suspicious transactions (NST<sup>27</sup>) is that in the period 2009-2010, 642 cases were opened and 235 NSTs sent to the competent authorities for further processing pursuant to the received reports on suspicious transactions. Or, out of 1,231 suspicious transactions reported by reporting entities in the period from 2009 to 2010, the Office opened 642 cases (52% of suspicious transactions reported in this period), whereas 235 NSTs submitted account for 19% of the total suspicious transaction reports.

<sup>24</sup> Regulations on the Notification of the Anti-Money Laundering Office of Suspicious Transactions and Persons (Croatian version, OG 1/09).

<sup>25</sup> Entities subject to the measures, actions and procedures for the prevention and detection of money laundering and terrorist financing are specified in Article 4 of the AMLTFA.

<sup>26</sup> The Ministry of Finance Annual Reports for 2009 and 2010; available at: [<http://www.mfin.hr/hr/godisnjaci-ministarstva>].

<sup>27</sup> Notifications of suspicions of money laundering or terrorist financing in the country or abroad, submitted by the Office to the competent state authorities and the responsible foreign FIU for further processing.

### 5.1.1.2 Slovenia, Romania and Ukraine

*Slovenia* also saw a decline in reported suspicious transactions in 2009. However, worth noting are some typical characteristics of the money laundering (and terrorist financing) prevention practice in Slovenia. The Slovenian Anti-Money Laundering and Terrorist Financing Act<sup>28</sup> came into force in mid-2007. A comparison between the number of suspicious transaction reports in 2005 (116) and 2006, when a rule-based approach was used (165), suggests their increase. But as early as 2007, after the harmonisation of the national legislation with international standards and the introduction of a risk assessment system in the middle of the year, only a minor increase was observed in reported suspicious transactions (192), probably due to the new principle of operation. In 2008, however, their number rose to 248, but fell again to 199 in 2009. Another increase in the number of reported suspicious transactions was seen in 2010 (233). As these were only slight changes in the already small number of reported suspicious transactions, and one could hardly talk about regularity in the number of suspicious transactions as the result of application of the risk assessment system. The only constant was the active participation of the financial sector, notably banks, (with 75% to 80%) in the total number of reported suspicious transactions in the period 2008-2010<sup>29</sup>. Nevertheless, the fact that the total number of reported suspicious transactions equals the number of open cases suggests that there is some degree of awareness among Slovenian reporting entities about this matter and that Slovenia's Office works efficiently.

Like most countries, *Romania* aligned its legislation with international regulatory standards as late as 2008, although it had recognised the importance of the prevention of terrorist financing back in 2002. Judging by statistics, a downward trend in reported suspicious transactions was observed in the period 2005-2009, with the exception of 2010, when an increase was recorded. As the number of suspicious transactions went up (to 2,925 in 2010), credit and financial institutions continued to account for a large share (90%) in total reported suspicious transactions. In 2010, however, the number of reported suspicious transactions increased by 29% from 2009, as a result of training within a twinning project in cooperation with the Polish FIU<sup>30</sup> and the application of on-line reporting parameters (Cindori, 2008). The increase in the number of suspicious transactions by raising the awareness of the financial sector (primarily through training) certainly suggests a positive trend. However, giving prominence to on-line reporting as an indicator of an (artificial) increase in this number is surely negative.

<sup>28</sup> Zakon o preprečevanju pranja denarja in financiranja terorizma (Ur. l. RS 60/07).

<sup>29</sup> Poročilo o delu Urada Republike Slovenije za preprečevanje pranja denarja za leto 2010; available at: [[http://www.uppd.gov.si/si/delovna\\_podrocja/podatki\\_o\\_delu\\_urada/](http://www.uppd.gov.si/si/delovna_podrocja/podatki_o_delu_urada/)].

<sup>30</sup> Main elements related to National Office for Prevention and Control of Money Laundering's activity, performed within the year 2010, Synthesis of the activity report; available at: [<http://www.onpcsb.ro./pdf/NOPCML%20Report%202010.pdf>].

Besides Croatia, Slovenia and Romania, *Ukraine* is also on the list of countries showing a downward trend in suspicious transaction reporting. This country is special in terms of its system for the prevention of money laundering and terrorist financing, as it had no adequate national legislation to this effect until 2003, but exclusively followed the relevant international standards, primarily the FATF Recommendations. It was therefore put on a “blacklist” of non-cooperative countries (Cindori, 2010). Based on a Law on the Prevention of and Counteraction to Legalisation (Laundering) of Illegal Proceeds from Crimes that entered into force in 2003, the country established a money laundering prevention system and harmonised its legislation with the Third Directive by introducing a Law on the Prevention of and Counteraction to Legalisation (Laundering) of Illegal Proceeds from Crimes and Terrorist Financing in 2010.<sup>31</sup>

Despite the small size of Ukraine, statistical data suggest an enormous number of reported suspicious transactions in the country. Despite a fall in these transactions from 350,000 in 2005 to 96,221 in 2010, their number is still huge. Even the smallest recorded number of suspicious transactions (96,221) reported in 2010 (the figure refers to the period before 1 August 2010) is 160 times the number of such transactions reported for the same year in, e.g. Croatia (602). According to the statistical data given in table 1 and their comparison with the data on reported suspicious transactions in Ukraine, the real number of reported suspicious transactions is expected to decline in the future, due to compliance with international standards and the implementation of a risk assessment system.

### 5.1.2 An increase in the number of reported suspicious transactions

In contrast to the described downward trend in reported suspicious transactions in Croatia, Slovenia, Romania and Ukraine, the Final Study supports the view that an increase in the number of reported suspicious transaction can be accounted for by a comprehensive implementation of the risk assessment system. The following statistics for a number of developed Western and North European countries will show whether this is really true and to what extent the evaluation of a risk assessment system can be based on the number of reported suspicious transactions.

#### 5.1.2.1 Switzerland, France, the Netherlands and Germany

*Switzerland* saw a modest increase in reported suspicious transactions from 2006–2009, which was even sharper in 2010 (29%). In the Annual Report for 2010<sup>32</sup> the upsurge in reported suspicious transactions was accounted for by the investigation of two complex cases in the banking sector which resulted in a large number of reports on suspicious transactions (144). Despite this, the banking sector continued to participate with 71% in the total number of reported suspicious transac-

<sup>31</sup> Law of Ukraine on Prevention and Counteraction to Legalization (Laundering) of the Proceeds from Crime or Terrorist Financing as of 18 May 2010, No 2258.

<sup>32</sup> Annual report by the Money Laundering Reporting Office Switzerland (MROS): a publication of the Federal Office of Police, Bern; available at: [<http://www.fedpol.admin.ch/content/fedpol/en/home/dokumentation/berichte/geldwaescherei.html>].



tions. An increase in the number of reports on suspicious transactions was also observed in the payment services sector, fiduciaries (trustees) and asset managers.

However, a real indicator of a highly developed risk assessment system is the number of suspicious transactions reported on the basis of own assessment rather than on the basis of strict legal provisions. The former type of reports is typical of the financial sector (banks and the payment service sector) and it accounts for one sixth of total reported suspicious transactions over the last eight years. The total number of reports based on own assessment grew in the reference period (2005-2010) due to legislative changes allowing the submission of reports directly to the MROS (the Swiss FIU) and not thanks to the criminal prosecution authorities.

We can therefore conclude that the Swiss system for prevention of money laundering and terrorist financing raises the awareness of the non-banking and non-financial sectors, which results in a larger number of suspicious transaction reports coming exactly from these sectors. However, an increase in the number of suspicious transactions reported on the basis of own assessment was also noticed.

Furthermore, the above described policy also raises the issue of delivery of information on attempted money laundering, i.e. on funds related to criminal organisations and funds derived from serious crimes, or generated by criminal organisations. This relates to a situation when a transaction has not yet been executed, or a business relationship has not yet been established<sup>33</sup>. In such cases, it is difficult to prove the predicate offence, or initiate criminal proceedings. However, the Swiss Federal Law on Combating Money Laundering in the Financial Sector is primarily a preventive piece of legislation the purpose of which is achieved merely by preventing money launderers from the execution of actual transactions. Although the notifications of unexecuted transactions have not been sent to the MROS, money launderers have still failed to place the funds into the financial system, which markedly limited their activities.

*France* is another good example of the risk-based system implementation. The statistical review of reported suspicious transactions for this country in the period 2005-2010 suggests continued growth in their number. What makes the French system unique and highly effective is the decline in banks' participation in the total number of reported suspicious transactions (although this number has grown from year to year). In 2010, they participated with less than 75% in the total. A marked increase in suspicious transaction reports was observed in authorised exchange offices, due to the growing trade in gold and other precious metals, which is considered a safe investment in times of economic and financial crises. Besides, the increase in this type of transactions may also be due to innovative methods and techniques of money laundering aimed at avoiding the sophisticated anti-money laundering methods employed by the banking sector.

<sup>33</sup> Articles 305 and 260 of the Federal Act on Combating Money Laundering in the Financial Sector.

An increase in the number of reported suspicious transactions has also been observed in investment firms, financial investment advisers, brokers and portfolio management companies. A clear evidence of effective implementation of the risk assessment system in France is provided in the statistics of non-financial institutions, especially notaries public, auctioneers, casinos, auditors and chartered accountants<sup>34</sup> that suggest sizeable growth of suspicious transactions. Such a statistical analysis shows that money launderers have spared no effort in finding new, innovative ways of legalization of illicitly acquired funds. On the other hand, the French example shows the high awareness and willingness to detect suspicious and illogical transactions in all areas of prevention of money laundering and terrorist financing.

A statistical analysis of the Dutch system of prevention of money laundering and terrorist financing also gives positive results. In *the Netherlands*, suspicious transactions are statistically presented in the system of prevention of money laundering and terrorist financing at two levels: at the level of cash and the level of non-cash suspicious transactions. Despite being mentioned in the Final Study as a country with a falling number of reported suspicious transactions, this fall only relates to cash transfers (which totalled 32,100 and 29,795 in 2009 and 2010 respectively).

On the other hand, an increase in the number of reported suspicious transactions, established in the statistical analysis, relates to non-cash transfers (3,453 in 2009 and 4,408 in 2010). In the category of reported suspicious non-cash transactions, the share of banks in the total number of such transactions increased by 28% in 2010 from 2009. The same is true for suspicious transactions reported by casinos and payment card companies (although their relative shares in the total remained unchanged). By contrast, reported transactions involving non-cash transfers trended downwards, particularly in freelance occupations (-14%) and companies providing money transfer services (-19%). This negative trend does not support the implementation of the risk assessment system. Taking also into account the reduced share of banks in the total number of reported suspicious cash transactions, one can conclude that money launderers trying to legalize their illicit earnings increasingly use new technologies available within the financial sector, i.e. they use all forms of fund transfer offered by the modern technology.

A statistical analysis of the data on reported suspicious transactions in *Germany* shows a similar upward trend. In the period 2008-2010, the number of reported suspicious transactions increased, not only in the financial sector but also in insurance companies, tax advising companies, casinos and especially persons involved in trade. Compared with the data on suspicious transactions in table 1, Germany demonstrates a remarkable level of awareness of all institutions involved in

<sup>34</sup> Taken from the TRACFIN (2010).

the implementation of the system for prevention of money laundering and terrorist financing, especially those in the non-financial sector.

A 22% increase in the number of reported suspicious transactions (in terms of statistics), from 9,046 in 2009 to 11,042 in 2010, was rather insignificant, because almost 20% of transactions reported in the period 2009-2010 related to transfers of illicit funds across bank accounts to third persons and the theft of personal data from email accounts<sup>35</sup>. Viewed from this perspective, the total number of suspicious transaction reports in the period 2007-2010 has not changed significantly. In other words, the application of a prevention strategy to combat money laundering and terrorist financing remained constant, with a slight increase in 2010.

The reason for such a modest increase lies entirely in the legislation. The treatment of suspicious transactions is regulated in Article 11 of the German<sup>36</sup> Act on the Detection of Proceeds from Serious Crimes, which provides that, should entities covered by the Act have grounds to believe that (regardless of the amount of a transaction) a crime pursuant to Article 261 of the German Criminal Code (money laundering) or terrorist financing has been committed or attempted, they should without delay verbally inform the competent authority thereof. In order to explain the “borderline of suspicion” in detecting suspicious transactions, the German FIU passed an opinion that covered entities must have knowledge, a suspicion or reasonable suspicion that money laundering or terrorist financing will be attempted or committed. As a result of the said explanation of Article 11 of the German Criminal Code, the number of reported suspicions transactions rose slightly in 2010.

However, all this said, and having particularly in mind the relatively small number of reported suspicious transactions, account should be taken of the fact that the German FIU is organised on the model of a police unit, which has certain consequences. Such FIUs are not suitable for direct contacts with non-financial institutions, as they are focused on investigation rather than on prevention measures. For this reason, they are constantly faced with distrust of financial institutions (notably banks), especially with regard to the categorisation of transactions that are not defined by legislation but show inconsistencies in operations. Indeed, such FIUs can be disinclined to “participate actively”, as required by financial institutions, especially in those banking systems where the banking secret has traditionally been regulated (Condemni and Pascal, 2005).

### 5.1.2.2 Serbia, Bulgaria and Liechtenstein

*Serbia* harmonised its legislation with international standards, notably the Third Directive, during 2009. Statistics on reported suspicious transactions (4,537) cle-

<sup>35</sup> For more information, see: Federal Criminal Police Office, FIU Germany Annual Report 2010; available at: [[http://www.bka.de/nm\\_195184/EN/Publications/AnnualReportsAndSituationAssessments/FinancialIntelligenceUnitFiuGermany/financialIntelligenceUnitFiuGermany\\_\\_node.html?\\_\\_nnn=true](http://www.bka.de/nm_195184/EN/Publications/AnnualReportsAndSituationAssessments/FinancialIntelligenceUnitFiuGermany/financialIntelligenceUnitFiuGermany__node.html?__nnn=true)].

<sup>36</sup> Act on the Detection of Proceeds from Serious Crimes (August, 2008).

arly point to their growth. However, it is interesting to note that the bulk of reports come from the financial sector, i.e. banks. Moreover, according to the Annual Report<sup>37</sup>, total number of reported transactions (including cash and suspicious transactions) declined from 2009.

As this paper focuses on the value of the definition of suspicious transactions, which reflects itself in practice through statistical data, it is interesting to draw a comparison between the Croatian and Serbian legislations, as their conceptions are very similar, except for the substantial difference in the definitions of suspicious transactions. Despite similarities in the development history of the anti-money laundering legislation and harmonisation with international standards, statistical data show diametrically opposed results in practice.

A comparison between the Croatian and Serbian legislations and the statistical data presented in table 1, some conclusions can be drawn with respect to the implementation of the risk assessment system. The two countries' laws on the prevention of money laundering and terrorist financing do not only bear the same name, but they are also similar in content, although in Croatia, most essential issues are regulated by subordinate legislation (regulations). Nevertheless, there are differences in the treatment of suspicious transactions. Thus, while the Croatian Anti-Money laundering and Terrorist Financing Act provides a very detailed description of a suspicious transaction, there is no definition of this concept in the Serbian law. As concerns the obligation to submit data on suspicious transactions, Article 37 of the Serbian Act only generally lays down this obligation. Moreover, as a result of alignment with international standards and acting in accordance with the provisions of the AMLTFA, Croatia introduced radical changes in the concept of and reporting on suspicious transactions as early as next year (2009). During the reference period (2005-2010), Serbia saw a continuous increase in suspicious transaction reports, suggesting that, despite the new legislation, this country preserved its former principles of operation. In other words, the normative acceptance of a risk-based system was not adequately reflected in practice.

*Bulgaria* also saw an increase in the number of reported suspicious transactions in the period 2005-2010, with a surge recorded in 2010. The number of reported suspicious transactions rose from 883 in 2009 to 1,460 in 2010 (up 60%), exclusively due to a large number of reports coming from heads of Securities Registers and monetary institutions. In the period 2005-2009, banks accounted for as much as 80% of suspicious transaction reports (only 50% in 2010). Monetary institutions participated with 35% in the total number of suspicious transactions in 2010. The numbers of reports from other financial and non-financial institutions remained below average.

<sup>37</sup> Izvještaj o radu Uprave za sprečavanje pranja novca za 2010.

The last country covered by the statistical analysis of reported suspicious transactions in the period 2005-2010 is *Liechtenstein*. It appears in table 1 as a negative example of the risk-based system application, which is not too surprising, given that it was placed on the “blacklist” of non-cooperative countries in 2000. The attitudes of some countries to Liechtenstein in this respect have not changed significantly since then. Slovenia, for example, pursuant to Article 22 and 38 of its Anti-Money Laundering and Terrorist Financing Act, has put this country on a list of countries that pose ML/TF risks. Supporting this attitude is also the fact that the FIU of Liechtenstein (a country with 34,000 inhabitants and an area of 160 square kilometres) received 261 reports on suspicious transactions (the figure relates to the period ending 1 October 2010)<sup>38</sup>. This shows that the increase in the number of reported suspicious transactions in this country, regardless of its compliance with international standards, is by no means the result of the risk-based system implementation. Otherwise, this figure would speak in favour of Slovenia’s ranking this country among the high-risk countries with respect to money laundering and terrorist financing. This is confirmed by the fact that the number of cases submitted to the competent authorities for further processing is very close to the number of reported suspicious transactions, which again equals the number of open cases at the FIU of Liechtenstein.

## 5.2 A BRIEF OVERVIEW OF ANALYSED COUNTRIES WITH REGARD TO THE RISK-BASED SYSTEM APPLICATION

As indicated in the Final Study, the upward trend in reported suspicious transactions in some of the observed countries really suggests that effective risk assessment systems are in place. Successful risk categorisation and assessment in Switzerland, France and Germany is reflected not only in a higher total number of reported suspicious transactions but also in the growing participation of the non-banking and non-financial sectors in this upward trend. However, the examples of Serbia and Bulgaria show that only one indicator, in our case the reports on suspicious transactions, is not enough evidence of the risk-based system implementation, because the statistical analyses in these countries have revealed an increase in reported suspicious transactions exclusively in the banking sector.

In Croatia, the number of reported suspicious transactions, which is obviously on the decline, also points to effective implementation of the risk-based system. This conclusion is based on the relevant legislation that provides a very detailed description of suspicious transactions, and on the active involvement of reporting entities in the prevention of money laundering and terrorist financing (through the formulation of indicators, education and, finally, being subject to penal provisions). The reports on suspicious transactions have thus gained importance and quality, as shown by the ratio between reported transactions and cases opened by the Office. However, there is still room for improvement.

<sup>38</sup> For more information, see MONEYVAL (2010).

The analyses of reported suspicious transactions for the Netherlands and Slovenia lead to several possible conclusions. Despite irregularities in reporting on suspicious transactions, (variability in the number of reports in the observed period), Slovenia shows an effective application of the risk-based system, given a low number of reported suspicious transactions that always equals the number of open cases at the Slovenian FIU. In the Netherlands, however, cash transactions are strictly separated from non-cash transactions, with a strong increase observed in suspicious non-cash transactions reported by banks, and a decline in the number of suspicious non-cash transactions reported by the non-financial sector. While these data do not corroborate the application of a risk-based system, the situation they describe can still be justified by new trends in money laundering.

Regardless of the fall in reported suspicious transactions in Ukraine and a rise in Liechtenstein, the conclusion of the reported suspicious transaction analysis for these two countries is obvious. The excessive total number of reports suggests deficiencies in several areas, from legislation through implementation in practice, which once again confirms that the number of reported suspicious transactions is an inadequate criterion for the efficiency evaluation of a risk assessment system.

To sum up, indicators of an efficient a risk-based system application must be sought in multiple areas, separately analysing each particular system for prevention of money laundering and terrorist financing, from the development of legislation to practical measures taken by each individual country.

## 6 CONCLUSION

Taking into account all efforts to define an effective money laundering prevention system based on risk assessment, comprehensive statistical data, as a reflection of practice, support the following conclusions:

- An effective risk assessment system requires an appropriate legal framework including a detailed definition of suspicious transactions, efficient supervision and appropriate sanctions in the cases of non-compliance with regulations.
- A risk assessment system requires that an increasing portion of suspicious transactions be reported by non-financial institutions as evidence of raising awareness in this sector.
- There is a need for ongoing education of all institutions involved in the implementation of anti-money laundering and terrorist financing measures at the national level.

These conclusions have also been supported by the previous statistical analysis of ten countries based on the criterion of an increase vs. decrease in the number of reported suspicious transactions. The effectiveness of a risk assessment system cannot be measured by the number of reported suspicious transactions. While in some countries, such as Switzerland, France, Germany and the Netherlands, such

an increase provides evidence of an effective risk assessment system being in place, in others, like Serbia, Bulgaria and Liechtenstein, it proves quite the opposite, even taking into account the organisational differences among the national FIUs.

Similarly, a fall in reported suspicious transactions in Croatia, Slovenia or Romania does not mean inadequate application of the risk-based system. On the contrary, by harmonising their respective legislations with the international money laundering and terrorist financing standards, these countries have proved their willingness to reduce the number of reported suspicious transactions, while ensuring high quality of their content.

The above analysis clearly demonstrates that informed decisions on a customer's behaviour or on an executed transaction can only be made on the basis of comprehensive legislation, ongoing education, an up-to-date perception of risks and, finally, learning on errors.

It follows that the development of any system, including the risk-based system, requires a wide range of information sources and thorough processing of information, as well as a long-standing practice, in order to ensure the best possible interpretation of collected information and its categorisation. The application of such a system provides a basis for further development of operational policies and procedures, while improving the system in order to successfully respond to new challenges on a daily basis.

## REFERENCES

1. Act on the Detection of Proceeds from Serious Crimes, August 2008 (Germany). Available at: <[http://www.bka.de/nn\\_194638/SharedDocs/Downloads/EN/Subjects\\_\\_A\\_\\_Z/FIU/moneyLaunderingAct2008.html?\\_\\_nnn=true](http://www.bka.de/nn_194638/SharedDocs/Downloads/EN/Subjects__A__Z/FIU/moneyLaunderingAct2008.html?__nnn=true)>.
2. Cindori, S., 2008. Organizacija financijsko-obavještajnih jedinica za sprječavanje pranja novca. *Hrvatska javna uprava*, 8(1), pp. 171-203.
3. Cindori, S., 2010. *Sustav sprječavanja pranja novca*. Zagreb, Faculty of Law.
4. Condemi, M. and De Pascal, F., 2005. *International profiles of the activity to prevent and combat money laundering*. Roma: Ufficio italiano dei cambi.
5. Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering.
6. Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering
7. Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.
8. FATF, 2007. *Guidance on the Risk-Based Approach to combating money laundering and terrorist financing*. Paris: Financial Action Task Force.
9. FATF, 2012. *Methodology for Assessing Compliance with the FATF 40 Recommendations and the FATF 9 Special Recommendations*. Paris: Financial Action Task Force.
10. Federal Criminal Police Office, 2010. *Annual Report 2010* [online]. Available at: <[http://www.bka.de/nn\\_195184/EN/Publications/AnnualReportsAndSituationAssessments/FinancialIntelligenceUnitFiuGermany/financialIntelligenceUnitFiuGermany\\_\\_node.html?\\_\\_nnn=true](http://www.bka.de/nn_195184/EN/Publications/AnnualReportsAndSituationAssessments/FinancialIntelligenceUnitFiuGermany/financialIntelligenceUnitFiuGermany__node.html?__nnn=true)>.
11. Federal Office of Police, 2010. *Annual report 2010* [online]. Available at: <<http://www.fedpol.admin.ch/content/fedpol/en/home/dokumentation/berichte/geldwaescherei.html>>.
12. Final Study on the Application of the Anti-Money Laundering Directive, Service Contract ETD/2009/IM/F2/90, 2009, Brussels, European Commission DG Internal Market and Services – Budget.
13. Government Decision no. 594/2008 on the approval of the Regulation for application of the provisions of the Law no. 656/2002 for the prevention and sanctioning money laundering as well as for instituting of some measures for prevention and combating terrorism financing acts (Romania).
14. Graham, T., Bell, E. and Elliott, N., 2006. *Money Laundering*. Wiltshire: Butterworth-Heinemann.
15. Heršak, G., 1993. Pranje novca i policija. *Policija i sigurnost*, 1(1-2), pp. 3-4.



16. Law no. 656 of December 7th, 2002 on the prevention and sanctioning of money laundering and on setting up of certain measures for the prevention and combating terrorism financing, consequently amended and completed (Romania).
17. Law of Ukraine on Prevention and Counteraction to Legalization (Laundering) of the Proceeds from Crime or Terrorist Financing as of 18 May 2010, no 2258 [online]. Available at: <[http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/progress%20reports/MONEYVAL\(2010\)1\\_ProgRep\\_UKR\\_en.pdf](http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/progress%20reports/MONEYVAL(2010)1_ProgRep_UKR_en.pdf)>.
18. Main elements related to National Office for Prevention and Control of Money Laundering's activity, performed within the year 2010, Synthesis of the activity report. Bucharest.
19. Ministastvo za finance Republike Slovenije. *Poročilo o delu Urada Republike Slovenije za preprečevanje pranja denarja za leto 2010* [online]. Available at: <[http://www.uppd.gov.si/si/delovna\\_podrocja/podatki\\_o\\_delu\\_urada/](http://www.uppd.gov.si/si/delovna_podrocja/podatki_o_delu_urada/)>.
20. Ministry of Finance of RC. *Annual Reports of Ministry of Finance, 2009-2010* [online]. Available at: <<http://www.mfin.hr/en/annual-reports-of-ministry-of-finance>>.
21. Mitsilegas, V., 2003. *Money Laundering Counter-Measures in the European Union: A New Paradigm of Security Governance Versus Fundamental Legal Principles*. The Hague: Kluwer Law International.
22. MONEYVAL, 2010. *Izveštaj o radu Uprave za sprečavanje pranja novca za 2010* [online]. Available at: <[http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/progress%20reports/MONEYVAL\(2010\)33ProgRep-SRB\\_en.pdf](http://www.coe.int/t/dghl/monitoring/moneyval/Evaluations/progress%20reports/MONEYVAL(2010)33ProgRep-SRB_en.pdf)>.
23. MONEYVAL, 2011. *Croatia: Progress report and written analysis by the Secretariat of Core Recommendations* [online]. Available at: <<http://goo.gl/WZRq7>>.
24. Pravilnik o obavješćivanju Ureda za sprječavanje pranja novca o sumnjivim transakcijama i osobama, NN 1/09. Zagreb: Narodne novine.
25. Richards, J., 1998. *Transnational Criminal Organizations, Cybercrime, and Money Laundering: A Handbook for Law Enforcement Officers, Auditors and Financial Investigators*. Florida: CRC Press LLC. doi: 10.1201/9781420048728
26. Savona, E., 2004. *Responding to Money Laundering: International Perspectives*. London: Harwood Academic Publishers.
27. The Federal Act on Combating Money Laundering in the Financial Sector (Anti-Money Laundering Act) of 10 October 1997 (Switzerland).
28. TRAFICIN, 2010. *Rapport d'activité 2010*. Montreuil-sous-Bois cedex, France [online]. Available at: <<http://www.sacem.fr/cms/home/la-sacem/rapports-activite>>.

29. Uredba o unutarnjem ustrojstvu Ministarstva financija, NN 29/09. Zagreb: Narodne novine.
30. Zakon o sprečavanju pranja denarja in financiranja terorizma, Ur. l. RS 60/07, 47/09, 48/09, 19/10 and 77/11. Ljubljana: Uradni list.
31. Zakon o sprečavanju pranja novca i finansiranja terorizma, Službeni glasnik RS, 20/09, 72/09 and 91/10.
32. Zakon o sprječavanju pranja novca i financiranja terorizma, NN 87/08. Zagreb: Narodne novine.
33. Zakon o sprječavanju pranja novca, NN 69/97, 106/97, 67/01, 114/01, 117/03 and 142/03. Zagreb: Narodne novine.