Otakar Schlossberger et al.

ANTI-MONEY LAUNDERING

Vysoká škola finanční a správní, o.p.s.

www.vsfs.cz

Otakar Schlossberger et al.

Anti-Money Laundering

EUPRESS
Vysoká škola finanční a správní

SCHLOSSBERGER, Otakar et al. *Anti-Money Laundering.* Project identification code VG20122014087. First edition. Prague: Vysoká škola finanční a správní, 2014. 115 p. EUPRESS. ISBN 978-80-7408-094-4.

AUTHORS OF INDIVIDUAL CHAPTERS:
Head of the authors' collective:

JUDr. Ing. Otakar Schlossberger, Ph.D.	Chapter 1 Chapter 2, Sections 2.1, 2.3, and 2.4 Chapter 3, Sections 3.1, 3.2, and 3.9 (co-author) Chapter 4, Section 4.1; and Chapter 5 (co-author) Executive Summary
Ing. Naděžda Blahová, Ph.D.	Chapter 2, Section 2.2.
Assoc. prof. Ing. Jaroslav Brada, Ph.D.	Chapter 3, Section 3.4
Ing. Josef Budík, CSc.	Chapter 3, Sections 3.5 and 3.6
JUDr. Michaela Katolická	Chapter 4, Section 4.2
Ing. Petra Korbasová	Chapter 3, Section 3.3
Assoc. prof. Ing. Vladislav Pavlát, CSc.	Chapter 3, Sections 3.7 and 3.8
Dr. Ján Šugár, CSc.	Chapter 3, Section 3.9 (co-author)
JUDr. Adriana Vavrušková	Chapter 4, Section 4.3, and Chapter 5 (co-author)

REVIEWERS:
Assoc. prof. Ing. Karel Havlíček, Ph.D., MBA
Assoc. prof. PhDr. Petr Teplý, Ph.D

EDITOR:
Assoc. prof. Ing. Milan Kašík, CSc.

Issue the monograph was approved by editors of scientific publishing.

All rights reserved. No part of this publication may be reproduced and used in electronic form, copied and recorded without the prior written consent of the publisher.

© 2014 Otakar Schlossberger et al.
© 2014 Vysoká škola finanční a správní, o.p.s.

ISBN 978-80-7408-094-4

This book has been prepared as part of the project of the Ministry of the Interior of the Czech Republic implemented by Vysoká škola finanční a správní, o.p.s. (University of Finance and Administration), Department of Finance, entitled ***"Increasing the effectiveness of procedures and measures for detecting legalization of the proceeds from crime and preventing the financing of criminal structures within the sector of the financial service providers"*** (project identification code VG20122014087, with total support of CZK 2,238 thousand). The leading author would like to thank all co-authors for their cooperation in establishing the concept of this publication and for preparing the relevant chapters hereof. The entire monograph forms an important project output and represents a source of suggestions for potential amendment of regulations and discussion *de lege ferenda*.

Table of Contents

List of abbreviations

AML	Anti-Money Laundering
AML/CFT	Anti-Money Laundering/Combating the Financing of Terrorism
ASPI	Automated System of Legal Information
ATM	Automated Teller Machine
BIS	Security Information Service (Bezpečnostní informační služba)
CERTIS	Czech Express Real Time Interbank Gross Settlement system
CFT	Counter-Terrorism Financing
CNB	Czech National Bank
EC	European Community
EU	European Union
FATF	Financial Action Task Force
FSB	Financial Stability Bureau
FSRB	FATF-Style Regional Body
FAU	Financial Analytical Unit of the Ministry of Finance of the Czech Republic
GDP	Gross domestic product
HW	Hardware
KYC	Know Your Customer
MoF CR	Ministry of Finance of the Czech Republic
ML/TF	Money Laundering/Terrorism Financing
OPDP	Office for Personal Data Protection
PEP	Politically exposed person
RBA	Risk Based Approach
ROP	Regional operational program
SEC	Securities Exchange Commission
SIFI	Systemically important financial institution
SW	Software
VŠFS	University of Finance and Administration (Vysoká škola finanční a správní)

1. Introduction

Various efforts aimed at legalizing unlawfully received values (e.g. money, but formerly also other units of value) are as old as mankind. To receive any assets, which could generate certain benefits fulfilling immediate or deferred needs of an individual – this has been an objective of a certain group of people within a society that consider such activities as implied. Alternatively, they have been aware of the fact they do something that had initially violated the morals of the given society they lived in; however, they were at peace with doing so. They were also prepared for a situation that their immoral activities might be exposed; they would then be willing and able to protect themselves in any manner whatsoever, albeit improper or even antisocial. Similar activities associated with efforts aimed at legalizing unearned assets carried over to the present. Moreover, various ways, methods, and practices of legalizing the proceeds from crime have been improving.

In case we apply the process of legalizing illegally generated assets to the area of financial services, and particularly banking, then the efforts aimed at the detection/exposure of such process are even more important. As stated by prof. Polouček[1]: "One of the possible ways of minimizing the room for illegal banking practices consists in establishing the simplest, transparent, and homogeneous banking system possible. It must comprise clear and uniform rules, with unambiguous, uniform, and as simple as possible regulation and protection…". Obviously, the aforementioned thesis is something we have to more than agree with; however, it may be supplemented with another thesis that is valid as well in the view of the authors of this publication. The point is that professional entities operating within the financial sector, particularly in banks, savings and credit cooperatives, payment institutions, insurance companies, and securities traders, need to be sure who their clients are and why, and what transactions are carried out with the given entity. The most crucial factor for successful legalization of the proceeds from crime[2] is the rapid capitalization thereof; this particularly concerns operational transfers of funds from one institution to another, i.e. specifically, for example, from an entity aiming to unlawfully gain cash funds from an ordinary client's accounts to another, etc. On the one hand, banks and other payment transaction/payment services procurers (as appropriate) try to expedite cash transfers in terms of applicable legal regulations[3] and in compliance with the relevant data formats, on the other hand, other applicable regulations (to be discussed later in the text) require such entities to dedicate sufficient time to the verification regarding the transfer/other transaction rightfulness and properly identify or examine their clients.

This activity is very demanding and is also affected by a number of subjective factors. One of the key factors is the human capital factor. Banks and other financial institutions employ people, who should be duly instructed, trained, and checked to ensure they are able to detect any activities of their clients that contradict not only applicable laws, but also morals and public order of the given society. This is such a subjective approach to cognition of people that it may only be required from them with extraordinary efforts made, combined with professional practice of the given individuals, their experience, and theoretical knowledge.

The submitted monograph should, at least to some degree, contribute to the fact that people, who are professionally engaged in the area of financial transactions or the analysis / implementation thereof,

---

1 POLOUČEK, S. et al. *Bankovnictví*. 2nd Edition. Prague: C. H. BECK, 2013. 480 pp. ISBN 978-80-7400-491-9, p. 393.

2 Any activity that is impeachable is illegal. However, it is safe to say that not every illegal activity must be in fact impeachable, as it may only be immoral or contrary to public order.

3 For example, Regulation (EU) No. 260/2012 of the European Parliament and of the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No. 924/2009, or Act no. 284/2009 Coll., on the Payment system.

gain new knowledge relating to the detection/exposure of efforts aimed at legalizing various assets, particularly in banks, but also in other financial institutions. The text of the book is composed of opinions, ideas, and facts provided by individual authors.

The whole monograph is divided into several sections. The first chapter, which is more general, mainly addresses legal issues associated with the legalization of the proceeds from crime and terrorism financing. It is partly written in a historical context of the legal development regulation within the territory of the Czech Republic and it partly addresses issues of potential legal changes. Such changes may take place for various reasons. One of the key reasons today is the requirement for transposition obligations arising from the membership of the Czech Republic in the European Union (hereinafter the "EU"). However, the area of anti-money laundering (hereinafter the "AML") is regulated not only by the laws of the EU, but also within a wider international context. Furthermore, it is necessary to take into account supranational activities of the Financial Action Task Force (hereinafter the "FATF") (see below). The aforementioned facts apply to all financial institutions, across the financial market in its entirety. This is the case for the most part of this publication.

The second section of the presented text will deal with more practical issues of the entire process involving various efforts aimed at legalizing the proceeds from crime. Practical issues of the "know your customer" process - to a point where we can actually say we truly know our client within financial institutions – will mainly focus on the area of banking; however, this also applies to the insurance industry or capital markets. In this section, readers will be presented with the results of research carried out by a team of the University of Finance and Administration as part of the project of the Ministry of the Interior of the Czech Republic implemented by Vysoká škola finanční a správní, o.p.s. (University of Finance and Administration), Department of Finance (hereinafter "VŠFS"), entitled "Increasing the effectiveness of procedures and measures for detecting legalization of the proceeds from crime and preventing the financing of criminal structures within the sector of the financial service providers". The research took place in the form of a questionnaire survey in various types of financial institutions within the financial market sector. It involved not only the key financal market playrs, such as banks, insurance companies, or securities traders, but also inquired investment funds or savings/credit cooperatives, for example. In this section, the monograph will bring an evaluation of the entire research and formulate certain conclusions arising therefrom. Furthermore, this section will also feature many charts and their explanations.

In the next section, which is no less important, the book will examine potential changes in the area of combating the legalization of the proceeds from crime and terrorism financing – specifically from the perspective of implementation of some international requirements. This section will directly follow up on the first technical part of the publication that deals with legal issues of the AML process. In this chapter, authors will also deliberate on what processes would need to be implemented or perfected to ensure suitable application of the foreseen changes and requirements. As part of the above mentioned project, VŠFS organized a workshop relating to "Risk Based Approach" (hereinafter the „RBA"), where FATF requirements arising from the revised version of the so-called 40 recommendations (to be further discussed in more detail) were presented. Some ideas and conclusions of the workshop have been summarized in this part of the monograph.

The AML process may be viewed as a very important activity, particularly in the area of financial markets. It particularly comprises the area of banking, even specialized financial institutions, such as building societies and/or investment banks, but also insurance companies, pension companies, securities traders, payment institutions, etc. Therefore, we believe the presented publication will contribute not only to clarification of the given problem area, but mainly to deliberations and actions that would facilitate this demanding process of detecting various efforts of legalizing unlawfully received funds. The objective of all participating authors was as follows: the publication should contribute to creating, fi-

nalizing, modifying, or adapting existing methodology procedures of various financial institutions and provide new approaches following the revision thereof. Naturally, the entire area of AML is regulated by generally binding legal regulations, which will also be discussed; however, there were efforts of finding further room for their improvement within the above mentioned project. Nevertheless, the legislative process is tedious, too distant and complex – particularly for entities without any direct legislative competence. In particular, it is complicated to enforce the given idea, though it had been discussed during specialized workshops, symposiums, or conferences. However, the authors believe they will succeed in this area as well.

As mentioned above, the presented monograph is one of the outputs of the applied research project and the output of the research conducted by a solver´s team that was represented by the team of authors. This monograph was based on general requirements for the research knowledge. For that reason, partial questions of AML processes were processed through the methods of induction, deduction and comparison. Besides these methods, the method of analysis was applied as well. The research method also worked with the hypothesis based on the argument whether „the current level of the identification of people communicating with financial institutions is sufficient or not". The research methods have to either rebut this hypothesis or to confirm it. Conclusions or possible orientation of the application of processes and phenomena in the area of enhanced efficiency of procedures and measures when uncovering the legalization of profits from punishable offence and preventing the funding of criminal groups in the area of providers of financial services are included in this monograph.

2. Legal aspects of the process of combating the legalization of the proceeds from crime and terrorism financing

2.1 Introduction

This section focuses on legal norms and institutions associated with/involved in combating the legalization of the proceeds from crime, specifically with combating money laundering, both nationally and internationally. It clarifies and explains the entire AML process, its individual steps, as well as the likelihood of detecting this type of crime during individual stages of the process. It addresses the sources of international law and institutions that are – considering the nature of the activity - crucial for successful prevention of the legalization of the proceeds from crime. Moreover, it also deals with the evolution of anti-money laundering activities in the Czech Republic. It is an introduction to the problem area, which, in a way, summarizes existing general resources.

The end of this section dedicated to legal aspects of combating the legalization of the proceeds from crime will address one sensitive, yet very important area– one of the basic obligations imposed on obliged entities foreseen by the law governing the AML process - i.e. the identification obligation. With regard to the aforementioned issues, the given section will examine the process of accepted identification for institutions that do not have to maintain any accounts and only act as middlemen for the given transactions.

2.2 AML process in the legal context

Long gone are the times when money laundering was associated with the legalization of the proceeds generated solely from illegal drug trade, prostitution, or extortion. A crime that generates illegal revenue, which is to be legalized (laundered), may be any crime, including corruption, frauds, tunneling/expropriation, and tax evasion, for example.

The term legalization of the proceeds from crime refers to any actions that lead to covering illegal origin of any proceeds from crime. Such actions are characterized by efforts that are to make such proceeds appear legal, i.e. generated/acquired in compliance with applicable legal regulations. This process is often referred to as "money laundering", where the term "money" should be viewed in a broad sense, i.e. as any proceeds or assets from committed crimes (e.g. real estate, securities, precious metals and stones, items with cultural value, etc.).

As suggested by the term "process", money laundering is an activity that takes place within a specific period of time, during which three basic steps occur. These steps are generally referred to as "stages" of legalization of the proceeds from crime; it specifically concerns the following stages: allocation – layering – utilization.

The first step – allocation – comprises activities that consist in gradual allocation of mainly cash funds generated from committed crimes within the financial system, which is characterized by movement of financial funds through execution of financial transactions. During this stage, institutions that offer and enable the allocation of such funds into the financial system play a key role. This is where such institutions (so-called obliged entities) have an absolutely irreplaceable role relating to the prevention of the legalization of the proceeds from crime – i.e. not only a number of measures that are to detect or complicate the money laundering process, that enable to drain such illegally acquired funds, and – last but not last, that lead to collecting and archiving of data on transactions and persons executing such transactions.

During the second stage of the money laundering process, a large number of various transactions are carried out using the funds that had been allocated within the financial system for the purpose of their legalization. The objective for executing such transactions across various financial institutions of the global financial system is to complicate the identification of or completely cover up the origin of the funds being "laundered". This stage very often involves intermingling of legal funds with proceeds from crime, and this is the fulfillment of the second step called layering.

As suggested by the name of the third stage of the money laundering process, utilization, the objective is to utilize the "laundered" proceeds from crime by the people, who had committed such crimes, not only to satisfy their own needs, but also to commit further crimes.

The likelihood of detecting the legalization of the proceeds from crime is the highest during the first stage. The likelihood significantly drops during stage two and stage three.

Since considerable share of financial funds of criminals enters the financial system through financial institutions and since the likelihood of detecting the legalization of the proceeds from crime is the highest during the stage of allocation of such funds within the financial system, the key players in the area of application of preventing measures shall mainly be financial service providers. The basic obligations of such entities as well as other "obliged entities" in the area of preventing the legalization of the proceeds from crime are imposed by Act no. 253/2008 Coll., on Selected measures against legalization of proceeds from crime and financing of terrorism.

The prevention of the legalization of the proceeds from crime definitely has an international dimension and may only be successful if individual states, their legal systems, and individual obliged entities proceed together and on a coordinated basis in detecting and combating the legalization of the proceeds from crime. This serves as the basis for activities of the relevant international institutions and bodies, which undoubtedly include, for example, the FATF, the Egmont Group, and, last but not least, various activities of the relevant bodies and committees of the EU. The objective is to set certain minimum standards for combating the legalization of the proceeds from crime and, at least since 2001, also for combating the terrorism financing, and to delegate to individual countries and their governments the obligation for their practical implementation and compliance.

The most effective measures of the prevention of money laundering mainly include the draining of such funds from criminals and establishment of suitable conditions for detecting the legalization of the proceeds from crime, including the requirements for archiving information about clients (persons, in whose names accounts are maintained or on whose behalf transactions were executed) and executed transactions.

Sources of international law

The FATF is an intergovernmental body founded in 1989 by ministers of member countries. The objective of the FATF is to set down measures for combating money laundering and terrorism financing and promote their effective implementation in practice. The FATF issues many Recommendations, deemed as recognized international standards for combating the legalization of the proceeds from crime, terrorism financing, and proliferation of weapons of mass destruction. First standards were already issued in 1990; in 2001, they were supplemented with the so-called Nine Special Recommendations on Terrorist Financing.

The basic FATF Recommendations, which should be implemented by individual countries, comprise:

- Measures aimed at identifying risks;
- Prosecution of the legalization of the proceeds from crime, terrorism financing, and proliferation of weapons of mass destruction;
- Implementation of preventive measures in the financial sector and other specified sectors;
- Establishment of rights and obligations within the system of laws;
- Promoting transparency and availability of information on beneficial owners;
- Implementation of steps that would facilitate international cooperation.

The latest amendment to the FATF Recommendations took place in February 2012, with the particular focus on risk assessment with a view to potentially apply the risk based approach (for more details, see Chapter 4). The principle of the approach consists in the implementation of steps that allow each country to properly identify, assess, and comprehend the risk of money laundering/terrorism financing, to which it is exposes, and subsequently adopt adequate measures aimed at eliminating such risks. Therefore, the risk based approach will allow each entity to adopt measures that would target the minimization of specific identified risks and that would be adequate to the nature of such risks. The risk based approach thus should contribute to effective investment of funds and effort.

Another feature of the amendment to the FATF Recommendations of February 2012 is the change relating to the incorporation of some of the original "nine FATF Recommendations on Terrorist Financing in the recommendations on combating money laundering. This change has not affected Recommendations that apply solely to combating terrorism financing (Recommendation 5, 6, and 8). New Recommendation no. 7 was issued as part of the amendment to the Recommendations, relating to the financing of weapons of mass destruction; it mainly deals with the implementation of specific financial sanctions declared by the UN.

The FATF is also engaged in the area of assessing the compliance with the given standards by its members and, through the Moneyval Committee - also a member of the FATF, oversees the assessment of individual Moneyval Committee member states (including the Czech Republic, among others). This contributes to increasing the level of measures adopted and implemented by individual countries with a view to combat the legalization of the proceeds from crime, terrorism financing, and recently also the proliferation of weapons of mass destruction. In 2011, the 4th round of the peer assessment took place in the Czech Republic. Compared to the 3rd round, the rating of the Czech Republic increased by two points in eight cases and by one point in one cases; the rating was only decreased in three cases.

The European Parliament and the Council of the European Union are bodies of the EU that endorse the enforcement of efficient and effective policy in the area of combating the legalization of the proceeds from crime and terrorism financing. They are actively involved in preparing and enforcing such policy, promoting compliance with the set standards by individual member states, including the performance of inspection[4] focused on the compliance with imposed obligations.

4 For more information on links to the financial market supervision, see, for example, BLAHOVÁ, Naďa. Změny regulačního a dohledového rámce finančních trhů v Evropské unii. *Český finanční a účetní časopis*, 2010, Vol. 5, No. 2, pp. 42–51. ISSN 1802-2200. (Changes to the regulatory and supervision framework of financial markets in the European Union).

The most important materials of the two institutions are as follows:

- Directive 2005/60/EC of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing;
- Commission Directive 2006/70/EC;
- Regulation (EC) No 1889/2005 on controls of cash entering or leaving the Community;
- Regulation (EC) No 1781/2006 on information on the payer accompanying transfers of funds.

Directive 2005/60/EC of the EP and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (so-called 3rd Money Laundering Directive) defined the (now) key terms and obligations for obliged entities, including the basic contents thereof. This mainly concerns the client due diligence process and the performance thereof, client due diligence/simplified due diligence, specification of obligations in the area of fulfillment of obligations by third parties, notification of suspicious transactions, etc.

Commission Directive 2006/70/EC set down, among others, the definition of a politically exposed person and defined technical criteria for simplified customer due diligence procedures and for exemption on grounds of financial activities, which are subject to AML/CFT regulation, conducted on an occasional or very limited basis (e.g. hotel exchange office).

Regulation (EC) No 1889/2005 on controls of cash entering or leaving the Community imposes obligations on individuals, who shall – upon entering or leaving the European Community - notify the customs authorities of any imports/exports of legal tender, checks, money orders, securities, or any other investment instruments with the total value exceeding EUR 10,000.

Regulation (EC) No 1781/2006 on information on the payer accompanying transfers of funds sets down requirements for the scope of information, which must accompany transfers of funds, and defines the range of transfers, to which such obligation applies. The scope of information that must accompany transfers of funds is differentiated for transfers carried out within the EC only (simplified scope) and for transfers carried out from the EC outside of the EC (so-called complete scope of information on the payer).

Evolution of the prevention of money laundering in the Czech Republic

The first legal regulation that set down obligations relating to the prevention of the legalization of the proceeds from crime was Act no. 61/1996 Coll., on Selected measures against the legalization of proceeds from crime, which came into effect on 1 July 1996. On the same date, the Financial Analytical Unit of the Ministry of Finance of the Czech Republic was formed, mainly responsible for accepting and analyzing reports on suspicious transactions. The Ministry of Finance of the Czech Republic also issued Decree no. 183/1996 Coll., setting down technical parameters of the notification of suspicious transactions.

This started a new stage in the prevention of money laundering, which had previously been ensured by the Police of the Czech Republic, specifically by the Service for Detection of Corruption and Substantial Economic Activity, which; however, did not have any special authority with regards to financial institutions. The abovementioned Act has been subject to several amendments, with the amendment of 2000 being one of the more significant ones, already executed on the basis of experience obtained in application of obligations set down by the original Act.

In 1997, the multilateral Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (so-called Strasbourg Convention) of 1990 came into effect in the Czech Republic; it contributed to improving the effectiveness of prevention of money laundering by allowing information exchange on investigated entities between partnership financial units of signatories.

Act no. 254/2004 Coll., on Restriction of cash payments, the amendment of which is currently being prepared[5], also plays an important role in combatting money laundering. The fundamental idea behind the regulation of cash payments remains unchanged. Only some partial elements of the regulation change with a view to eliminate imperfections in the wording of the original Act. A cash payment would newly refer to any factual flow of cash between two entities, irrespective of the legal grounds for such flow (originally, a cash payment only referred to the settlement of a liability – i.e. provision of a loan/credit was not considered a cash payment). The Act should also newly apply to payments executed by Czech entities abroad, which should prevent evasion of the Act by executing cash payments outside of the territory of the Czech Republic (whether really or fictitiously). Significant intensification of the cash payment regulation also consists in the fact that the limit of CZK 350,000 (maximum amount that may be transferred by means of a cash payment) will apply to any 28 consecutive days – and not to a single calendar day, as has been the case, since it was possible to simply divide any cash payments exceeding CZK 350,000 into several payments executed on the required number of consecutive days.

In connection with the implementation of the relevant regulations of the European Communities, particularly the so-called 3rd Money Laundering Directive No. 2005/60/EC of 2005, Act no. 253/2008 Coll., on Selected measures against legalization of proceeds from crime and financing of terrorism, was adopted in the Czech Republic, with the effective date of 1 September 2008. This Act had fully implemented the requirements of the 3rd Money Laundering Directive of the EC, thereby resulting in compliance of the national law with the requirements of the law of the European Communities (and within the required period of time).

An amendment to the Act, which reduced the limit for general obligation to identify clients to EUR 1,000, mainly introduced changes in the area of identifying clients, because it enabled the use of new form of client identification, e.g. acceptance of identification, not permitted by the previous regulation at all. The amended wording also set down new obligations in terms of the key client due diligence, review of the sources of financial funds, and also introduced exceptions to client identification and due diligence in cases foreseen and specified by the Act. The definition of a politically exposed person and the imposition of obligations that must be met in entering into transactions or business relations with politically exposed persons were also new. Furthermore, the amendment to the Act also reduced the ban on the disclosure of information on submitted notifications of suspicious transactions between related parties, with a view to ensure more attention for other transactions of such clients. With regard to banks and similar institutions, the amendment set down explicit ban on correspondence dealings with "shell banks" and banks that promote their activities. Last but not least, the amendment defined the term beneficial owner and broadened examples of suspicious transactions.

On the same date, i.e. 1 September 2008, Decree no. 281/2008 Coll., on certain requirements for the system of internal rules, procedures and control measures against the legitimization of the proceeds of crime and financing of terrorism, came into effect; it governs obligations relating to client due diligence, risk assessment and management, and internal control applicable to entities that are subject to the supervision of the CNB.[6]

The Decree of the CNB was issued in compliance with the enabling provision of Act no. 253/2008 Coll., specifically to procedures for performing client due diligence and determining the scope of the client due diligence process corresponding to the risk of legalization of the proceeds from crime and terrorism financing depending on the client type, business relation, product or transaction, and also adequate and suitable methods and procedures for risk assessment and management, internal control, and ensuring control over compliance with the obligations set down by Act no. 253/2008 Coll.

5 At the turn of 2013 – 2014.

6 In compliance with Act no. 253/2008 Coll., the CNB acts as the authority for administrative supervision over the fulfillment of obligations set down by the Act for obliged entities supervised by the CNB.

Act no. 69/2006 Coll., on Implementation of international sanctions, which is a general and procedural regulation for the area of international sanctions, has a crucial role in the area of terrorism financing prevention. It does not set down sanctions for specific entities – such sanctions are determined on its basis. The following international sanctions are legally binding in the Czech Republic: sanctions imposed by a Government Regulation issued on the basis of Act no. 69/2006 Coll., and also regulation issued on its basis (Government Regulation no. 210/2008 Coll., regarding the implementation of special measures in the fight against terrorism, as amended by Government Regulation no. 88/2009 Coll.), and sanctions imposed by directly applicable legal regulations of the EU, issued by competent bodies of the EU, and published in the Official Journal of the EU.

Financial Analytical Unit

The Financial Analytical Unit (hereinafter the "FAU") was formed in 1996, as a financial intelligence unit of administrative type, attached to the MoF CR. The key objective of the FAU is to accept and analyze notifications/reports on suspicious transactions, and file criminal complaints in case of a suspected crime. In order to fulfill its obligations, the FAU has a number of powers (request for information from obliged entities, blocking of transferred financial funds, inspection rights, etc.) and cooperates with a number of state administration authorities (General Directorate of Customs, financial administration authorities, tax authorities, etc.).

Other important tasks of the FAU comprise: performance of inspections of the compliance with obligations set down by Act no. 253/2008 Coll. at obliged entities, ensuring international cooperation with foreign partners, and legal activities in the area of preventing the legalization of the proceeds from crime and terrorism financing, including the provision of methodological standpoints. The FAU also acts as a coordinator for the area of international sanctions and exceptions to such sanctions. The performance of the aforementioned obligations, rights, and responsibilities is also reflected in the internal structure of the Unit, comprising international, analytical, inspectional, and data collecting and processing departments.

Evaluation

The term money laundering is well known; however, people are usually less familiar with the enormous risk these activities represent for the stability of the financial sector and the economy as a whole. This problem area, which has special significance for the entire society, must be adequately legally regulated. The nature of the money laundering activities requires legal regulation on the supranational level, whereas the legal regulations of individual countries must also be very sophisticated. The Czech Republic fell behind slightly in this area during the initial stage of its transformation; however, it is currently safe to state that the relevant institutions are successfully applying demanding requirements imposed by legal regulations. Moreover, integration of our experts within working groups, which are being formed on the supranational level at key institutions involved, has been exemplary.

2.3 Accepted identification and remote identification

Definition of the problem

The area of client identification was covered in the publication Know your customer – from general perspective in Chapter 2.2 and from special perspective in Chapter 3.3[7]. In this context, the given problem area will be further supplemented with opportunities and deliberations regarding the legal interpretation of accepted identification or its application by selected institutions.

Accepted identification has been adopted by the Czech legal regulation from the so-called 3rd Money Laundering Directive of the EU, published as Directive 2005/60/EC of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. Specifically, the accepted identification is described in Sections 11(1) through (3) of Act no. 253/2008 Coll., on Selected measures against legalization of proceeds from crime and financing of terrorism. The remote identification process is then described in Section 11(4). Furthermore, the Act specifies situations, when it is not necessary to identify clients (Sections 13(1) through (3)), as well as provisions specifying exceptions to client identification (Section 13(4)). We should also note that the given problem area is not subject to an interpretation or interpretation standpoint; however, the FAU[8] or the CNB, as appropriate, has been involved in the interpretation of the Act and its provisions.

Accepted identification and associated issues

The first area that may be underlined within the existing legal regulation is the possibility to use accepted identification. In practice, this means that identification has already been performed by another obliged entity and the third party thus assumes, in good faith, that its subject – client – has undergone proper identification process within the original entity. The obliged entities authorized to use the accepted identification are clearly specified in Sections 2(1)(a) and (b) of the Act. It mainly concerns banks and savings/credit cooperatives (so-called credit institutions) and also entities referred-to by the Act as financial institutions. This concerns, for example, entities with a license to provide investment services with the exception of investment intermediaries, investment companies, investment funds, pension companies, pension funds, payment institutions, providers of small extent payment services, electronic money institutions, issuers of electronic money of small extent, entities authorized to provide leasing, guarantees, credit or loans, entities authorized to broker savings, leasing, credit or loans, insurance or re-insurance companies, insurance agents or insurance settlement agent performing activities related to life insurance, persons licensed to perform foreign currency exchange pursuant to the Foreign Exchange Act, and other entities/persons. It is apparent from the aforementioned that accepted identification may be used by a number of entities. Considering the aforementioned, the author will use the term "financial institutions" to refer to all of the above mentioned entities for the remainder of this section.

At the first glance, it may appear that the acceptance of client identification for the needs of financial institutions is very beneficial for clients, as they do not have to undergo the entire identification procedure – although it is not too demanding for clients. Identification elements in terms of the provisions of Section 8(2) may be corroborated very easily. Individuals simply present their identity

7 KYNCL, Libor a kol. Poznej svého klienta – základní zásady finančního práva. 1st Edition, Brno: ACTA UNIVERSITATIS BRUNENSIS, IURIDICA, 2012. No. 433. 165 pages. ISBN 978-80-210-6085-2. (Know your customer – basic principles of financial law).

8 For example, in the Interpretation of the application of the so-called accepted identification process in terms of Section 10 of Act no. 253/2008 Coll., available at: http://www.mfcr.cz/cs/verejny-sektor/regulace/boj-proti-prani-penez-a-financovani-tero/zprostredkovana-identifikace

card, i.e. "občanský průkaz" (personal identity card) for Czech citizens, while foreign nationals present their passport or other official documents, recognized by the given country (e.g. driver's license, birth certificate, etc.), from which all the necessary identification elements are apparent. This is analogous for legal entities, which present current extract from the Commercial Register or notarial record of incorporation, or other documents, as appropriate, as the document for the verification of identification elements. Statutory representatives of legal entities then present their identity card once again. However, based on practical experience, we can say that the risk of identification in case of accepted identification may be viewed with regard to a financial institution. The question is why. The demonstrative list of entities that are considered financial institutions for the purpose of accepted identification was not purposeless. It is to show the number of entities that may act as financial institutions. Many of these entities are registered with the CNB due to the fact they had received a permit (license) to act as the given financial institution (e.g. banks, insurance companies, pension companies, securities traders, insurance settlement agents, etc.).

Therefore, if solely the entities registered in registers publicly available at the CNB website communicate, the situation is much simpler, as we can very their basic information and particularly the fact they are in fact financial institutions. Additional data are also available in the Commercial Register[9], in case of legal entities, or Trade Licensing Register[10] in case of individuals (but also legal entities). However, the list of financial institutions that may benefit from accepted identification also includes entities that are not subject to such registration – i.e. the verification of their actual existence or authorization to carry out the given activities is less "reliable". This concerns, for example, leasing companies or loan providers/intermediaries, etc. Although they may also be verified in Trade Licensing/Commercial Registers, the fact they are not subject to supervision of a specialized state administration authority may be viewed as a riskier factor. Moreover, both groups of entities are exposed to potential risk of their mutual communication itself, consisting in a request of one entity to another for delivery of ID cards and other documents intended for corroboration of identification data of the relevant client in terms of Section 11(2) of the Act. However, in the immediately next section, the Act specifies a situation, where one applying entity is not sure whether the information received from another entity is relevant. In this case, it is basically required not to accept such information – i.e. not to apply this client identification method (subsection 3 of the same section). Even more risk is associated with the situation, where financial institutions are in a position of an institution disclosing client data. This institution is at "risk" of disclosing its client data to an entity not entitled to such data. It mainly concerns a situation, where communication may take place via email. Client information should not be provided upon telephone requests or inquiries. There should always be verifiable and objective communication, whereas it is always necessary to eliminate counterparty risk. In practice, this means that the financial institution, which received a request, must be absolutely sure the applicant is one of the entities entitled to work with accepted identification and that this entity does in fact exist. Communication (information sharing) through data mailbox, featuring an electronic signature, would be ideal; however, mail messages of commercial nature are not active for financial institutions and the section of the data mailbox dedicated to communication with state administration authorities cannot be used for this purpose. It is thus safe to say that communication of two financial institutions will always entail certain counterparty risk, whereas such risk will be slightly lower for financial institutions registered with the CNB or similar state administration authority abroad. For the purpose of using accepted identification and ensuring mutual positive communication of two financial entities, it would be ideal for representatives of both parties to know each other from their professional dealings, thereby essentially eliminating counterparty risk, provided both representatives act in the interest of their respective institutions. However, since the general practice is so diverse, the counterparty risk for both entities – i.e. the applicant and the respondent – is reduced by mutual verification of the actual existence of the

9 See: http://portal.justice.cz/Justice2/Uvod/uvod.aspx, section "Veřejný rejstřík" (Public Register).

10 For example, see: http://www.rzp.cz/cgi-bin/aps_cacheWEB.sh?VSS_SERV=ZVWSBJFND

given entity/counterparty. This prolongs the entire process. The subsequent effect of the verification of identification elements may then take considerably longer. Therefore, this proceeding may only be recommended for the case of cross-border or foreign clients and their identification, although it is more suitable to ensure the so-called mediated identification in terms of Section 10 of the Act[11].

Accepted identification is also associated with the fact that financial institutions may accept identification data that are later found to be false, incorrect, or relating to a different person (e.g. unauthorized use of personal data of another individual). The question is who would be liable for damage, for example, that could be incurred by a financial institution accepting such data from another institution in good faith, assuming the correctness of such data. We cannot anticipate decisions of a court of law in case of disputes between such financial institutions; however, it is apparent from the aforementioned that it is not possible to rely on accepted identification elements, particularly in case of active transactions (i.e. loans). How to prevent such situation? Do not use the institute of accepted identification. We advise financial institutions to perform the client identification process on their own, using accepted identification as little as possible. After all, the client identification process in the presence of an individual or statutory body/proxy of a legal entity is not that complicated and lengthy. At the same time, it is possible to use, for example, mediated identification or identification on the basis of power of attorney.

Another aspect relating to the client identification process of financial institutions concerns the fact that financial institutions may not perform the client identification at all, because the provisions of Section 13, particularly subsections 1 and 2, allow this. Once again, these provisions specify the types of clients/entities, for which it is not necessary to identify business transaction parties. The inclusion of some entities is very logical. For example, this concerns credit institutions, where the client is another financial institution. Furthermore, it concerns entities with funds deposited in notarial custody, state administration authorities, etc., but also other business entities (e.g. providers of payment services through mobile network or entities generating electronic money to the extent foreseen by law, etc.). In terms of practical examples, there are payment institutions that execute payment transactions on the account of their clients (these are most frequently online stores, for which payment institutions or providers of small extent payment services settle payments for goods purchased online). It concerns cashless transfers of funds from accounts of clients of banks and other payment service providers or transfers of electronic money from entities entitled to issue electronic money. Since payment service providers are registered entities and subject to special legal regulation[12], the CNB rightfully requires them to prepare an internal regulation – System of internal rules (see Section 21), which should also comprise, among others, rules for performing client identification (Section 21(5)(b)). Naturally, the material should contain principles of identification for clients, who have an account with the given entity; however, it is not adequate to require such institution to set down principles for verifying facts relating to a payer. In this regard, we should not that not only payment institutions, but also payment systems in general, and particularly banks and savings/credit cooperatives, rely on a good faith institute in processing payment transactions - i.e. that proper payer identification (in case of transfer of funds initiated by a payer) had been performed by the relevant financial institution (namely a payment service provider) of the payer. The monitoring of the overall annual turnover limit for such client of EUR 2,500 per year seems rather impractical, with the need to perform additional identification once this limit is exceeded. Therefore, we recommend that the provider of such services always performs client identification.

11 It is also possible to use the methodological instruction of the FAU available at: http://www.mfcr.cz/cs/verejny-sektor/regulace/boj-proti-prani-penez-a-financovani-tero/zprostredkovana-identifikace

12 Act no. 284/2009 Coll., on the Payment system.

Transferred identification and new Civil Code

Following the effectiveness of the new Civil Code[13], new issues may emerge in connection with the fact that it is possible to conclude any contracts without the requirement for their formal expression – i.e. written form (subject to various exceptions, e.g. consumer loan contract[14]). Until the end of 2013, written form was required for contracts, e.g. for current accounts, and a failure to comply with such form would render the given contract null and void. Contracts on the provision of payment services no longer require written form; consequently, some provisions of the Act on Selected measures against legalization of proceeds from crime and financing of terrorism, Section 13(2)(f)(1), should be interpreted in the context of special legal regulations that discuss specific products. We expect that practical dealings will stem from well-established and proven methodological procedures, where contracts are in writing even if it is not explicitly required by the Act[15].

Issues relating to remote identification

The finale of this section is dedicated to the issue of client identification performed remotely. In principle, it is a method where a client, who wishes to become a customer of a financial institution, may perform his/her identification remotely, provided it is permitted by the given financial institution. Section 11(4) of the Act refers to this process as the remote identification. The Act then directly specifies prospective client's obligations, the fulfillment of which must be corroborated by the given financial institution. In short, this concerns the client's obligation to create a true copy of his/her identity card, deliver this copy to the new financial institution, and subsequently execute first payment to the benefit of the newly opened payment/equivalent account with such institution from another credit institution (i.e. from a bank or savings/credit cooperation only, not from a payment institution account), whereas copies of documents relating to such account are also made and sent to the given financial institution. This face may be evaluated as very risky, particularly if it concerns individuals, who are not sufficiently literate. The client's counterparty risk is so significant in this case that it is not used, with the exception of renowned financial institutions. Potential frauds and subsequent unauthorized use of personal data were discussed in the publication "Know your customer"[16]. Therefore, we should note that this method of identification should be approached even more cautiously than accepted identification. The reason for this is the fact that accepted identification involves two professional and financially erudite entities, while remote identification involves one absolutely amateur entity – usually a consumer – and one professional party to the transaction – i.e. a financial institution. In case the professional party involves at least institutions registered with the Czech National Bank, we may assume "self-preservation"; therefore, such institutions or their employees, as appropriate, will not perform activities that would contradict the law. Internal controlling and inspection systems of the given institution should immediately defect any such conduct. However, if this concerns any financial entity or even any obliged entity in terms of Section 2 of the Act, which is not subject to supervision of a state administration authority, the risk increases significantly. Therefore, it would be beneficial to urge modification of the applicable Act no. 253/2008 Coll., on Selected measures against legalization of proceeds from crime and financing of terrorism, and exclude some entities from the process of potential remote identification.

13 Act no. 89/2012 Coll., Civil Code.

14 See Section 6(1) of Act no. 145/2010 Coll., on Consumer credit.

15 For example, Act no. 513/1991 Coll., Commercial Code, in force and effect until the end of 2013, did not require a written contract for loans. Contracts in banks and other credit institutions, as appropriate, had always been entered into in writing only.

16 See chapter 3.3 of the book: KYNCL, Libor a kol. Poznej svého klienta – základní zásady finančního práva. 1st Edition, Brno: ACTA UNIVERSITATIS BRUNENSIS, IURIDICA, 2012. No 433. 165 pages. ISBN 978-80-210-6085-2. (Know your customer – basic principles of financial law).

2.4 Simplified identification process

Definition of the problem

Proper client identification is the basis for performing due prevention of money laundering and terrorism financing. The client identification process is most comprehensively discussed solely by Act no. 253/2008 Coll., on Selected measures against legalization of proceeds from crime and financing of terrorism (in this section hereinafter the "AML Act"). In its Chapter I, the Act defines basic obligations, which must be performed with regard to a transaction party identification by obliged entities, including financial institutions. Some pitfalls of the identification process were already discussed in Section 2.3; however, one important fact was intentionally omitted – i.e. deliberation on potential approach to applying the so-called simplified identification process. The following section will briefly explain why this process may actually be considered.

Identification in relation to the transaction type

The provisions of Section 7 of the AML Act set down the general obligation to identify party to a transaction - provided such transaction exceeds the amount of EUR 1,000; the identification is to always take place prior to the transaction itself. The following provisions of the AML Act (subsection 2) then specify the client identification method. The identification elements are specified in Section 5 of the AML Act.

With regard to individuals, they are as follows:

- All names and surnames;
- National/personal identification number (date of birth if not assigned);
- Date of birth;
- Gender;
- Permanent or another residence;
- Citizenship.

With regard to entrepreneurs, it is also necessary to verify their trade name, place of business, and identification number. These facts must be verified on the basis of an identity card, if specified therein. Moreover, it is necessary to enter the identity card number, issuing country/authority, and expiration in an information system or records. The relevant person performing the identification shall verify that the identity card photo matches that of the holder. The aforementioned obligations alone result in various questions. One of those questions: what to do if an identity card does not include all the required data? For example, identity cards of people born outside of the territory of the Czech Republic do not feature a place of birth, but the country. Passports, which represent the basic identity card for foreign nationals outside of the EEA, often do not show permanent residence/place of residence, etc. Therefore, in practice, the missing data are replaced with a requirement for the given person's affidavit relating to the place of his/her birth or residence. In case of stricter process, it might be possible to require a birth certificate, but this is not the case in practice. On the other hand; however, the AML Act ultimately does not impose an obligation to request an affidavit or other action on the part of the person being identified/entity performing identification. Therefore, the Act does not impose such obligation; however, it does not prohibit it either.

The identification process is similar for legal entities, whereas the following identification elements are considered to be the basic elements under the AML Act:

- Trade name or appendix to the trade name;
- Registered office;
- Identification number or similar number assigned abroad; and
- Identification elements for the statutory representatives under the rules set down by the AML Act for individuals.

With regard to legal entities, it is also assumed that all the identification elements required in the course of the identification process will be verified from "*from their business registration documents…*"[17]. Therefore, it is apparent from the aforementioned that such identification shall be verified and recorded from available deeds (documents) recognized by the given state for all the given elements; with regard to foreign nationals, they shall also feature an apostille or super-legalization[18].

The original Act, which dealt with anti-money laundering (see Section 2.2 above), set down simpler identification elements, specifically for individuals:

- Name and surname;
- Address; and
- National/personal identification number or date of birth or identification number, as appropriate.

With regard to legal entities, it concerned the same elements as those foreseen by the AML Act; however, only the three identification elements specified above were required for statutory representatives. These elements are still used as the basis for Act no. 21/12992 Coll., o Banks, for the purpose of insurance of deposit receivables[19]. The additional elements, which must be verified for individuals, had been introduced by the 3rd Money Laundering Directive, which was transposed into the Czech AML Act in 2008.

This transposition somewhat complicated the practical application of the identification process for some transactions. The AML Act permits a number of exceptions to the identification process – specifically listed in the provisions of Section 13. However, real life may result in situations that may hardly match any of the given reasons and, if so, the relevant financial institutions – and banks in particular – may be exposed to higher risk by not performing proper identification in terms of the AML Act.

What products or services may this refer to? It mainly concerns third-party cash deposits made to an account; however, it may comprise other services, where identification is currently required under the AML Act and where obliged entities (banks in particular) have hard time applying exceptions permitted under the provisions of Section 13 of the AML Act.

Simplified identification could specifically be used on the basis of the wording of Section 13(2)(e) of the Act. The provisions may be characterized as follows:

The exception to the identification obligation (or client due diligence, as appropriate) could be applied or *"the obligation to identify and perform due diligence of a client does not have to be performed for…..e) other products, should they pose low risk of abuse for the purposes of legitimization of proceeds of crime*

17 Section 8(2)(b) of Act no. 253/2007 Coll., on Selected measures against legalization of proceeds from crime and financing of terrorism

18 Super-legalization = higher authentication of a deed/document. For more details, see, for example: Schlossberger, Otakar. Platební služby. 1st Edition. Prague: Management Press, 2012, 325 pages. ISBN 978-80-7261-238-3, pp. 45 – 47. (Payment services).

19 Sections 41c(3)(a) and (b)

or financing of terrorism and meet the following conditions ……. 1. Are accompanied by a written contract; 2. Payments are made solely via an account held on the customer's name at a credit institution …..".

Therefore, it is apparent from the above mentioned that a deposit to an account, which has always had a written form so far[20], thus also meets the other precondition consisting in the fact that payments are subsequently executed from an identified (not anonymous) account. However, cash deposits are not considered payments in terms of a special legal regulation[21] - they represent a spate payment service. In a wider context; however, a cash deposit to an account maintained by a bank or credit/savings cooperative could be considered a transaction (service) that might be excluded from identification. Nevertheless, in practice, persons depositing funds up to the equivalent of EUR 1,000 need not be identified, unless otherwise determined by the recipient considering the facts that might lead to suspicion over the legality of such actions. In case of amounts exceeding EUR 1,000, it is sufficient to perform identification process described as simplified identification. In practice, this would mean that only the basic identification elements would be verified for the depositor, as set down by Act no. 21/1992 Coll., on Banks, for the purpose of the insurance of deposit receivables. Therefore, this would always concern the following elements for the given individual: name and surname, place of residence or permanent residence, and national/personal identification number or equivalent identification number. Such facts may be verified on the basis of a basic identity card, such as personal identity card ("občanský průkaz"). In case such person deposits funds on behalf of an institution, the basic identification elements of such institution would also be verified – i.e. trade name, registered office, and (company) identification number. It is more than recommended to include these particulars in the documents of credit institutions, provided they use them. If this is not the case, such information will need to be entered directly in the financial institution's system.

In case a credit institution opts to use this type of simplified identification, not recognized by law for the time being, it would be appropriate to recommend including this procedure of the identification process in the System of internal rules pursuant to Section 21(5)(b), with proper justification that leads the bank or credit/savings cooperative to believe the risk of such transaction is either low or virtually none at all. The reason for this is as follows: in case a client / account holder had been duly identified and we know such client, his activities, there is no reason to believe that the funds that might be deposited to such account would be used for the legalization thereof or even terrorism financing. Nevertheless, even cash deposits to accounts must be given proper attention.

Conclusion

However, to ensure unambiguous legal specification, it would be suitable to amend the AML Act and expand it with the possibility to perform the so-called simplified identification for selected transactions. We could certainly find more transactions or actions, where the application of the simplified identification process would result in less administration for the obliged entities on the one hand and for clients of banks and other financial institutions on the other hand.

---

20 Until the end of December 2013, it virtually always concerned a current account contract in terms of the provisions of Section 708 of the former Act no. 513/1991 Coll., Commercial Code, which required written form. The practice of banks and savings/credit cooperatives, which are the only entities entitled to accept deposits, remains the same even after the effective date of Act no. 89/2012 Coll., Civil Code, although it no longer requires a written form. This is also how the situation is resolved under the special legal regulation, i.e. Act no. 284/2009 Coll., on the Payment system in this case, which requires the following for payment account contracts: rights and obligations of the parties must be recorded on a medium allowing permanent records (the contents of the contract must be recorded on a permanent data carrier – i.e. also a paper form).

21 Again, this concerns Act no. 284/2009 Coll., on the Payment system. A payment is a special type of the payment service, similarly as an account deposit – see Section 3. For more detail, see, for example, SCHLOSSBERGER, Otakar. *Platební služby*. 1st Edition. Prague: Management Press, 2012, 325 pages. ISBN 978-80-7261-238-3, p. 13 an. (Payment services).

3. Process of combating the legalization of the proceeds from crime and terrorism financing – selected issues

3.1 Introduction

In this section, the authors will address selected issues relating to the process of combating the legalization of the proceeds from crime that have or may have some connection to the applied practice. The presented topics are very diverse and each of them may affect the AML process.

We will first discuss the possibility of archiving documents or other information, as appropriate, within the context of combating the legalization of the proceeds from crime and terrorism financing. Banks as well as other financial institutions are required to archive any and all information, documents, and other facts, as appropriate, for a period of time set down by law. The methods and form of archiving such information vary, including possible audio or video recordings. In this section, we will demonstrate issues relating to potential archiving of, for example, video recordings made within workplaces of banks.

The author subsequently thought over three key areas of the KYC process – i.e. client identification, client audit, and regular and continuous monitoring. Moreover, we will characterize the procedure of assessing clients within the KYC process and specify individual approaches to KYC. The paper also deals with the scope of information that might be required for identifying beneficial owners.

Furthermore, this section will examine certain requirements imposed on systems of internal rules, processes, and control measures aimed at preventing the legalization of the proceeds from crime and terrorism financing in financial institutions and banks in particular. In terms of caution, the issue of money laundering must be given maximum attention; this is why it will be emphasized that it is necessary to detect "unfair" practices of financial institutions as well as other financial market participants. Unfair practices shall also refer to those that contradict rules set down by regulators and other institutions governing the operational framework of financial institutions. However, this must be done with maximum prudence in order to prevent false accusations and negative sentiments on the financial markets, as a result of excessive regulation in the area. One of the suitable instruments that could potentially assist in detecting unfair practices in financial institutions is greater deal of attention to accounting and statistical reports/statements that national and supranational regulators or supervisory authorities receive from financial market entities. On the other hand, financial market entities should ensure the data presented in submitted reports/statements are of the highest possible quality in terms of the monitored information, with the highest possible explanatory power. With the discipline on the part of obliged entities and regulators, it may be possible to eliminate risks associated with the utilization of financial institutions as money laundering vehicles in the financial markets.

The fourth section of this chapter will discuss a slightly different area that pertains to higher effectiveness in detecting the legalization of the proceeds from crime and terrorism financing. This concerns the area of work available data sources that might be useful for expert investigations in the area of the so-called financial crime. We will also present problems encountered by experts in the Czech Republic in connection with efforts to obtain and use such data sources. It is a known fact that the amount of information contained in bank account statements from individual banks varies. Information provided by the CNB is often not sufficient for withdrawing licenses from regulated entities. Information of the FAU represents a valuable source of information about the now non-existent bank accounts. EDGAR database, maintained by the SEC[22], is a very useful source of information. This part will be followed by a

22 SEC – Securities Exchange Commission (will be discussed later).

section on economic and financial crime as one of the side effects of the process of legalization of the proceeds from crime.

The next part of this chapter will be devoted to the consideration of the challenges of banks or other financial institutions, or even entities required to ascertain and verify whether clients are politically exposed persons or their relatives. It is true that a bank may not carry out a transaction for (to provide a service or product to) a politically exposed person, if it does not know the origin of the financial assets. The article links the obligations of banks and other institutions, particularly financial institutions, and control procedures in public administration.

The objective of the seventh and eighth sections of this chapter is to explain the importance of identifying financial institutions to increase financial security in the world. First, the author thought about the possibility and method of identifying the financial markets participants; in the next section, he discusses the legal entity identifier. The first subchapter of this part outlines various aspects of financial security and the so-called safety net. The second subchapter deals with the influence of recent international Summits on increasing the safety of the financial market operations throughout the world. The third subchapter briefly characterizes the results of Cannes Summit. The fourth subchapter discusses the problem of regulating systemically important banks, which is to reduce the risk of impaired financial stability as an important element of financial security. The fifth subchapter is devoted to various aspects of the legal entity identifier composition. At the end, the author emphasizes the need for rational connection between the financial safety system structure and the practice of combating financial crime. The real security of financial transactions in today's world of rapid economic and financial fluctuations is subject to timely identification of the need to change the established system and early/timely response to this need.

At the end of this chapter we discuss some of the problems in detecting the legalization of the proceeds from crime in practice and the findings of the questionnaire survey with selected financial services providers in the Czech Republic. This survey was, inter alia, the basis for the outputs of the project "Increasing the effectiveness of procedures and measures for detecting legalization of the proceeds from crime and preventing the financing of criminal structures within the sector of the financial service providers". Furthermore, we provide some basic statistical data on the frequency of notifications of suspicious transactions in recent years.

3.2 Archiving documents, records, and other facts and their connection to AML

Introduction

This chapter will deal with the possible retention of electronic records made by banks or other financial institutions. Archiving documents or other information, as appropriate, that corroborate the existence of transactions is very important from different perspectives. This comprises a business perspective, legal perspective relating to potential enforcement of rights or obligations arising from the given business relationship, and the perspective of anti-money laundering activities. The area of banking or the financial market as a whole, as appropriate, is one of the sectors, where money is the subject matter of legal relations. It is this area that emphasizes the retention of information, records, documents, and other facts that corroborate the identity of entities involved in transactions, inception of a business transaction, etc. moreover, the means for storing and processing such information vary today. In addition to the physical archiving of paper documents (hardcopies), we may also consider audio or video recordings.

First, we can recall several fundamental legal regulations that are related to AML activities, with relation to the retention of documents, records in any form, and of other facts. It namely concerns the following legal regulations:

Act no. no. 563/1991 Coll., on Accounting;
Act no. 101/2000 Coll., on Personal data protection;
Act no. 127/2005 Coll., on Electronic communications;
Act no. 499/2004 Coll., on Archiving and documentary services;
Act no. 253/2008 Coll., on Selected measures against legalization of proceeds from crime and financing of terrorism; and
Act no. 89/2012 Coll., Civil Code.

With regard to prudential business activities of banks and other financial institutions in relation to anti--money laundering activities, it is often necessary to resort to such facts that are sometimes related to the legal limit in the acquisition and other use of evidence. It concerns the following: these entities, while trying to detect crimes that could impact the area of money laundering in the financial markets if successful, use or would like to use methods and procedures that would disclose or contribute to disclosing illegal activity.

The system of laws provides a variety of options for, or sometimes even orders, obliged entities to retain facts for a specific period of time from the moment of business relation termination. How are these facts characterized? For example, Section 16 of Act no. 253/2009 Coll., Selected measures against legalization of proceeds from crime and financing of terrorism, refers to identification data or documents and data on transactions. In practice, this concerns electronic records within banks' information systems or written / digitalized copies of documents such as extracts from various registers, founders' deeds, or copies of identity cards made by banks with the permission of their client. The law then requires obliged entities to preserve their clients' identification data or documents relating to transactions subject to identification requirement for the period of 10 years; other documents relating to transactions of up to EUR 10,000 are to be archived for the period of 5 years from the completion thereof, or 10 years if the aforementioned limit is exceeded.

Today, banks as well as other financial institutions today often resort to making video (camera) recordings – not only to protect the bank's assets, but also for safety/security reasons. Video recording systems appear not only on the outside of banks, but mainly within lobbies intended for clients, very carefully monitor cash counters or other high-risk bank workplaces, where nonstandard situations could occur. On the other hand, camera recordings also monitor activities of bank's employees, thereby indirectly protecting clients' interests.

The general opinion relating to the possibility of making camera recordings may clearly be inferred from the standpoint of the authority that protects mainly the personal and identity rights of individuals, i.e. of the Office for Personal Data Protection. Some time ago (specifically in 2006), the Office issued a communication that, although not legally binding, represents an interpretation of a competent public administration authority.

OPDP and video recording systems[23]

In this context, a video recording system may be viewed as "automatically operated, permanent technical system that enables to make and retain audio, video, or other recordings from monitored locations",

23 According to the Office for Personal Data Protection; Opinions of the Office/Current topic, available at: http://www.uoou.cz/uoou.aspx?menu=14&loc=328

for example, in the form of passive monitoring of an area or in the form of targeted images (motion capture) or reportage coverage. Naturally, video recording systems currently in use enable many methods of retaining recordings – from the slightly outdated form of video cassettes to the modern forms of digitalization and backups of data processed by means of computer technology.

However, anyone who intends to install a video recording system must, together with selecting the most appropriate technology, determine the purpose and means of data processing of data, provided their intention is to make and retain records of monitored locations, where other individuals are also present. It is at this stage of a decision-making process, where each video recording system operator should have already clarified the basic questions relating thereto – i.e. whether their intention is legitimate and what obligations, if any, in relation to other entities must be ensured and followed. Furthermore, they must consider, whether the use of a CCTV system is really necessary – i.e. whether another solution may be sufficient for achieving the given goals.

On the other hand, we must draw attention to the fact that the issue of potential clash of the CCTV utilization with the personal data protection principles is currently often and loudly discussed. The basic questions, for which answers must be sought in this connection, are mainly as follows:

a. When is a video recording system considered a personal data processing system and when is it not;

b. When is processed information considered personal data pursuant to Section 4(a) of Act no. 101/2000 Coll. or sensitive data pursuant to Section 4(b) of the aforementioned Act, as appropriate, and when is it not.

The first of the aforementioned problems may be viewed as follows: the Personal Data Protection Act shall apply to a CCTV operator in case such entity systematically processes collected information – in terms of the provisions of Section 4(e) of Act no. 101/2000 Coll. According to the OPDP, this will always be the case if a video recording system features a recording device aimed at monitoring of individuals. In this case, images of individuals are systematically collected in the space and time corresponding to the device settings. With regard to the given context, it is possible to presume to some degree that such images will be used further, as it is undeniable that the entire video recording system would not make any sense, if they were not to be further processed at all.

On the other hand, when a video recording system is "only" used to monitor locations under surveillance, the Personal Data Protection Act will not be applied; however, it does not preclude application of other legal regulations governing the protection of individuals' privacy, such as Article 8(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms, guaranteeing the right to respect for one's private and family life; Articles 7(1) and 10(2) of the Charter of Fundamental Rights and Basic Freedoms; or Section 12(1) of the Civil Code, according to which audio and video recordings relating to an individual may only be made with the consent of such individual, etc. However, for the sake of completeness, we should also mention the provisions of Section 1(2) of the Civil Code, according to which the Civil Code also governs the rights to protection of individuals, unless such civil relations are regulated by other acts. Such "other acts" definitely include Act no. 101/2000 Coll. Therefore, this means that in case the latter regulation is applied in connection with the operation of a video recording system, it is also necessary to exclude the effects of the relevant provisions of the Civil Code relating to the protection of personal rights.

However, the answer to the second of the above mentioned questions is much more complicated, also due to some difference of opinion concerning standpoints published so far (e.g. by means of the ASPI system) about determining when processed information is/is not personal information (data). In this connection, we must state that in case it is not possible to identify individual persons based on special

circumstances prevailing at the moment a recording is made, it can, generally speaking, be said that the data contained in the video recording systems do not reach the quality of personal data, since it is not possible to identify specific individuals solely on the basis of the video recording of such individuals, without using other accompanying information not included in such recording. Therefore, in case it is impossible to supplement the video recording system data with other information about the recorded individuals, such collected data cannot generally be linked to a specific or identifiable data subject.

Based on this logic, we could state that mere primary recordings of individuals retained in connection with video recording systems under operation will hardly allow unambiguous identification (without any additional data) of a specific or identifiable data subject; therefore, the application of Act no. 101/2000 Coll. may thus only be mentioned in intermediated context.

On the other hand; however, it is undeniable that each image capturing various features that make it possible to distinguish one individual from another (particularly facial features) turn such image, at least potentially, into personal data and it should be treated as such. We have After all, if we possess images of the aforementioned features, it is difficult to rule out future identification of the given individual, and, moreover, such identification is clearly the main reason why the recording takes place (see the definition of personal data under Section 4(a) of Act no. 101/2000 Coll.). As a side note, in case a video recording system is connected to an existing database that features personal data, this would clearly be a case of personal data processing, even at the first glance.

Under these circumstances, we can only recommend that a video recording system that allows tracking people and features a recording device be viewed as a device that performs personal data processing. However, each deployment of a video recording system (CCTV) should be assessed on a case by case basis.

Therefore, if we continue to follow the logic of Act no. 101/2000 Coll., it will also be necessary to determine the purpose for retaining CCTV recordings. It is undoubtedly derived from the usability of such images that must be assessed on the basis of any facts captured by the recordings and the purpose of their potential use. CCTV recordings may primarily be used as evidence a crime (mainly attempted "money laundering" activities in terms of banking) or damage caused within the monitored area. Furthermore, they may be used as evidence in proceedings on administrative offenses. In this case, it will particularly concern the use of recordings from video recording systems operated by the Police of the Czech Republic under Act no. 283/1991 Coll., as amended, or by municipal police forces under Act no. 553/1991 Coll., as amended. At the same time, administrative authorities may request recordings video recording systems at any time during the entire administrative proceedings. The aforementioned examples demonstrate the need to **consider objective periods of prescription relating to administrative offences when storing CCTV recordings**; save for various exceptions (e.g. crisis management), such periods do not exceed three years in most cases. However, a question arises in this context: are such recordings available with the given entities for the aforementioned period of time? Based on my own experience (author's note), it is safe to say that this is hardly the case.

In connection with the above mentioned standpoints relating to the application of the Personal Data Protection Act, there are various opinions with regard to the statement that the processing of information captured and stored by means of video recording systems does not concern personal data and that, consequently, the Personal Data Protection Act only applies to the treatment of the recordings from such video recording systems marginally, claiming that it is not necessary to limit the period of time, after which it would be necessary to destroy such video recordings, i.e. that it is in fact possible to store such recordings permanently, throughout the existence of such systems **or as long as there is sufficient capacity**, as appropriate. According to the deliberations and interpretation of the OPDP, such standpoint must be definitely dismissed, save for exceptions specified above – i.e. where monitoring

and storage of captured data reflects public interest, the objective of which is mainly the prevention and detection of illegal activities. Especially in case video recording systems are installed by private entities, such as banks or shopping centers, particularly as camera surveillance systems, **long-term retention of such data is associated with high risk of their unauthorized use**; this namely concerns the monitoring of clients or their practices.

In principle, we cannot agree with this opinion of the OPDP, because AML activities rely on legal provisions linked to EU legislation and even worldwide AML activities. AML activities can definitely be classified as "public interest", because the objective of CCTV recordings, for example in a bank, is to detect illegal actions. It is the retention of video recordings for a specific prolonged period of time that contributed to detection of crimes or attempted crimes. It is safe to unambiguously state **video recordings** monitoring the movement or activities of clients or other people in a bank or near banking facilities (e.g. ATM) **represent a precondition** to better and faster detection of attempted illegal conduct.

At this point, we should also examine the issue of the extent CCTV recordings represent sensitive data. In case we go back to their specification shown in Section 4(b) of Act no. 101/2000 Coll., it is clear that the only category of data that could be more or less relevant is the data related to national, racial, or ethnic origin. However, a question arises about the extent such images, often black and white, might make it possible to identify the aforementioned. However, if we were still to answer the above mentioned question affirmatively, it would be necessary to examine the purpose of the personal data processing. In the event such purpose is defined in a manner that the fulfillment thereof consists in systematic processing of such data/information, this would undoubtedly concern the processing of sensitive personal data. Therefore, when we refer to detecting thieves, it would only concern the processing of sensitive data if the system were to only detect perpetrators of predetermined ethnic origin. Nevertheless, such processing would have to be described as illegal, particularly with reference to the provisions of Section 10 of Act no. 101/2000 Coll. On the other hand; however, in case of detection of all perpetrators - irrespective of racial origin - the processing of sensitive data does not take place. This fact also applies to banks and other financial institutions.

In terms of the application of Act no. 101/2000 Coll., it is also very important to find legal title for the personal data processing in question. Without any doubt, it is possible to use monitoring systems to perform tasks set down by law; however, only a small group of entities is entitled to such deployment (for example, see the above mentioned Act no. 283/1991 Coll., on the Police of the Czech Republic). However, video recording systems may also be operated on the basis of proper consent of monitored individuals and, in particular, also on the basis of application of Section 5(2)(e) of Act no. 101/2000 Coll.

However, it will also be necessary to comply with other requirements imposed by Act no. 101/2000 Coll. First and foremost, it will be necessary to protect the given images/recordings from any disclosure/unauthorized access, even accident, in compliance with the provisions of § 13 of Act no. 101/2000 Coll., already during the phase of making such recordings and their transfer from the recorder to data carrier, comply with the reporting duty vis-à-vis data subjects, and also to register the given data processing with the Office for Personal Data Protection.

It is safe to say that, although the deployment of video recording systems will be subject to various future discussions, it is definitely necessary to consider the application of Act no. 101/2000 Coll. in this regard. Consequently, each existing and potential operator of a video recording system should pay special attention to this fact.

CCTV recordings and the new Civil Code

Following the effective date of the new Civil Code – i.e. Act no. 89/20012 Coll. – the existing situation will remain, i.e. making recordings by means of video recording systems or any other technology must have (with the exception of cases foreseen by law) a clear legal title going forward; this means that it must mainly be justifiable, why such deployment of a video recording system is taking place and that such act is adequate – i.e. that it is to ensure necessary protection of rights of an operator / personal data controller.

Nevertheless, with the exception of general periods of prescription, this Act fails to define, whether it is possible to keep recordings for a predetermined period of time.

As already mentioned, banks strive not only protect their own and their clients' assets entrusted to banks in the form of financial funds, documents containing clients' personal data (among others), but also to ensure AML activities. This is not only imposed on banks by Act no. 253/2008 Coll., but also by implementing regulations, e.g. Decree of the Czech National Bank no. 281/2008 Coll., on certain requirements for the system of internal rules, procedures and control measures against the legitimization of the proceeds of crime and financing of terrorism. Therefore, it would be most advisable for improving activities linked to AML to specify in a general legal regulation that **banks** and **other financial institutions** (as appropriate) operating financial activities in terms of special legal regulations (e.g. Act on Banks, Act on Credit Unions, Act on Capital Market Undertakings, Payment System Act, etc.) **should be required** to monitor high-risk sites/facilities (cash counters, lobbies, ATMs) and also to **store such recordings** for a specified period of time. Periods set down by Act no. 253/2008 Coll. – i.e. 5 or 10 years - appear to be suitable basic periods; it is also possible to set down other periods, e.g. at least for the duration of a complaints period or special periods set down for this purpose. The present situation is as follows: each bank or financial institution either does not store video recordings at all (with reference to the above mentioned interpretation of the OPDP) or stores them for different period of time (ranging from days to several months). It is about time to unify the periods in this area as well, to ensure that namely law enforcement authorities have an unambiguous possibility to request evidence. Moreover, the retention of such recordings may assist banks in resolving customer claims or complaints.

3.3 Reporting as financial institutions' anti-money laundering instrument

The financial and economic crisis represented a key test for the effectiveness of supervision and functioning of regulatory projects for banks, insurance companies, and other financial institutions. While the area of supervision has not brought any serious problems, the regulation was unable to indicate starting problems prior to the crisis. However, the crisis has provided politicians with an argument that it is necessary to increase regulation, and particularly in respect of financial markets, to prevent crises from reoccurring. This has resulted in a political pressure for extensive expansion of regulation, not for the higher quality thereof. As part of caution, it is also necessary to address the issue of legalization of the proceeds from crime and terrorism financing or "money laundering" in terms of tax policy, issues focusing on crime suppression, and respect for international embargoes and sanctions. This topic was important not only during the pre-crisis period, but also during the period of the subsiding crisis. The area is very relevant in connection with the social impact of crime; therefore, binding legal regulations that cover this area will be amended. Naturally, adaptation of the normative base also reflects the conduct of entities and emerging new forms of crime.

It must be emphasized that it is necessary to detect "unfair" practices, but this is to be done with extreme caution to avoid false accusations and negative sentiments in the financial markets. We can formu-

late the following hypothesis: if financial markets entities are motivated to report their accounting and statistical data in the highest possible quality, serious problems related to money laundering will only occur rarely. Conversely, if financial market regulators can rely on the reported data, it will also make their work much easier and they will be able to eliminate the risks associated with this problem.

Current situation regarding the identification of suspicious transactions

Since various reorganizations – mergers and acquisitions of financial institutions – are still taking place in the financial markets, it is important to address the issue of origin of financial funds or, as appropriate, to identity transactions with countries that are subject to international embargoes or other restrictions. This also concerns individuals, as it is often relevant to verify the origin of funds or country of the funds' beneficial owner.

A bank is one of the primary institutions in the financial market. Banks already have various rules in place, based on which they can classify suspicious transactions that supply financial funds from illicit activities, such as arms / drug trafficking. etc. Other financial institutions - i.e. credit unions, insurance and reinsurance companies, pension companies and pension company funds, securities traders, investment companies and funds, payment institutions and electronic money institutions, issuers of listed securities and other entities, settlement system operators and central depository, regulated market / multilateral trading facility operators, and, last but not least, exchange offices – are, for the most part, interested in setting up a system of internal rules, procedures, and control mechanisms, to ensure early/ timely identification of money laundering.

In case of execution of bank transactions that facilitate the legalization of the proceeds from crime, banks as well as other financial institutions face sanctions by regulators – in addition to financial sanctions, regulators may revoke banking licenses or restrict licenses for carrying out business activities within specific territories or with specific currencies.

National and international regulators strictly monitor transactions, for which banks are required to identify counterparties or final beneficiaries, not only for suspicious transactions. For example, in the case of bank transfers, it is necessary to prevent transactions from being executed "from" or "to" countries subject to embargoes or increased level of control. Alternatively, such transactions may include counterparties that do business in a criminal context or are subject of such trade in commodities and goods that are regulated or subject to the approval of national or international institutions (as appropriate) awarding licenses for the type of business, for example arms trade, trade in enriched uranium, etc. However, there are also normally traded commodities - such as precious metals or diamonds - that are used by perpetrators of crimes as a means of trading or maintaining the value of the proceeds from illegal activities that their owners/holders try to transfer to other countries and legalize the proceeds from crime by selling such commodities.

For this reason, banks always require the identification of an entity or beneficial owner of the company, to which the bank provides its banking services. Banks that are subject to regulation in developed countries usually have databases at their disposal that allow identification of high-risk individuals (individuals who were prosecuted or who do business in an area that is in conflict with the financial institution's strategy, or it may concern politically exposed persons, who are associated with increased risk due to the nature of their political involvement or nationality). Banks are required to examine in detail the beneficial owners of bank accounts they maintain and, in the event violations of rules are detected, to terminate cooperation and/or inform competent authorities about possible breach of anti-money laundering rules.

Some banks have been recently caught acting in conflict with the principles of internal rules, procedures, and control mechanisms for combating the legalization of the proceeds from crime and terrorism financing. For example, HSBC confessed and later apologized for the fact that its accounts in Mexico were used to launder money originating from crime –specifically from drug trafficking. This resulted in an imposition of penalty by American authorities and increased supervision over the bank's activities by American regulator[24]. For the period of 5 years, the bank is subject to stricter supervision of American authorities that monitor more stringent anti-money laundering rules and their practical adherence. It has recently been found that accounts of the British bank RBS[25] were used to transfer funds related to transactions "to" and "from" countries that are subject to embargoes (specifically Iran, Syria, and others).

Banks are also required to identify individual transactions between accounts that represent higher risk solely due to territorial risk and report such transactions to regulators or supervisory authorities. Each country determines its own terms and conditions of regulation and monitoring mechanisms. Banks operating within such territories are to implement such requirements; consequently, many banks with significant international presence are stricter in terms of monitoring (or supervision) that banks that only operate within a single country or region. Many banks also avoid transactions with or financing of certain types of commodities, such as precious metals, and refuse to trade in such commodities, as they are associated with higher risk of covering up proceeds of "illicit" origin.

Current state of reporting and prediction of its development

The European Union has recently introduced stricter rules of regulation financial markets, effective from the start of 2011. Existing supervisory and regulatory bodies that are in charge of the financial markets regulation within the European Union were reorganized, with some new bodies also being formed.

Similarly as in the area of banking, expert teams tried to detect problems of specific banks in time by setting up new or better rules using more sophisticated approach of various indicators. With regard to insurance companies, the new and improved approach is ensured by means of the "Solvency II" project.

Reports and notifications are currently being prepared in the European Union, on the basis of which individual European supervisory institutions will attempt to detect any impending problems in time and, naturally, to also ensure timely intervention.

Similarly, national regulators and supervisory authority, as appropriate, put more emphasis on the transparency of banking transactions to prevent money laundering. Banks already have various instruments in place that filter incoming and outgoing payments, which are associated with increased risk for them, particularly in terms of their reputation. This information is subsequently reported to a national supervisory authority – i.e. the Czech National Bank in the Czech Republic - on a monthly basis.

Unlike banking, the insurance industry operates on absolutely different principles. While most parameters are given in the area of banking, most facts in the insurance industry are determined on the basis of a "best estimate". Therefore, in order to predict the future, individual actuaries should do their best to estimate possible risks. The author believes that it is not possible to filter out suspicious transactions with the same accuracy in this area of business as in case of banks.

Payment of funds under insurance is not a standard business transaction; therefore, laws preventing money laundering in the Czech Republic do not apply to such transactions. Strict verification terms and

24 For example: http://www.bloomberg.com/news/2013-07-02/hsbc-judge-approves-1-9b-drug-money-laundering-accord.html

25 RBS – The Royal Bank of Scotland.

conditions are set down for payments over fifteen thousand euro (approximately CZK 375,000) both in the Czech Republic and the European Union. Companies and authorities must provide any and all information about the purpose and movement of funds. However, these strict terms and conditions do not have to be followed for payments made under insurance – this may be classified as a "legal loophole".

Unfortunately, it is not unusual for people to pay higher amounts in cash under certain circumstances, and the authorities cannot do anything, although effective legal regulation exists[26].

Suspicious transactions in the insurance sector may be indicated by the fact, for example, where a policy holder requires extreme increase in the insured sum or takes out several insurance policies for the benefit of several insureds. Furthermore, another warning sign is execution of multiple changes in accounts for the payment / refund of insurance premium. Another alarming signal is a change in the policy holder's behavior, such as a situation, where the policy holder suddenly makes a single advance payment for several years instead of regular contributions under an insurance scheme. In terms of payments, cash payments, payments by check or negotiations relating to the possibility to make more frequent payments are almost always a reason for concerns. Specific selection of products may also document efforts to launder money. A situation, where a client only selects insurance coverage for the case of death and severe illnesses, says about one's motivation. However, this is only associated with a low level of risk. The risk increases significantly in case a client pays insurance premium in the form of a single payment with the option of surrender value or flexible investment life insurance with the option of surrender value. We should also mention the geographical risk. It applies to countries with inadequate legislation and countries that provide financing or support of terrorist activities. This category also includes countries with significant level of corruption or other criminal activities.

Reports/statements aimed at identifying threats associated with money laundering

Verification of financial statements may contribute to timely identification of potential threats associated with the already mentioned area of money laundering. With regard to banks, submitted information may be used to identify potential increases of problematic assets, increasing percentage of risky loans, which result in rising adjustments/provisions for loans created by banks and other entities providing financing. Furthermore, it may also be a decreasing volume of primary deposits, which puts pressure on banks' liquidity and consequently on an increase in interest rates on interbank markets, mismatch between the maturities of banks' assets and liabilities – particularly in a way that banks are unable to raise funds in the market to secure necessary liquidity, especially in the short term, and to fund current needs and due liabilities. Moreover, this translates into rising interest rates and declining loan volume due to the aforementioned increase in interest rates. The above mentioned indicators are rather specific in terms of the potential risk of a financial crisis. In case of an imminent monetary or foreign exchange crisis, as appropriate, indicators identifying rising foreign exchange liabilities or declining foreign exchange receivables, etc. would obviously be applicable.

In case we examine all the collected data in detail, we may come to a conclusion that the report containing the volumes of cross-border collections and payments is one of the key indicators for assessing money laundering risks.

It is a balance of the volume of cross-border collections and payments made by a bank/foreign bank branch during a month under review in convertible foreign currencies and Czech crowns relating to selected transactions, broken down by sales/purchases of foreign currency structured by currency, financial services structured by country (the statement contains cross-border collections and payments of domestic banks/foreign bank branches vis-à-vis foreign commercial banks for provided and received

26 Act no. 254/2004 Coll., Restriction of cash payments.

financial services in executing own transactions or transactions on behalf of clients), generated profits/incurred losses in respect of financial derivatives and structured by underlying asset.

The statement with the volume of cross-border collections and payments made by a bank/foreign bank branch contains mandatory fields, where banks must report the country of the transaction origin, transaction currency, and other fact that may indicate a risky/risk-free transaction. As already mentioned, the transaction amount/volume certainly matters. In practice, we may also come across some reporting entities that corrected or modified data so that such data do not have to be reported as classified to the supervisory authority. In situations, where accounting systems were unable to provide comprehensive data, incomplete data were deleted or reduced or even incorrectly supplemented. We cannot say with certainty that such modified data were intentionally distorted; however, in case such data also included suspicious transactions, the aforementioned interferences resulted in the failure to identify and subsequently to detect legalization of the proceeds from crime.

As a result of this analysis, a change in the present state of reporting might be considered. One option would be to set requirements for such data that would better classify potentially impending risky conduct. Naturally, this would not be done at the expense of higher volume of required data and, consequently, higher burden for reporting institutions; however, qualitative revisions of such data could be considered. This could represent a guide for preventing nonstandard situations – not only on the national level, but also globally. With gradual transition to centralized reporting of data to centralized supervisory institutions, another important factor will be the frequency of data collections/submissions. Another crucial criterion will be the fact whether national supervisory authorities would continue to monitor – in much shorter periods of time – important indicators that could be used to prevent nonstandard situations associated with attempts at legalizing the proceeds from crime or terrorism financing. Since some bank statements/reports and all statements/reports of insurance companies are now open for discussion as a result of the Basel III and Basel IV projects and the Solvency II project, respectively, it is solely up to the European central authorities, whether they will subjectively make a correct decision about the need to monitor truly important data, refraining from data redundancy without the desired explanatory power. It is now up to national regulators or supervisory authorities, as appropriate, whether they will care and be willing to enforce their requirements and opinions vis-à-vis central institutions.

Conclusion

The objective of this part of the third chapter was to point out the importance of timely and accurate reporting as well as the fact that it is inevitable to examine, in a timely and rigorous manner, the data regularly received by regulators / supervisory authorities (as appropriate) from the "market". Accounting and statistical statements/reports may be used for timely identification of externalities that occur in the market, whereas such inconsistencies may serve for the identification of threats associated with money laundering. However, it is necessary to proceed very cautiously to prevent the spreading of negative sentiments among the financial market entities and subsequent factitious panic.

The question whether it would not be convenient to reconsider/revise the existing state of reporting to ensure it even better classifies potential issues associated with the detection of proceeds from crime and terrorism financing. Naturally, all this would not be done by increasing the volume of required data, but by revising the quality thereof.

We can certainly recommend placing greater emphasis on accounting and statistical reports/statements received by national/supranational regulators or supervisory authorities (as appropriate) from the financial market entities. On the other hand, the data provided by the financial market entities within their submitted reports/statements should be of the highest possible quality and with maximum

explanatory power. With the discipline on the part of obliged entities and regulators, it may be possible to eliminate risks associated with the utilization of financial institutions as money laundering intermediaries in the financial markets.

Data required by regulators or supervisory authorities (as appropriate) from individual financial institutions should be as uncomplicated as possible. This means that they should be easily accessible, have certain explanatory power, and not be duplicate and thus redundant.

3.4 Expert view of the sources of information and illicit financial flows

In general, policemen consider investigations relating to the so-called economic crime to be the most complex types of crimes, because it requires significant expertise on the part of investigators, availability of background materials, and sufficient time for obtaining and processing such materials. The work of experts is also very challenging and difficult, as they typically have to become familiar with tens of thousands of pages of documents of different quality. Furthermore, based on detailed, seemingly unrelated data, such experts must logically and comprehensibly describe events that had taken place in their expert evidence. Specific factors of police work relating to the investigation of economic crime are discussed in the work of J. Mazánek[27]. Potential indicators concerning problems of companies that may arise (among others) as a result of criminal activities on the part of the company management/owners in the economic area are discussed in the work of J. Brada[28] and others.

The work refers to problems encountered by experts providing professional consulting services to law enforcement authorities in connection with their attempts to get sufficient background materials necessary for tracking flows of assets and particularly financial funds relating to criminal activity, specifically "white-collar" crime. A number of institutions and authors cover the area of economic crime in the Czech Republic; for example, we can mention the works of Baloun[29] or Cejp[30].

Thou shalt not steal

Although Moses was given the "Thou shalt not steal" commandment from the Lord for his people on Mount Sinai (Exodus 20:15), it was clear to our ancestors and it is clear to our fellow citizens that the mankind has not been truly mindful of the Lord's commandment. From the perspective of economists, the objective of property crime is to generate property benefits for the perpetrators of such crime or benefit for entities that provide some type of benefits to the perpetrators. Therefore, the aforementioned crime is commonly coupled with transfers of assets from injured/aggrieved entities to perpetrators or other entities, for which perpetrators wish to secure property-related benefits.

---

27 MAZÁNEK, J. Specifika dokazování hospodářské trestné činnosti. In *Trestní právo*, 2008, Vol. 13, No. 2, pp. 5 – 13. (Specificities of proving economic crime).

28 BRADA, J. Hodnocení úvěrové bonity obchodní společnosti. In *Zadlužení – fenomén současnosti.* Prague: Soukromá vysoká škola ekonomických studií, s.r.o., 2012. pp. 108-116, 8 pages. ISBN 978-80-86744-92-6. (Assessing creditworthiness of a company).

29 BALOUN, V. *Finanční kriminalita v České republice*, Prague, 2004, Institute of Criminology and Social Prevention, Partial study under the project "Research of economic crime" (Financial crime in the Czech Republic).

30 CEJP, M. *Organizovaný zločin v České republice III*, Institute of Criminology and Social Prevention, 2004, Prague, Institute of Criminology and Social Prevention. (Organized crime in the Czech Republic III).

Property benefits from illegal activities

From the practical point of view, the flows of assets in the form of money may be considered the most important flow of property benefits. Assets in the form of money allow perpetrators of property crime to purchase necessary goods and services, without being too limited by problems related to converting nonmonetary tangible assets (real estate, works of art, collectables) into liquid assets. However, we should remember that some types of assets – e.g. dematerialized securities – may also be considered assets that are close to financial funds in nature, because the conversion of such assets into liquid assets need not be associated with substantial financial or time cost.

With regard to the practice of authorized experts/expert witnesses, an integral part of work of expert witnesses, policemen, and prosecutors is the search for and identification of flows of tangible assets, particularly in the form of cash flows in bank accounts. In some cases, this even includes flows of intangible assets – e.g. receivables from purchased securities, etc.

If we were to abstract from the prevention of crime and arising losses, the law enforcement authorities strive to document property crime, convict and subsequently discipline/punish specific perpetrators. Actions of perpetrators of property crime aimed at preventing the localization and potential recovery of unlawful property benefits to original owners are pertinently described in the statement of former Prime Minister and later President of the Czech Republic, V. Klaus: "*I know where the money is, but why do you wish to know?*"[31]

Therefore, in this piece, we will focus on describing information sources that are used by experts in the course of their work and on presenting the problems associated with the acquisition and specific use of available information sources during the process of investigating property transfers or transfers of property benefits, as appropriate, from aggrieved parties to perpetrators from the perspective of expert witness practice.

Sources of illegal property benefits

Since 1993, the classic sources of "modern" illicit funds in the Czech Republic have been activities associated with white-collar crime:

a) State-owned or national companies/enterprises were significantly damaged (tunneled) or impaired by their management. In the past, management would typically incorporate different companies, to which profitable activities of state-owned companies were subsequently transferred. Today, this impairment takes the form of awarding of public contracts to affiliates of the management by means of manipulated tender procedures;

b) Banks – The economic substance of gaining unjustified property benefits from banking resources took the form of intentional failure to repay loans, often with assistance of upper management of banks (both state-owned banks and banks set up after 1990) and acquisition of interests in "associated" economic entities by banks, e.g. in the form of purchases of overpriced interests in joint-stock companies. This stage effectively ended in 2001 – with the bankruptcy of Investiční a Poštovní banka. However, we are currently witnessing the renaissance of these activities in credit unions.

c) Undertakings for collective investments – This typically concerns investments of investment and mutual funds management by investment companies and also investments of the so-called "pension funds" in assets by purchasing securities of their "associated" entities and affiliates.

31 http://cs.wikiquote.org/wiki/Václav_Klaus)

d) Investments of municipalities and public administration authorities – This concerns awarding of public contracts to associated entities of the management via predetermined tender procedures, for example.

e) Tax evasion – From the macroeconomic perspective, this refers to execution of untaxed (i.e. illegal) economic activities. Common examples include unauthorized "VAT" deductions and failure to pay excise tax.

The author understands that various legal regulations and by-laws strive to prevent or at least significantly limit the above mentioned activities. However, the expertise and time required to investigate potential illegal activities in this area do not overly support the hypothesis that the successfulness of law enforcement would considerably reduce the volume of property benefits generated from illegal activities in the above mentioned areas.

In addition to illicit funds generated as a result of white-collar crime, there are also illicit funds generated as a result of standard/conventional crime that are "legalized" in the form of investments in "moral activities".

Nevertheless, from professional point of view, there is no difference in investigating flows of property benefits arising from illegal activities of conventional (violent) crime and from white-collar crime (including illegal business activities).

General sources of information used inexpert investigations

Irrespective of whether the source of information is specified in an investigation or criminal file or whether an expert requests information from competent investigating authorities, information for analyzing property flows mainly originate from banks, securities traders, security depositories, real estate register, commercial registers, and government and public administration authorities (CNB, MoF CR, and others).

Therefore, the following sections will examine the most important types of information in more detail and remind the significance of such information for the purpose of expert investigations of property flows that might result from criminal activities.

Banks

Information from bank institutions has absolutely unique position in terms of expert investigations, since it is automatically assumed for bank institutions (banks) that records and copies of relevant documents identifying bank account holders and persons authorized to dispose of funds in bank accounts as well as persons depositing or withdrawing funds may be unambiguously and expertly matched to real existing entities.

Furthermore, it is automatically assumed that financial flows shown in bank accounts and provided by the bank in paper or electronic form are complete and flawless.

Although it is possible to come across some unwillingness of banks to provide information to law enforcement authorities, the overall will of banks to provide information may be rated as good.

Nevertheless, the provision by banks of their clients' account statements also has some deficiencies, such as:

- Absence of a particularly important "text field" (information provided by a payer) that makes expert investigation of the relevant financial flows, links to other financial flows, and reasons for such flows much easier;

- Account statements provided in electronic form solely as statements of archaic transaction sentence of intra-bank payment system, which not only has variable length, but also dates back to times when Microsoft operated from a garage;

- Accounts statements provided solely in the form of pdf files that are absolutely illegibility.

When asked about bank accounts of interest entities, banks also leave out inactive (extinct) bank accounts and, consequently, these historical statements are not provided to law enforcement authorities. After all, banks often forget account statements for entities that had the same names in the past as currently existing entities. Due to the above mentioned factors, it is highly advisable to submit a request for all available information on all interest entities to the Financial Analytical Unit of the Ministry of Finance as well, as the Unit may have records about transfers of funds of such interest entities that took places within later closed bank accounts – i.e. there is a great hope it might be possible to obtain important information about expired numbers of bank institutions without the time-consuming analysis of flows of payments in accounts of interest entities.

Note: According to information available to the author at the time of compilation of this publication, nonbank institutions that intermediate international payment system with the use of the payment system carried out outside of the "government regulated" banking sector no longer operate in the Czech Republic (or should we say "for the time being"?).

Securities traders and depositories (records)

In terms of its nature, information provided by securities traders (this sometimes involves bank institutions) is very similar to the information provided by bank institutions. We typically assume exact and precise identification of entities holding property and financial accounts with a securities trader.

A situation, where client's transactions and property transfers are registered on client accounts with a securities trader is slightly more complicated, as securities traders tend to have so-called joint accounts of a Czech securities trader with an American securities trader in the United States (typically with Penson). In terms of the existing legal regulation and based on standpoints of the regulatory authorities in the Czech Republic, this practice is not illegal, provided the parties – i.e. securities trader and the securities trader's client – agree on this.

From the economic perspective, this is a problem, because in case of a securities trader's bankruptcy, any securities in such "joint account" may represent the bankrupt entity's property – i.e. such joint accounts generally cannot ensure division of clients' assets from assets of the securities trader in the Czech Republic.

Furthermore, the existence of joint accounts of "Czech securities traders" with foreign securities traders significantly complicates the possibility to identify ownership of securities, as such securities are owned exclusively by a Czech securities trader from the perspective of a foreign securities trader.

In case of the so-called depositories (central registration authorities) of securities, there is a problem that mainly concerns discarding periods. Even though it is clear from electronic records that some economic entity submitted an order for transfer of securities; however, it is absolutely unclear, who submitted such order or whether a signature on such order for transfer of securities was not either allegedly or actually forged.

Registers relating to real-estate and commercial registers

The economic problem of all public or semi-public registers of assets (e.g. Real Estate Cadaster or Commercial Register in the Czech Republic) is the fact that ownership in the legal sense (i.e. ownership shown in the relevant register) is replaced with economic ownership – i.e. an owner *de jure* is not identical with an owner in the economic sense.

At present, it is common that the applicable law of different countries requires that there be evidence available of owners of trade shares, ownership interests, or real estate (property). A classic example is the transition from using bearer shares to using registered shares, where a joint stock company is required to keep records of its shareholders. Records relating to ownership interests of a particular company then may be accessed by government and public administration authorities, particularly revenue authorities. Similarly, data about owners of companies are used to create various systematic records in the form of commercial registers. Selected data from these registers may also be accessed by individuals or legal entities. For the sake of simplicity, we will use the collective term "public" to refer to any entities that may be interested in identifying the actual (beneficial) owners of specific companies.

The basic way of hiding ownership from uninvolved public is to replace the property in the legal sense with ownership in the economic sense. In the legal sense, the owner of a company is a person, who is registered as the owner in the appropriate register. In the Czech Republic, for example, an owner of a limited liability company is a person registered in the Commercial Register as a partner (shareholder), an owner of a joint-stock company that issues registered shares is a shareholder specified in a list maintained by the company. Naturally, if a joint stock company issues bearer shares, the holder of such shares is also an owner of the relevant share in the joint-stock company's registered capital (share capital).

From the economic perspective, a company is owned by the so-called beneficiary – i.e. usually an individual. A beneficiary is in fact able to dispose of the company's assets without any limitations. The beneficiary's rights to dispose of such assets are not limited by owners (in the legal sense), who are visibly and more or less publicly registered as owners of the company. In English, such owner in the economic sense is referred to as "beneficial owner" (authorized owner).

The first step to replacing ownership in the legal sense is to "gain" control of a company operating abroad. It is not advised to carry out the below described transactions within a single national legal regime, e.g. in the Czech Republic, because the authority/rights of "domestic" national supervisory and regulatory bodies/authorities, revenue authorities or the Police of the Czech Republic to investigate suspicious business activities carried out by foreign entities operating in the Czech Republic as well as abroad are much more limited.

Entities operating within the territory of the Czech Republic typically use the following ways to acquire (i.e. purchase or otherwise gain control of) foreign companies:

a) Acquisition (purchase) of an existing or newly incorporated foreign company from a Czech intermediary – typically, this may concern the company Akont Trust Company, s.r.o., for example;

b) Incorporation of a new company through a law firm operating in the Czech Republic that also provides legal services associated with the incorporation and administration/management of foreign companies;

c) Incorporation or purchase of an existing company through a foreign law firm (contacts may be found on the Internet). This is the most expensive method of incorporating and managing foreign companies; however, it is the safest in terms of the perpetrator, as the majority of necessary documents for potential investigation of criminal activities are abroad and, moreover, protected by duty of confidentiality of an attorney.

The standard process of transferring ownership rights from owners of a specific company to a beneficiary involves a power of attorney, which is given by owners (in the legal sense) of a company. From the economic point of view, this power of attorney is the closest to the so-called procuration. In English, this general authorization is referred to as "Power of Attorney". Exceptionally, the author of this publication has also come across the term "General Power of Attorney". The typical features of a power of attorney are as follows:

- The beneficiary gains unlimited right to dispose of the company's assets, including the right to draw on loans, pledge the company's assets, appoint other individuals and legal entities authorized to dispose of the company's assets, etc.

- It is virtually impossible for donors of the power of attorney to revoke it with regard to the beneficiary. Therefore, a power of attorney includes provisions that exclude any invalidation or revocation of such power of attorney – e.g. a power of attorney may only be terminated in case the "beneficiary reliably finds out about the power of attorney revocation", that the "beneficiary is to appear, on a specific date and time each year, in a law firm, where the power of attorney may be revoked", etc. A power of attorney may also be entered into for a specific period of time (with unlimited option for renewal of such power of attorney); however, according to the author's knowledge, this only occurs in exceptional cases.

The provision of a power of attorney by owners (in the legal sense) to the beneficiary (i.e. owner in the economic sense) of a company results in the beneficiary's right to dispose of the company's assets without any limitations – i.e. it effectively results in the replacement of "ownership in the legal sense" with the so-called "ownership in the economic sense".

It is obvious that in the context of the aforementioned, it does not make too much sense, from the professional point of view, to make efforts aimed at ensuring that shares are only in the form of registered shares, that public contracts are only awarded to companies with demonstrable owners, etc.

FAU, CNB, SEC, and others

In principle, information (available from) from the FAU, CNB, revenue authorities, etc. may solely be accessed for the purpose of preparing expert testimonies for law enforcement authorities – i.e. typically upon request of the Police of the Czech Republic.

From the perspective of experts, the *Financial Analytical Unit of the Ministry of Finance of the Czech Republic* is a very important entity that may provide significant information.

The typical feature of analyses relating to extensive white-collar crime is a longstanding (typically for several years) execution of illegal or semi-legal economic activities that are typically accompanied by various "suspicious transactions" in bank accounts that banks report to the FAU.

The long-term nature of the said transactions is important - in the course of time, a number of companies are formed and dissolved, divided or merged, many bank accounts are opened, etc. in case of financial crimes committed by a group of individuals. Luckily for authorized experts, banks often capture some unusual transactions that take place and report them to the FAU – consequently, the FAU also features names of companies, individuals, and their bank account numbers. The transaction description and the circumstances that accompany such transactions tend not to be that important in practice. In case banks are later contact with a request for information about the so-called interest entities for the purpose of expert investigation, banks quite often do not provide complete information – e.g. bank accounts of such interest entities were closed long time ago, companies have been renamed, bank accounts renumbered, etc. This is why data from the FAU are exceptionally important – they provide information about bank accounts existing in the past, which – if necessary – makes it possible to formulate specific inquiries to banks and other entities, as appropriate, thereby supplementing the image of financial or other property flows relating to property crime of interconnected group of individuals.

Classic "suspicious transactions" involve, for example, "multiple cash withdrawals" following a receipt of a very substantial amount to a client's account, inflow of large amounts to a bank account with "almost zero" balance and subsequent transfers to other accounts, etc. On the other hand, authorized experts encounter in their professional practice many clearly highly unusual financial transactions that banks were unable to detect within their information systems and thus did not report them to the FAU. However, to stick up for such banks, we should note that some banks are repeatedly unwilling and reluctant to provide assistance to law enforcement authorities. Therefore, we cannot completely rule such behavior of banks in respect of the FAU, i.e. we cannot rule out that some banks do not notify the FAU about ascertained facts relating to identified "suspicious transactions" at all.

Recently, financial crime has been more and more associated with situations, where property transfers are not accompanied by cash flows; this unpleasantly complicates expert investigations.

The Czech National Bank, as a banking regulation/supervisory authority and as a supervisory authority for the capital market, is a useful source of information from the perspective of experts.

However, there is a relatively significant "but" from the perspective of needs associated with the practical work of experts. The CNB may obtain information from entities important to experts solely on the basis of a legal authorization – i.e. in case the Czech National Bank is not by law authorized to carry out supervision over the given interest entities – i.e. banks, insurance companies, securities traders or investment intermediaries/brokers – the CNB has no options *ex post* to obtain information that might be useful for experts. Typically, this concerns situations after a waiver or revocation of a banking license, license of a securities trader or investment intermediary/broker, or upon the commencement of a liquidation process, etc. This is also a hindrance that limits the possibilities of the regulator to learn from their errors, if any, since the regulator cannot obtain additional information *ex post* – i.e. in cyber terminology, the regulator does not get any feedback that is so needed for its ability to hone and develop their skills. Therefore, information and data collected about interest entities in the past remain for the purpose of expert investigations (e.g. protocols/minutes of onsite inspections, diaries of securities traders, etc.). However, collected data are often incomplete in terms of time – this has to do with randomly/suddenly performed inspections of the CNB with interest entities in the past. In certain situations, information obtained from the CERTIS system operated by the CNB may be useful.

The CNB has an absolutely vital role as an access point to information on foreign entities operating in the financial markets. This typically concerns bank entities or entities/undertakings operating in the financial markets – particularly securities dealers. Expertise of the CNB personnel essentially prevents redundant or incomplete information about foreign interest trade companies operating in the financial sector. This way, it is possible to obtain "business" information on entities operating in the financial sector, through

Europol or Interpol, which typically obtains them through queries to appropriate "registers of economic entities" in individual member states – they provide significant amounts of meaningless (ballast) information, whereas information relevant to expert investigations tend not to be sufficiently extensive.

For example, information typically obtained from the U.S. Securities and Exchange Commission (hereinafter the "SEC"), with the assistance on the part of the CNB, is particularly valuable.

The SEC is a very valuable source of information, particularly about business activities of entities operating in the Czech Republic, such as securities traders. Czech securities traders have so-called nominee accounts of their (Czech) clients with American securities traders, and they use such accounts to purchase and sell securities or to carry out margin or sell short transactions. American securities traders are subject to regulation by the SEC. The amount of available information relating to business activities of Czech securities traders obtained via the SEC tends to be uncommonly substantial and the quality of such information makes it an important source to be used in expert investigations.

For the purpose of examining property transfers of securities or mere security transactions with securities dealers, it is also useful to recall the existence of the EDGAR database, which is available free of charge, e.g. via the SEC website. The said database contains information, which must be provided by entities that are subject to control or supervision by the SEC. It is a completely unique (on a global basis) and extremely extensive database of documents; furthermore, it also provides opportunity to use full text search for keywords in most of the available documents. The database features prospectuses of security issuers, reports provided by economic entities, or annual reports, for example.

In case we compare the extensiveness of information available from the EDGAR database with the amount of information available from the *Central Securities Depository* (formerly the Securities Center), it is easy to understand why the protection of investors in the United States has been at a much higher level than in the Czech Republic.

Individual sources of information used in expert investigations

Any illegal economic activity related to money laundering is almost always accompanied by a noncash flow of funds and other property flows (e.g. transfer of real estate) recorded in official registers. In the practice of experts, the so-called financial crime does not frequently use cash funds, although there are exceptions to the "rule" – e.g. using cash for bribes or drug trafficking. Any transfers of cash or noncash assets logically tend to be accompanied or justified by other types of documents, unique (individual) to the given case, that represent valuable source of information for the purpose of expert investigation of the given case.

As a classic example of individual documents justifying the existence of financial/property flows in the commission of crimes, we can mention documents containing justifications that are used by entities committing such criminal activities for the transfer of funds to companies or individuals (or that are used to justify such activities):

- Contracts containing contractual penalties of sanctions for more or less hypothetical breaches (e.g. for minor delays of payments, failure to provide services, etc.). This is the most frequent reason used to justify the need for the transfer of funds. Alternatively to a contractual penalty, forfeiture of pledge/deposit is used, with one company using a financial amount or property to guarantee the performance of its obligation or liability (more or less hypothetical, once again).

- Contracts securing fees for the provision of trademarks or know-how. Typically, no one can later explain the substance of such know-how.

- Contracts securing fees for the provision of loans (credit), typically from a domestic company to a foreign company, whereas the remuneration for the loan provision is derived from the profit generated by the creditor company. The typical feature is, for example, that the higher the profit generated by the debtor, the higher fee paid by the debtor. (*Note*: Although the aforementioned method of providing financial funds is typical for the so-called Islamic banking, authorized experts and auditors in the Czech Republic and the EU also come across such practice between entities, for which economic conduct pursuant to "Islamic banking" cannot be assumed.). A loan is often not repaid, for various reasons.

A special type of expert investigations is the analysis of financial activities carried out between groups of domestic companies and foreign companies that are part of the multinational holdings (groups)[32]. Such investigations mainly focus on the correctness of invoiced amounts that are charged for the goods and services provided between individual members of the group. In case of different tax regimes for individual companies (that are part of such group), it is possible that the invoiced prices are, from the economic perspective, so-called transfer prices. Unreasonably high or low transfer prices may easily be used to transfer the tax base to countries with low tax base taxation. The objective of expert investigations in this area is not the existence or accuracy of the justification of economic flows, but solely the economic justification for the amount of cash flows.

Conclusion

We have comprehensively introduced available sources of data useful for expert investigations in the area of the so-called financial crime. Furthermore, we have described problems encountered by authorized experts in the Czech Republic in connection with their efforts to obtain and use the said data sources. We have stated, among others, that the amount of information in account statements from different banks varies. The information provided by supervisory/indirect regulation authority (CNB) is not sufficient after a license is revoked from regulated entities. Data from the FAU are a valuable source of information about bank accounts that no longer exist. Furthermore, the EDGAR database maintained by the SEC represents a useful source of information.

3.5 Economic and financial crime

Introduction

In the course of the project "Increasing the effectiveness of procedures and measures for detecting legalization of the proceeds from crime and preventing the financing of criminal structures within the sector of the financial service providers", it is also possible to follow publications and information that are available and that newly come into existence. The term "economic crime" is more and more frequent.

Economic crime is one of the most significant factors that adversely affect present business activities. It is thus absolutely clear that we must combat such crime. In this chapter, we define economic crime, its features, and causes that facilitate the occurrence of economic crime.

32 BUUS, T., BRADA, J. *Economics of Transfer Pricing Reviewed*, 2010, (available online at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=954333)

From the perspective of theory and practice, economic crime is addressed by Chmelík, Hájek and Nečas[33], who deal with the theoretical question of defining economic crime, economic and financial crimes and their mutual relations. Therefore, the key content of their publication is the theoretical analysis and definition of economic and financial crime and their interrelation, and methods and forms of outflow of crime-related profits (proceeds from crime). On the basis of a model, the authors provide examples of activities of criminal organizations in legalizing their proceeds and basic instructions for the resolution thereof. This process is referred to as the theory of progression of investing funds. Another area discussed in the publication is the relation of economic crime and organized crime, because economic crime is inherently associated with organized crime. It has been a relatively constant phenomenon in terms of crimes committed in the Czech Republic, whereas its significance is quickly increasing.

Statistics of economic and financial crime

Economic crime from the perspective of theory and practice is covered in the work of Fryšták[34]. His publication presents an introduction to the area of economic crime to ensure that the given topic is, in terms of quality and quantity of its contents, also comprehensible to wider general public (outside of legal professionals), for which it is intended. The basis of the publication comprises chapters on economic crime from the perspective of substantive law, procedural law, criminalistics, and criminology. In addition to this, it also contains statistical data relating to economic crime, sample questions for preparing specialized statements and expert evidence in the area of economics as well as the list of applicable legal regulations that must be used in the course of analyzing individual merits failing within economic crime.

According to their relationship to specific economic entities, perpetrators of economic crimes may be divided as follows:

- Employees;
- Individuals within an economic entity that is a victim to criminal activity;
- Owners or co-owners of a company, shareholders; whereas such persons commit crimes to increase their profits and improve their standing in the financial markets. This category also includes owners that use so-called "tunneling" (financial fraud) in a company, where they own certain property interest. Damages that result from economic crime tend to be very high compared to general crime.

Combating crime is part of a more extensive goal, i.e. achieving more effective, fair, and superior for of the complex of financial services. The methods of prevention may rely on various models prepared in the world and are also inspired by techniques proposed for the public administration or other segments of the economy. Several recommendations were already published some time ago[35] and contain the following measures (among others):

- Develop internal financial management systems that would ensure sufficient and effective control of the utilization of resources;
- Create sufficient internal control mechanisms aimed at ensuring quick and effective change of controversial decisions;
- Hold managers at all levels accountable for activities of their subordinates;

---

33 CHMELÍK, J. et al. *Úvod do hospodářské kriminality*. 1st Edition. Prague: Vydavatelství a naklad. Aleš Čeněk, s.r.o., 2005. 167 pages. ISBN 80-86898-13-X. (Introduction to economic crime).

34 FRYŠTÁK, M. *Hospodářská kriminalita z pohledu teorie a praxe*. Prague: KEY Publishing, 2007. 208 pages. ISBN 978-80-87071-18-2. pp. 10 et seq. and 200 at seq. (Economic crime from the perspective of theory and practice).

35 EIGEN, P. et al. *Kniha protikorupčních strategií*. Prague: Transparency International, 2000. 117 pages. p. 99. (Book of anticorruption strategies).

- Increase supervision effectivity;
- Carry out unannounced inspections of employees' working activities, etc.

As mentioned by Chmelík[36], economic crime may be viewed from three different perspectives:
- Economic crime shall mean crime targeting economic order and its functioning, where economic instruments are being abused;
- Economic crime shall mean any crime of perpetrators active within the economic life of society;
- Economic crime shall mean any crime in the area of economics; this comprises not only crimes specified in Chapter II of the special section of the Penal Code, but also selected crimes described in Chapter X of the Penal Code, if carried out within an economy."

In addition to books, economic and financial crimes are also discussed in periodicals. Issue no. 6/2011 of the "Auditor" magazine was dedicated to economic crime. In the *"Psychologie dnes" magazine no. 10/2006, Čírtková states that: "At the time typical while collars are slipping towards unfair, criminal practice, they have had successful professional and social career and repeatedly had to overcome strong competition within various selection procedures. The work career of white collars requires personal qualities that are hardly compatible with ordinary street crime."*[37]

A specific term we can come across is "financial crime". This type of crime may be encountered in the area of:
- Banking and financial institutions;
- Capital markets;
- Evasion of tax and other mandatory payments;
- Falsification of checks, currency, and other means of payment.

In general, financial crime may be defined as one that attacks the financial system, i.e. institutions that form such system. Financial crime differs from economic crime as follows: it affects specific areas of the economy, i.e. money and securities as assets that may be easily stolen.

The above mentioned specifics of financial crime predetermine a special group of perpetrators, but also of victims. The special feature that you can identify with perpetrators of financial crime is the fact they directly dispose of the assets that form the subject matter of their crime, i.e. exercise factual powers over such assets, even if such powers are only entrusted. With regard to victims, who recruit from virtually all social classes and groups, the effects of such illegal financial actions are usually devastating. However, despite these differences, financial crime may be referred to as a subcategory of economic crime. It has a specific place within economic crime, particularly in terms of the area of its operation on monetary and capital markets in the context of collective investments in connection with the activities of banks, investment companies and funds, securities dealers, and pension funds.

In financial institutions, all operations are supported by information technology. Crime may be closely related to the use of such technology. In 2007, Jírovský[38] published a book that informs readers interested in the area of illegal attacks on computer systems, viruses, worms, Trojan horses, and misuse of data flows or intrusions into remote computers about the real danger relating to data.

---

36 CHMELÍK, J. et al. *Úvod do hospodářské kriminality*. 1st Edition. Prague: Vydavatelství a naklad. Aleš Čeněk, s.r.o., 2005. 167 pages. ISBN 80-86898-13-X. (Introduction to economic crime).

37 ČÍRTKOVÁ, L. Finanční zločinci. [online] *Psychologie DNES*. 2006, No. 10. [quoted on 21 May 2012]. Available from: http://www.portal.cz/scripts/detail.php?id=20138. (Financial criminals).

38 JÍROVSKÝ, V. *Kybernetická kriminalita – nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1st Edition. Prague 2007. ISBN 978-80-247-1561-2. pp. 91 et seq. (Cybercrime – not only about hacking, cracking, viruses, and Trojan horses without any secrets).

Cross-border forms of economic crime

None of the forms and methods of financial crime is confined to one state. Swiss banks generated slush funds for the purpose of illegal financing of political parties and there is a suspicion that some of the money "leaked" into the pockets of private individuals.[39]

According to statistics available on the FBI website[40], 5628 financial institutions did in fact fall victim to theft, robbery, or larceny in the total amount of USD 43 million in 2010. More than 5000 of these damaged financial institutions were commercial banks. 5363 cases consisted robberies at branches (their counters), usually located in commercial zones or shopping centers. In most cases, alarms and cameras were functional (and activated), i.e. technology aimed at preventing robberies and at facilitating their subsequent investigation. In about 1500 cases, perpetrators used firearms; in 3096 cases perpetrators verbally threatened to use weapons.

The winners of the imaginary competition for the largest financial swindler of the past decade also come from the United States, specifically Bernard Madoff and Allen Stanford. The whopping USD 65 billion embezzled by Madoff represents the largest amount in the history of American finance so far that someone bilked their clients out of. Longstanding icon of financial traders, Chairman of the Board of Directors of the company Bernard L. Madoff Investment Securities, founder and former Chairman of the American Stock Exchange NASDAQ, and the leading figure of the New York Jewish philanthropy, Bernard Madoff rightfully takes the first place on our imaginary list of biggest embezzlers.

Victims did not include just banks and institutions, such as Japanese Nomura or English investment bank HSBC, Swiss BNP Paribas, but also clients of the Spanish bank Santander, or the Steven Spielberg Foundation. They are followed by about five thousand deluded "retail" investors, largely consisting of celebrities of the American society.

However, the way in which Madoff managed to deceive the world for decades, is not unusual. His "investment" company was nothing but a Ponzi scheme, known as the "plane scheme" in the Czech Republic. The principle is that the money received for management from new investors is used to pay interest attributable to deposits received from the earlier ones.

In 2008, financial crisis hit. Until then, for long seventeen years, most clients did not need their money and enjoyed the accrued interest. However, the crisis was also associated with more significant withdrawals of the funds. And the system began to crumble. Madoff was not able to repay initial investments to all applicants; the court then found Bernard Madoff guilty of fraud and embezzlement of USD 65 billion.

The Faculty of Law at the Trnava University in Trnava is the home to prof. PhDr. Gustav Dianiška, whose name is associated with a publication published in 2011. It talks about economic crime in the Slovak Republic. It is a set of nine essays that tackle the economic crime in the Slovak Republic from different perspectives, including economic aspects, their specificities, prevention, and more.

39 EIGEN, P. et al. *Kniha protikorupčních strategií*. Praha: Transparency International, 2000. 117 pages. p. 8. (Book of anticorruption strategies).

40 Reports and Publications. [online] Federal Bureau of Investigation [quoted on 20 May 2012] Available from: <http://fbi.gov/stats-service/publications/>

Baloun[41] published a fairly extensive work, with several chapters devoted to offenses against the banking system and capital markets. However, he focused on individual cases, such as Moravia Banka, IPB, and others. Similarly, he presented case studies from the capital market. With regard to the Czech capital market, he divided the offenses, from the perspective of time: as follows: the period of privatization and the period of the standard function of the capital market. He performed a categorization of perpetrators; it revealed the fact that banks are extremely vulnerable to risks from various social groups and social environments. It is logical that less sophisticated methods (armed robbery of funds amounting to about CZK 100 mil. or minor credit frauds of hundreds of thousands), albeit illegal, are associated with a significantly lower social dangerousness than in case of sophisticated crime. Furthermore, such more elaborate crimes are often difficult to prove and thus unpunished - despite the fact it concerns huge amounts (the amount of CZK 500 billion is usually mentioned – i.e. about 70% of the state budget).

For example, the bankruptcy of Private Investors in May 2001 affected about 2500 clients, who lost about one billion Czech crowns, as the company declared unexpected bankruptcy on 21 May 2001. At first, the company management only stated that the reason for the bankruptcy related to adverse developments on American stock markets. However, they later admitted trading with funds that the company obtained in the form of loans in return for the clients' securities. As the business speculations failed, the brokerage firm was forced to sell clients' assets and pay outstanding debts.

The media constantly inform us about new cases of crime related to financial transactions. For example, according to Hospodářské noviny[42], business with misused bills of exchange is blossoming in the Czech Republic. The reason for this is the fact that clients provided blank bills to dealers of two (installment) companies as security for loans amounting to tens of thousands of Czech crowns. Amounts in the bills were missing and when clients repaid their loans, the companies did not return the bills. Instead, they filled in amounts and resold them. The problem affected approximately twenty thousand people.

Hospodářské noviny[43] also give another example: Conmen steal the identity of customers. Identity theft takes place as follows: an offender obtains personal data by advertising offers to provide nonbank loans on the Internet. He/she then elicits a photocopy of an identity card/driving license and an account statement from an applicant (maintained with another bank in the applicant's name).

The perpetrator then sends such obtained copies of documents to a bank, in which he/she intends to open an account in another person's name. Together with the number of a newly opened account, the bank informs the perpetrator that the account will be activated after at least one Czech crown is sent to it from an existing account. This is a confirmation for the bank, in line with rules set down by law, that the identification data match the data on copies sent.

To meet this condition, the perpetrator asks the nonbank loan applicant to transfer at least one Czech crown from his/her existing account to a specific account (newly opened for the perpetrator by the bank). After the payment is received, the bank sends a key and password for online banking to the perpetrator, allowing him/her to control the account - without the original person interested in the nonbank loan knowing about the existence of an account opened in his/her name.

---

41 BALOUN, V. *Finanční kriminalita v České republice*, Partial study under the project "Research of economic crime", Prague, 2004, Institute of Criminology and Social Prevention, 2004. 183 pages. ISBN 80-7338-029-3. pp. 18 – 53 and 54 – 88. (Financial crime in the Czech Republic).

42 *Hospodářské noviny* no. 089 of 7 May 2012, p. 1.

43 *Hospodářské noviny* no. 088 of 4 – 6 May 2012, p. 1 or Czech Republic affected by identity thefts. Frauds will open an account in your name. [online] MAFRA, a. s. Updated on 4 May 2012. [quoted on 22 May 2012]. Available from: <http://ekonomika.idnes.cz/cesko-zasahly-kradeze-identit-dkl-/ekonomika.aspx?c=A120504_085107_ekonomika->.

In the final phase of the fraud, the perpetrator only informs the applicant that his/her loan was not granted and discontinues any further communication. The common feature is that the bank, the perpetrator, and the applicant do not come into direct personal contact with each other. All communication takes place solely in electronic form or via telephone, whereas the perpetrator usually uses specially set up email addresses and anonymous prepaid cards for individual cases.

Statistics on the prevalence of economic crime

Another typical feature and a warning sign could be the fact that a perpetrator is trying to appear as a reputable provider in his/her online loan offer; however, it is impossible to find any references about him/her through publicly available sources.

Ernst & Young experts performed an objective survey to map the current situation. In the period of 4 January – 1 February 2011, they addressed a total of 2365 respondents from 25 European countries. The survey took place on the Internet, via telephone or by means of a personal interview, and it included listed companies or multinational companies with more than 1000 employees. The objective of the survey was to find out how companies manage the risks associated with fraud and corruption under the present, rapidly changing legislative and economic terms and conditions.[44]

More than a third of addressed employees of large European companies are willing to offer a bribe, give a personal gift, or pay above standard expenses to get a contract. The situation is even more alarming in the Czech Republic: more than half of Czech managers admit unethical conduct for the purpose of obtaining a contract. Therefore, it is not surprising that 83% of Czechs require stricter oversight by regulatory and government authorities. However, only 6% of them believe that regulatory authorities are willing and able to effectively prosecute corruption. Unlike the representatives of the countries of Western Europe, fewer Czechs believe that company's good reputation pays off.

Overall, 8 of 10 respondents in the Czech Republic agree that corruption is widespread in our country (European average is at 62%). In terms of Europe, bribery in the business sector may most likely be encountered in Greece (44%) and Russia (39%), while Norway (6%) and France (5%) are among the countries where bribes are least common. In total, 41% of surveyed managers stated that extra representation expenses are justifiable in order to obtain a contract (17% on average in Europe). One third would be willing to consider a bribe to get a contract (17% on average in Europe). In the Czech Republic, one of three managers and 23% of all respondents would be willing to offer a bribe to secure a contract. Employees believe that unethical behavior is perceived with much more tolerance than ever before and that anticorruption measures are less and less emphasized. At the same time, good reputation and business ethics should be a priority for the management of European companies.

The frustration of employees resulting from the management's attitude is best illustrated by the growing calls for tighter oversight by regulators. Overall, 77% of addressed Europeans demand that regulators do more for reducing the risk of fraud and corruption. The numbers are even higher in countries most affected by the recent economic crisis – more than 80% of respondents ask for stricter supervision in Portugal, Ireland, Spain and Greece.

Only 6% of Czech respondents believe that regulators are willing and able to effectively prosecute corruption and 41% of respondents think that the regulators do not wish to combat corruption. Respondents believe that regulators are unwilling or unable to prosecute corruption, stating that corrup-

44 European companies underestimate increased risk associated with frauds and corruption [online]. Ernst & Young Global Limited. Updated on 24 May 2011. [quoted on 20 May 2012] Available from: <http://www.ey.com/CZ/cs/Newsroom/News-releases/2011_Europeanfraudsurvey_CZ_>.

tion and fraud are too widespread to be combated effectively (50%) or that the relevant authorities do not have the necessary powers (44%).

The fear of sanctions by the regulatory authorities should not be the only reason for the management to emphasize ethical behavior. The results of the survey show that honest and fair conduct can also have commercial benefits. Three quarters of the respondents indicated that it is beneficial for a company if it is viewed as a "fair player". In comparison with the European average (66%), the percentage of the Czech respondents, who believe that good reputation is a plus for a company from the business perspective, is significantly lower (37%). The result is a sad report card on the state of competition in the Czech Republic.

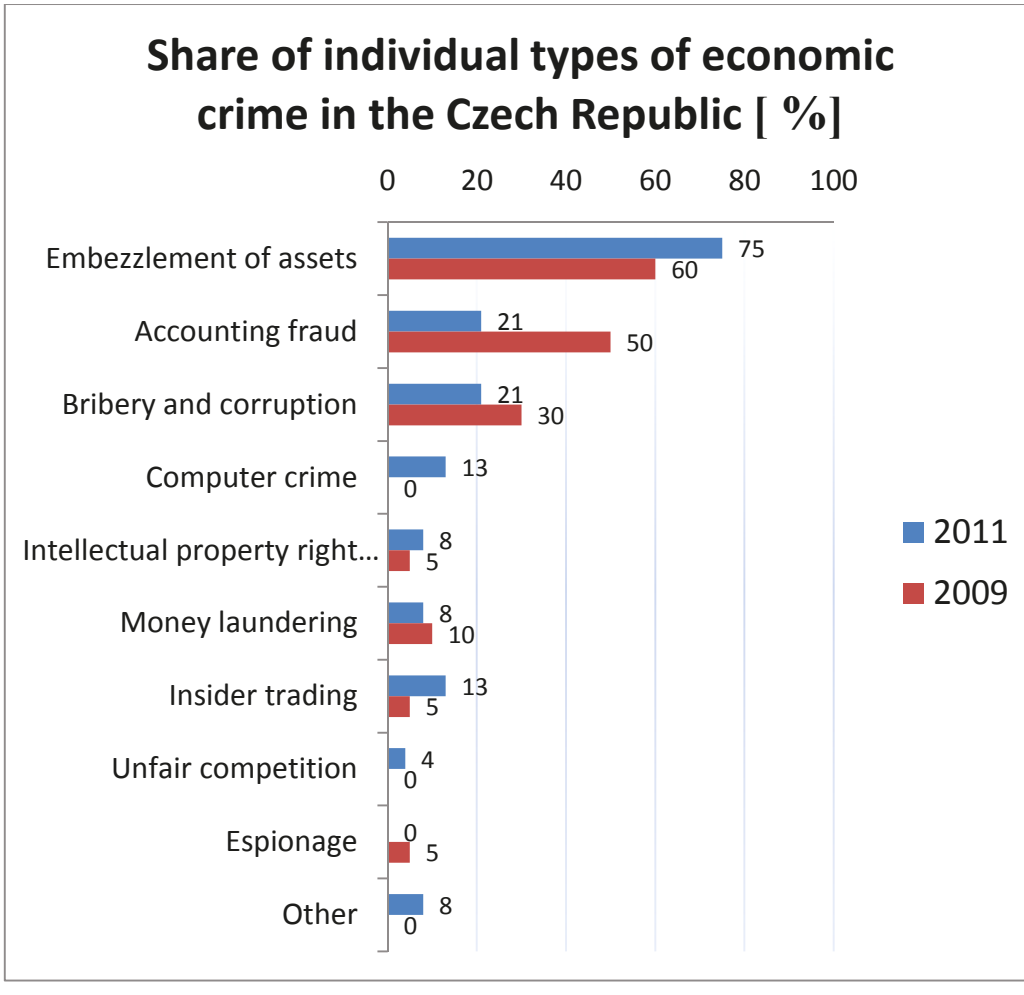
In connection with the crime relating to companies and banks, we have come to use the term economic crime, even though most of us have no detailed information about the contents of this term. However, even the professionals/experts often define economic crime differently. Sometimes, we can come across the term "economic crime" (*note: same in English; however, in Czech "ekonomická kriminalita" vs. "hospodářská kriminalita"*). However, this should not confuse us, as they are synonyms of one and the same illegal phenomenon. Another view of economic crime was presented in a study by the leading audit and consulting firm PricewaterhouseCoopers (PwC). One of the study results is shown below as the "Conclusion from research".

The chart below shows that embezzlement of assets remains the most common type of economic crime in the Czech Republic (75%). The situation is also the same in Central and Eastern Europe (69%) and globally (72%). This result is not surprising given the fact that embezzlement is generally easier to detect than other types of fraud.

The next most frequent type of fraud in the Czech Republic concerns accounting fraud (21%) or corruption and bribery (21%). Although the proportion of these types of crime compared to 2009 decreased, when we should be creating our conclusions careful. Experience PwC show that the incidence of bribery and corruption is probably much higher, because the fraud is very difficult to identify and often remain undetected. Compared with the average of Central and Eastern Europe achieved in 2011 (36%) also indicates that the result for the Czech Republic will probably reach higher levels in real terms.

Although the proportion of these types of crime declined compared to 2009, we should be careful when it comes to conclusions. The experience of PwC suggests that the prevalence of bribery and corruption is probably much higher, because this type of fraud is very difficult to identify and often remains undetected. Furthermore, a comparison with the average of Central and Eastern Europe for 2011 (36%) also indicates that the result for the Czech Republic will probably reach higher levels in real terms.

Figure 1: Conclusion from research of PricewaterhouseCoopers (PwC)



Source: PwC

In addition to the view of journalists and conducted surveys, there is another, significantly more objective view of economic crime. It is based on statistics or analytically oriented monographs. For example, in 2008, Tomášek[45] characterized the structure of crime in the Czech Republic using information from the Police Presidium as follows:

- Property-related 63%;
- Economic 9%;
- Other 6%;
- Violent 5%;
- Immoral 1%;
- Remaining 16%.

45 TOMÁŠEK, J. *Úvod do kriminologie*. 1st Edition. Prague: Grada Publishing, a.s., 2010. 214 pages., ISBN 978-80-247-2982-4, p. 68 (Introduction to criminology).

The statistics of the Ministry of the Interior show that economic crime is observed in about sixty different groups. Numbers shown in the table "Selected crimes in 2011" were published for 2011. The statistics[46] show that in the context of banking operations, there were more crimes related to unauthorized possession of payment cards than in connection with credit fraud in 2011. There were no crimes identified for securities and investment instruments.

Table 1: Selected crimes in 2011; source: ownelaboration based on Statistical overviews of crime for 2011

Name (characteristics)	Total crimes	Explained	Damage (CZK thousands)
Embezzlement	337	171	1 035 012
Fraud	699	333	2 372 622
Misuse of information	17	5	86 698
Unauthorized possession of payment cards	281	50	75 478
Bribery	108	97	197
Favoring creditors	3	0	0
Unauthorized issue of securities	0	0	0
Tampering with the price of investment instruments	0	0	0
Credit fraud	115	63	1 258 222
Fraud with subsidies	24	14	223 691

Source: Available on 25 May 2012 from: http://www.policie.cz/clanek/statisticke-prehledy-kriminality-za--rok-2011.aspx [online]. Updated in 2012

Summary

More sources basically agree that prevention may be defined as a set of measures that are to prevent certain undesirable phenomenon, in this case the legalization of proceeds from crime. The main principles of prevention under the fight against legalization of proceeds from crime, which are applied in banking, include the following:

- Know your customer;
- Understanding the presented transactions, verification of their economic justification and assessment of associated risks;
- Transaction assessment from the perspective of the client's standard profile that should be known to a bank.

The focus of prevention relating to money laundering is mainly rigorous and high-quality processing of comprehensive internal procedures aimed at eliminating all forms of legalization of the proceeds from crime as well as a system for analyzing information about clients and their transfers of funds and other transactions, including the sharing of such information with all departments of the given bank.

46 Statistical overviews of crime for 2011. [online] Police of the Czech Republic. Updated in 2012 [quoted on 25 May 2012]. Available from: <http://www.policie.cz/clanek/statisticke-prehledy-kriminality-za-rok-2011.aspx>.

3.6 Fraud in public administration – not just politically exposed persons

Introduction

The topic of "know your customer", i.e. a client of financial institutions, logically appears in the majority of papers published in sources dealing with the AML process. However, one can ask if it is not already too late to deal with the problems of money laundering at bank branches and in financial institutions. If our answer is yes, then we must look elsewhere, specifically at sources of illicit funds. But what are these sources? In the European context, unauthorized use of various European funds does not appear to be significant. However, according to the media in the Czech Republic, this is a relatively "popular" source of money for illegal use.

General scheme

The Czech Republic is a small, open, export-oriented economy, with central location in Europe. However, some analysts believe that it is still strongly focused on cash-based transactions, regardless of the development of modern payment methods and means. In some sectors, this allows mixing crime with legitimate business activities. Nonpayment of customs duties, counterfeit of brand-name products, narcotics, and human trafficking are still listed in foreign analyses as the primary sources of laundered assets. This information has been published in databases[47], which also state that the local Czech and foreign organized crime launders money generated from criminal activities using financial institutions within the territory of the Czech Republic. The listed criminal activities usually include theft, corruption, drug trafficking, human trafficking (and sex), tax fraud, and armed robberies. They are predominantly carried out by foreign groups, particularly from the former Soviet republics, the Balkans, and Asia. The area of operations against money laundering in banks was addressed by Schlossberger[48], but he did not deal with the sources of illegal income of banks' clients in detail.

Only some general schemes of the money laundering process include illegal operations with public funds, i.e. fraud in public administration, stealing from public funds, and corruption environment that was created therein. According to the Penal Code, fraud refers to one's enrichment or enrichment of someone else by misleading another person using their mistake, or withholding materials facts, thereby causing substantial damage to third-party property. In general, the public views frauds as any behavior that contradicts applicable rules. This means that, in addition to intentional evasion of imposed rules, this category also includes any behavior that is unintended; however, ultimately contradicts such rules as well. For example, this concerns errors, mistakes, inefficiency, and poor quality of work.

Any fraud, which may be characterized as abuse of one's status or position and which is often associated with the violation of the principle of impartiality in decision making, is generally referred to as corruption. Corruption in Europe is also addressed by the European Commission, for example. Table 1 shows the share of respondents, who view corruption as a social problem in selected countries. The Czech Republic is closer to Greece than to Denmark.

In addition to other authors, the problem of stealing was also tackled by Levi[49], whose works are significant in the field of criminology, criminal law, and prison service. It is useful for research, academia as well as students. It contains an extensive set of essays suitable for gaining an insight into the latest theories and discoveries in this rapidly developing field of criminal activities.

---

47 Money Laundering and Financial Crimes Country Database, p. 107.

48 SCHLOSSBERGER, Otakar. AML procedures in financial institutions - suggestions for changes. In *Platební služby on-line v EU, praktické aplikační problémy elektronických platebních prostředků*. 2012.

49 LEVI, Michael. *Fraud: Organization, Motivation and Control*. Ashgate, 1999. 1036 pages. ISBN 978-18-552-1716-4.

Organized and sometimes also unorganized crime (tax evasion of companies) needs to legalize illegally generated money. It uses various financial market entities and other institutions, such as banks in different countries, abroad, and in tax havens. It uses investments in real estate, investment funds, game rooms, as well as the capital market. The circulation of money between financial and other involved institutions leads to the fact that it is ultimately difficult to find the links and connections between one's original crime and their subsequent life of luxury.

Effective tools aimed at detecting fraud and corruption in public administration may radically reduce their occurrence, whereas they should mainly work preventively.

The following areas are suitable for deployment of tools for proactive fraud detection: systems for the collection of taxes and fees, systems for distributing benefits and allowances, i.e. areas that handle larger volumes of funds. It all starts with fraud detection.

During the implementation of the project *"Increasing the effectiveness of procedures and measures for detecting legalization of the proceeds from crime and preventing the financing of criminal structures within the sector of the financial service providers"*, it proved useful to study the three basic approaches to fraud detection, i.e. use of expert rules, use of past data and extrapolation of development into the future, and search for anomalies (particularly during inspections and audits).

Table 2: Share of respondents, who view corruption as a social problem in selected states

Country	Share [%]
Greece	98
Bulgaria	97
Hungary	96
Malta	95
Portugal	93
Czech Republic	88
Spain	88
Ireland	85

Country	Share [%]
Italy	83
Poland	81
Germany	75
Austria	61
The Netherlands	51
Sweden	37
Denmark	22

Source: http://ec.europa.eu/public_opinion/archives/ebs/ebs_325_sum_en.pdf available online on 27 December 2013

Three approaches to fraud detection

The first approach is the use of expert rules, which evaluate the circumstances of transactions (e.g. claim for benefits, medical examination) or properties of the transaction participants. Based on such attributes, the given tool tries to define the range of problematic cases that need to be examined. Expert rules are often not very effective and lead to too many "false" alarms or large number of unidentified cases.

The second approach consists in extrapolating past data and building a predictive model that estimates the probability of fraud/error existence in the given case, in line with past data on fraud and errors. The model requires the so-called training set, for which we in fact know the cases that involved fraud and the cases that were fine. In case high-quality training data on fraud and errors from the past exist, these methods are very effective, reliable, and also available with the use of statistical applications. The disadvantage and limitation is the quality and quantity of the training data set. To prepare it really well requires a lot of time and quality expert team.

The third approach is to identify anomalies: we examine data to identify cases, which clearly deviate from a comparable group. In principle, it works on the basis of a simple idea that similar cases should behave similarly. In case different conduct is identified, there must be something that has caused it - maybe it is a data error or it may appear to be different, because data are missing, and maybe it is a fraud. It is necessary to examine the given case. The model success rate depends on the cooperation between statisticians and experts in the field of fraud detection.

Financing fraud detection tools

The actual deployment of tools for active fraud detection has a strong preventive effect, increases the efficiency of systems for distributing funds, and strengthens citizens' confidence in these systems. Their success depends on the systems, to which they are deployed, and the degree, to which fraud had previously been combated. The experience from around the world shows that the return on investment in such instruments ranges in months.

Naturally, the issue relating to the funding of these instruments is also important. One of the relatively innovative and not commonly used models is the so-called "benefit sharing" model, where the supplier remuneration is determined as a share in generated savings. This model does not bring any investment costs for the contracting authority, with the exception of costs of cooperation with the given supplier. To ensure such model is successful, it is necessary to define in detail the term savings, how to measure them, and set up a number of procedural and organizational rules. Many details must be considered; this will ensure that the idea of "covering the project costs via a share in the generated savings" will translate into reality and both parties will be satisfied.

Corruption and public resources (funds)

Public resources represent the volume of money that is needed for a functioning state, i.e. its ministries, government, and social services. However, it also seems to be a very interesting source of illicit funds that may be used for corruption.

The surge in illegal transactions relating to public administration in the Czech Republic was caused by resources from European funds intended for regional development. Billions from European funds attracted the interest of local businesses and initiated the establishment of structures that provided these businesses with access to regional politicians who influenced the allocation of such European funds. Their activities resulted in corruption and overpriced contracts, i.e. processes referred to in the world as a form of organized crime. This was also confirmed by the 2012 Annual Report of BIS[50], which focused on two main aspects of organized crime in the Czech Republic - dysfunction of government (public administration) authorities and activities of regional structures relying on clientelism. Under no circumstances should the described phenomena be regarded as something new in 2012. Many of the reported adverse effects have been present in the society – in various forms and shapes - at least since the end of the last century. Among others, BIS registered activities of groups using illegitimate methods to affect the top decision-making authorities of the state administration, local governments, and the legislative process in the Czech Republic, all this in a manner that negatively affected the performance of the state's fundamental functions. According to BIS, the structures of organized crime have, systematically and for a prolonged period of time, ensured outflow of funds from public budgets. To do so, they use, for example, subsidies, public contracts, and public services outsourcing. In particular; however, they were able to influence important decisions of state and local authorities that concerned infrastructure projects, grant programs, public contracts relating to the provision of public services, or the legislative process itself. BIS believes that organized crime in the Czech Republic successfully uses

50 2012 Annual Report available on 29 November 2013 at http://www.bis.cz/n/2013-11-07-vyrocni-zprava-2012.html

a state, which may – in simple terms - be characterized as a fundamental absence of factual personal accountability of representatives of state/local government authorities and of representatives elected by citizens for the decisions made.

According to BIS, the gloomy state also results from the generally low respect for the law and the absence of certain legal regulations in some areas or legislation implemented through laws that were subject to heavy lobbying and thereby regulation "tailored" to certain interest groups.

In the view of BIS, one of the key signs of the public administration dysfunction is the conflict of interest, which was most frequently registered in the course of allocation of the European grants from operational programs and allocation of public contracts. It concerned a direct interconnection of members of companies' statutory bodies, to which public contracts or European grants were awarded, to public entities that allocated such contracts or grants.

Therefore, the European funds create a specific environment for corruption. Their official objective is to promote economic development of regions, where GDP per capita is lower than 75% of the EU average, or regions that are dealing with restructuring. The amount of money is interesting and, in some regions, it really promotes the development of business activities, education, and protection and maintenance of historic buildings or historic town centers.

It is clear from the table of the utilization of expenditure in the Czech Republic in the period of 2004 - 2006 that no problems with the use of the European funds were identified in the previous programming period, whereas the funds were used to the maximum.

Table 3: Allocation of financial resources from the funds during the programming period of 2004 – 2006

Operational programs and funds	Allocation for the period of 2004 - 2006 (EUR)	Utilized from the allocation (EUR)	Utilized from the allocation
Total	1 692 594 657	1 684 759 313	99.5 %

Source: http://www.strukturalni-fondy.cz/cs/dostupný online of 20 September 2010

At the same time; however, the European Commission was busy working on an audit strategy. The joint audit strategy was first adopted in 2005 and was based on the recommendations in the Commission Communication of August 2004 on specific steps for ensuring support of comprehensive audit methodology for audits performed by services departments of the Commission under the shared management system. Its objective is, if practicable, to synchronize as much as possible the audit strategy for funds in individual countries and encourage a common approach in order to achieve uniform focus of audit work. This was considered particularly important for the stage of preparation for the closure of the programming period 2000 - 2006 and for structuring the audit in the programming period 2007 – 2013. The audit strategy covered three programming period, specifically 2007-2013, 2000-2006, and 1994-1999, which are subject to three different legal regimes.

Key objectives for activities of audit units in respect of the funds

The key objectives for activities of audit units of all institutions that manage structural funds is to gain adequate assurance that the management and control systems set up and implemented by individual member states and stated admitted to the EU:

a) Comply with the requirements of Community regulations;

b) Operate effectively – i.e. they are able to prevent and detect errors and discrepancies and ensure legality and rightness of expenditure reported to the Commission.

In case errors are identified within the systems, clear recommendations are given for corrective measures and, in severe cases and/or where appropriate measures are not taken immediately, the payments are stopped and financial corrections are made.

Overall risks

The management of structural projects is associated with the inherent risk, if it is ensured by a large number of organizations and systems and if it includes a very large number of diverse transactions. This condition is fulfilled when it comes to work with EU funds in the Czech Republic. As of 5 June 2013, applicants submitted 70,053 applications for grants from the Structural Funds and national funds for individual projects amounting to a total of CZK 1,264.8 billion.

The main risk in the financial management of structural projects consists in the fact the Commission cannot detect all cases of ineligible expenditure reported by some of the states, because it lacks adequate documents.

For any expenditure, the risk is affected by:

a) Significance of the relevant expenditure;

b) Credibility of the management and control systems of member states or admitted states;

c) Quality, quantity, and nature of audits carried out by the audit authorities of member states or admitted states;

d) Nature and complexity of management and control systems and co-financed operations.

This risk is mainly reduced by reliable financial management and control systems, certification of the expenditure adequacy by the responsible authority of a member state or admitted state, framework rules for suspension of payments or application of financial corrections in connection to the findings of subsequently performed audits, measures taken to simplify the legal/regulatory framework, and measures taken in the areas of leadership and training for all persons involved in the work with money from the EU funds.

The systemic risk is usually minimized by implementing good audit strategy at the national level and in the EU as a whole. Implementation of a good audit strategy provides foundation for the management of identified risks and implementation of corrective measures. It also supports the creation of system improvements that should lead to error rate reduction.

Utilization of funds during the programming period 2007 – 2013

Tightening of the audit strategy led to the fact that the certification of expenditure relating to the implementation of projects financed from operational programs listed in Table no. 4 in the period of 2011-2013, whereas the requests for reimbursement were not sent from the Czech Republic at all.

Table 4: Overview of suspended certification of expenditure

Operational Program (OP)	Operational Program Management Body	Certification suspension date
ROP*/North-East	Regional Council (RC) North-East	25. 3. 2011
ROP Central Bohemia	RC Central Bohemia	22. 5. 2012
ROP Central Moravia	RC Central Moravia	16. 1. 2013
ROP North-East	RC North-East	16. 1. 2013
Integrated OP	Ministry of Regional Development of the Czech Republic	16. 1. 2013
ROP Moravia-Silesia	RC Moravia-Silesia	17. 1. 2013
OP Enterprise and Innovation	Ministry of Industry and Trade of the Czech Republic	17. 1 2013
OP Prague–Adaptability	Prague City Council	4. 4. 2013

** ROP - Regional Operational Program.*

Source: http://www.strukturalni-fondy.cz/getmedia/ available online on 17 September 2013

The main reasons, why the utilization of resources from the European funds is unsatisfactory, are known:

a) Improper setup of implementation structure;

b) Complexity and initial absence of methodology;

c) High fluctuation of personnel;

d) Significant problems in the project management of beneficiaries, quality of tenders, appeals of individual unsuccessful candidates, periods of the Office for the Protection of Competition;

e) Conclusions of audits conducted by the European Commission that uncovered errors in the program setups;

f) Unclear interpretation of inspection/audit results.

The Ministry of Regional Development of the Czech Republic considers the above listed causes to be relevant. However, independent analysts come to the conclusion that regional clientelism systems that focus on ensuring the outflow of funds from public budgets have penetrated the public administration on the regional level as well as the business community. The development of regional clientelism was significantly promoted by multiple overlapping of offices/functions and the resulting interconnection of ROP bodies with regional authorities and local governments, minimal personal accountability of regional representatives in ROP bodies, and the absence of independent substantive inspections with regard to effectiveness of projects applying for grants.

Conclusion

We can generally say that the view of corruption in society may be distorted. On the one hand, we must state that corruption - as any other negative phenomena in society – concerns each citizen. It is not an

isolated phenomenon that appears just "somewhere". Corruption practices can be found at all levels public administration – i.e. municipality – region – state, as well as in other areas. One of the effective methods that can minimize corruption is to combat this negative phenomenon at the lowest levels already. However, this requires personal accountability of every citizen and every elected representative of citizens, properly set control mechanisms, as well as high-quality work of auditors.

3.7 Can we identify "invisible" financial market participants?

The "know your customer" principle is very important from the perspective of a bank; however, it is only one side of the coin for mutual trust between a bank and its customer. From the perspective of a bank's customer, the "know your banker" principle is equally important. This essay is mainly devoted to first mentioned principle, which is used to build trust in the area of banking.

Identification of a bank's customer is only a small part of the extensive issue of fairness, integrity, and efficiency of the financial market, but it certainly is an essential part of the banking practice. We also should note that the "know your customer" principle, i.e. a microeconomic issue from the perspective of a bank, necessarily has broader implications for the macroeconomics of a bank or for the entire banking sector, as appropriate. If one or several banks neglect the principle of prudential business activities, it can have significant adverse consequences for the entire national economy. Regretfully, the European banking scene has recently been documenting just that.

In addition to standard participants in the financial markets, there may also be certain entities that cannot always be identified or cannot be identified sufficiently reliably. This may concern individuals or legal entities, which are referred to as the so-called individual entities (clients) in this paper.

These "invisible entities" shall mean entities that use the opportunity – either through legal means or by breaching applicable regulations – to either partially or fully hide their true identity. The most common crimes, which are committed by such invisible entities, include fraud, theft, and other iniquities.

The "know your customer" principle applies not only to financial markets, but virtually to any kind of business activities: every businessman should know his business counterparties - customers and suppliers, intermediaries, and basically all other persons, with whom he or his company trades. The level of detail of information collected about them depends on his decision, facilities, and, last but not least, the costs associated with such process. It usually pays off to know your "counterparty".

It is absolutely essential for a bank to know its clients – i.e. its "counterparties" in the position of loan applicants, ergo prospective debtors, or in the position of depositors, ergo prospective creditors.[51] This is even more important for banks than for other businesses, mainly because banks are responsible for entrusted depositors' funds and may not manage such funds improperly, i.e. may not expose them to unnecessary risk. In terms of lending, banks can never be too careful, which is eloquently documented by various scandals relating to non-performing loans that cannot be "hidden" off balance sheet without risk - as a key under a doormat.

In the past decade, the counterparty risk has increased and is not declining even now - as documented by various recent international surveys. Recently, risk management has become one of the bank's management priorities, if not the number one issue.

---

51 International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations. [online] Financial Action Task Force. 1990 [cit. 5. 10. 2012]. Available from: <http://www.fatf-gafi.org>.

The term "invisible clients" may be further categorized based on their individual roles they might play using their invisibility. One of the best known categories of these invisible entities is the category of the so-called straw-men, whose role is to conceal or disguise the true identity of their supporters, godfathers, bosses, and various managing officers in the hierarchy of crime. This category of people represents mere "wage earners". They always stand in the front line when dirty work is needed and they also tend to be swept away first. The hierarchy of invisible entities also includes the category of "accomplices", teammates or members. Therefore, the actual transactions are usually decided by other persons, whose true identities are even more difficult to identify than those of straw-men.

In practice, there are several different approaches to resolving the issue of banking clients' identities:

- State ensures the safety of the financial sector by issuing regulations, which define activities deemed illegal, thereby making it possible to punish their perpetrators. In doing so, the state seeks to create favorable environment in the financial markets, while also addressing the protection of consumers of financial services: it imposes obligations on banks that must be met in respect of consumers. Banks are required to following applicable regulations and protect consumers, i.e. their customers;

- Banks protect themselves from theft and fraud to avoid damage to their assets and losses from insufficient protection of their clients, as they carry on their shoulders not only the counterparty risk, but also the regulatory risk, reputational risk, and other risks (as appropriate) – based on the specific situation of the given bank;

- Banks' clients are primarily to protect themselves, but they are not always able to do so due to their indifference, laziness, and financial illiteracy.

With regard to the protection of their security against invasions of invisible clients, banks can presently rely, among others, on the results of new research on consumer behavior and their scientific analysis.[52] More recent research that tries to answer the question of how to increase the safety of financial services consumers, rely on the assumption that it is useful to divide the protection of security of such services into several parts.

The following components are necessary for an effective system for the protection of financial services consumers:

- Physical prevention measures;

- Account monitoring;

- Agency monitoring;

- Password security;

- Risky behavior avoidance.

These components are almost orthogonal, which causes the tendency of consumers to only select one of the said elements of behavior; however, they are not interested in any other components. As a result

52 Some forms of offenses associated with banks such deals: BALOUN, V. *Finanční kriminalita v České republice*. Dílčí studie úkolu „Výzkum ekonomické kriminality." Praha: Institut pro kriminologii a sociální prevenci, 2004. 183 p. ISBN 80-7338-029-3. pp. 18 – 53.

of this bias of consumer behavior, there are serious gaps in the overall system, which is intended to protect them against fraud and identity theft. Therefore, when instructing and persuading financial services consumers, it is necessary to strive to make consumers realize that, to ensure the protection of their identity against its theft and against fraud, they must learn to use all of the above mentioned components of behavior, thereby minimizing the potential risks and losses.

Nature of financial markets and selected impediments associated with identification of its participants

Financial markets comprise of a complex, amply structured set of relations. In addition to their common features, which help them to form a single unit, individual market segments also have a number of specific features that differentiate them. For example, these specific features consist in the fact that individual segments differ in terms of products (financial instruments), type and number of participants, different transparency, the way they operate, and undoubtedly in terms of their respective significance. Contemporary financial markets are dynamic; today's high volatility in some of their segments (especially the financial derivatives market) is higher than in the past, leading to higher risks.

Financial markets are exposed to the risk of different types of illegal activities. Invisible clients of banks and other financial market institutions, usually well aware of the specific conditions existing in the individual market segments, can take advantage of these specifics in their favor. Given that the level of regulation of individual market segments of the financial markets is not the same today, whereas the transparency individual segments also varies, it is safe to assume that the ground for illegal activities is better in in certain submarkets than in others.

In order to gradually limit illegal operations of financial market participants, who can be classified as the so-called invisible entities, the knowledge of specific features of individual market segments is particularly important. Although this paper mainly deals with the banking sector and banking markets, a slight detour may prove useful: we will briefly describe some types of markets, characterized by lower levels of transparency and regulation; it is safe to assume more opportunities for illegal activity in such markets.

In terms of the topic we address, it is namely useful to distinguish legal markets from markets on the edge of legality, and clearly illegal markets. The issue of invisible bank clients mainly concerns illegal markets. There are attempts to access the legal markets by holders of financial assets (especially cash funds) generated from activities in different financial markets, who cannot fully prove the origin of these assets, as it may be just barely legal.

Some types of markets are also called by their "color" as black market, gray market, or white market. The "black" market tends to be associated with the so-called underground economics ("basement" economics, controversial speculation, profiteering, illicit dealing, etc.),[53] which mainly blossoms in times of various economic disturbances, wars, etc. The designation of markets using different colors is associated with an attempt to distinguish the different nature of such markets. In the financial markets, the market "color" recognition and the related "colorblindness" (whether pretended consciously or unknowing) is usually associated with the area of "laundering" of money originating from gray or black markets.

The problems associated with insufficient identification of clients can also be found in the area of the so-called shadow economy and the associated finances/funds and shadow banking, which presently exists in parallel with the "official" banking.

53 ŠÁMAL, P. et al. *Podnikání a ekonomická kriminalita v České republice*. 1st Edition. Prague: C. H. BECK, 2001. 776 pages. ISBN 80-71794-93-7. pp. 438 – 475. (Business activities and economic crime in the Czech Republic).

The shadow banking emerged in the United States in the 1970s, with the emergence of money market funds. Accounts of these funds, which record financial assets in noncash form, usually have a similar to bank deposits; however, these funds are not subject to banking regulation.

Shadow banks may provide loans to traditional banks even cheaper than it is customary on the inter-bank market, because they have lower costs due to their specialization. Furthermore, shadow banks may also provide loans to people, who could never get loans from regulated traditional banks. Due to unclear boundaries between different types of financial assets existing in cash and noncash form, the system of shadow banks may receive financial funds (often from invisible clients) that eventually materialize in the form of cash.

The framework of shadow banking currently includes so-called hedge funds, money market funds, and so-called structured investment funds (structured investment vehicles - SIV).

The share of the shadow banking, which operates throughout the world today, in the volume of the global banking system is estimated at about 25-30% The value of this essentially unregulated sector, which amounted to USD 27 trillion in 2002, amounted to USD 60 trillion in 2010.[54]

Given the problems caused by the shadow banking, regulators in the United States and Europe seek to strengthen regulation of the sector. The final measures relating to the area of regulation and supervision in respect of shadow banks should be prepared by the end of 2012 in the United States and in the European Union.

The main objection against the shadow banking today is that it played a destabilizing role during the global financial crisis; due to the lack of regulation, activities of shadow banks endanger the national and international financial stability and increase the level of systemic risk.

Lord Turner sees the following three major risks of shadow banking: 1) pro-cyclicality of shadow banking; 2) nontransparent transformation of loan maturities in long complex chains; and 3) confusing relationship between funding and market liquidity.[55]

Table 5: Development of the share of shadow banking in the Czech Republic (%)

Country/Year	1999	2000	2001	2002	2003	2004	2005	2006	2007	Average
Czech Republic	19.3	19.1	18.9	18.8	18.7	18.4	17.8	17.3	17.00	18.4

Source: SCHNEIDER, F., BUEHN. A., MONTENEGRO, C.E. Shadow Economies All over the World. New Estimates for 162 Countries from 1999 to 2007. [online] The World Bank Development Research Group. July 2010. WPS5356. [quoted on 15 September 2012]

Quasi-banks (non-banks) that operate within the contemporary banking do not have a full banking license or they are not subject to the supervision of either a national or international regulator; they provide a range of financial services. These institutions include non-bank loan providers, some exchange offices, pawnshops, issuers of certain types of checks, etc. Certain regulation is also being prepared for these types of businesses; it will aid in reducing the number of controversial transactions that are just barely legal.

54 Shadow Banking Agenda Should Have "Bias Against Complex Interconnectivity" – Lord Turner. [online] Financial Services Authority. Published on 15 March 2012 [quoted on 5 April 2012]. Available from: <http://www.icffr.org/Resources/News/Shadow-Banking-Agenda-Should-Have--Bias-Against-Co.aspx>.

55 ibid.

In some types of financial markets, where banks as well as quasi-banks operate, the problem of clients' identifiability turns into a different problem: whether a bank actually wishes to identify a client or not, i.e. a problem of compliance with identification rules and regulations. In this regard, differences exist between licensed banks and quasi-banks (non-banks) in terms of the stringency of identification requirements. In the category of non-banks, these requirements are less rigorous, the discipline of non-banks tends to be looser, there are more opportunities for inflow of illegally generated funds into banks and their legalization, whereas potential sanctions for non-banks are significantly lower if any at all.

Role of systemically important financial institutions for the financial markets integrity

Problems associated with complications in identifying clients of banks and other financial institutions arise, among others, from the differences of national legislation and from limited application of international agreements/treaties aimed at tightening the obligations of financial institutions in terms of thorough client identification.

Particularly large, systemically important financial institutions, with significant economic power in the given economy, may play an important role in resolving the problem of invisible clients.

Some of the large international banks, which are currently included in the list of the so-called global systemically important financial institutions (the so-called G-SIFIs), formed the so-called Wolfsberg Group[56] in 2000. These banks came together to developed certain standards and associated products for the entire "financial industry". The standards and products relate to the following areas:

- Policies relating to the obligation of banks to know their customers;
- Anti-money laundering policies;
- Counter terrorist financing policies.

The objective of the Wolfsberg Group, which represented the crème de la crème of the international banking elite at the time, was an attempt to influence further development of existing regulations in a direction that was to reflect more the interests of involved banks, particularly in the area of private banking. Even at the time the Group was formed, the participating banks were among the most influential global banks, i.e. they were banks with substantial importance for the development of the banking sector worldwide and their activities had a significant impact on the safety of financial assets of the wealthiest groups of people in the world.

The Wolfsberg Group comprised the following 12 large international banks: ABN AMRO, Banco Santander, Bank of Tokyo-Mitsubishi UFJ, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, JP Morgan Chase, Société Générale, and USB. Upon formation of the group (in 2000 at the Swiss castle of Wolfsberg), the so-called Wolfsberg Principles were prepared and adopted with the participation of leading experts (including representatives of Transparency International). The first phase of works resulted in anti-money laundering policies, intended for private banks, which were published in October 2000 and revised in May 2002.

56 Wolfsberg News (14 October 2011) [online]. Wolfsberg Group [quoted on 28 April 2012] Available from: <http://www.wolfsberg-principles.com>.

In 2004, the global banks united within the Wolfsberg Group in cooperation with the Bankers' Almanac)[57] created a central location (the so-called central repository) for storing initial information the member banks require in performing inspections relating to transactions with counterparties (so-called due diligence). The repository assists banks in operating in compliance with the provisions of banking regulations by providing them with the services of specialists, who are engaged in combating illegal transactions ("money laundering") and have access to centralized information. The repository comprises around 36,000 different documents that contain information on nearly 11 thousand financial institutions in the world. Furthermore, the repository also features information on bank ownership, structure of various banking groups, data on banking sector regulators, and on banking products and services.

Table 6: Overview of documents of the Wolfsberg Group of global banks

Year	Document title
2002	Statement on the Financing of Terrorism Wolfsberg Anti-Money Laundering Principles for Correspondent Banking
2003	Wolfsberg Statement on Monitoring Screening and Searching
2004	Due diligence model for financial institutions, in cooperation with Banker's Almanac
2006	Guidance on a Risk Based Approach for Managing Money Laundering Risks AML Guidance for Mutual Funds and Other Pooled Investment Vehicles FAQ on AML issues in the Context of Investment and Commercial Banking FAQs on Correspondent Banking FAQs on Beneficial Ownership, Politically Exposed Persons and Intermediaries
2007	Statement against Corruption
2008	FAQs on PEPs (refreshment)
2009	Trade Finance Principles Guidance on Credit/Charge Card Issuing and Merchant Acquiring Activities
2011	Wolfsberg Anti-Corruption Guidance[58]
2012	Wolfsberg Private Banking Principles Wolfsberg FAQs on Intermediaries Wolfsberg FAQs on Beneficial Ownership

Source: Wolfsberg News (14 October 2011) [online]. Wolfsberg Group [quoted on 28 April 2012] Available from: <http://www.wolfsberg-principles.com>.

57 Due Diligence [online] Bankers' Almanac [quoted on 16 May 2012] Available from: <http://www.bankersalmanac.com/addcon/products/due_diligence.aspx>.

58 Wolfsberg Anti-Corruption Guidance Paper August-2011 (published).pdf. [online] Wolfsberg Group [quoted on 28 April 2012] Available from: <http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg%20Anti%20Corruption%20Guidance%20Paper%20August%2018-2011%20%28Published%29.pdf>.

The repository is used to store copies of banking documents that relate to the following facts:

- Copies of bank licenses and licenses of their subsidiaries or other official confirmations that banks can carry out banking transactions;
- Copies of documents relating to the governance of banks (such as internal bank regulations, excerpts from the Commercial Register, CVs of members of the bank's management and senior managers);
- Copies of documents relating to the policy of banks and correspondent banks in the area of legalization of proceeds from crime and documents on relevant procedures banks apply;
- USA PATRIOT Act Certification for banks, which are required to be certified in this manner;
- Bank's latest annual reports and annual report of its subsidiaries;
- Questionnaire of the Wolfsberg Group on "money laundering".

To demonstrate the scope of business activities of the largest international banks, we present selected data for two of these banks (although we understand that such data cannot be generalized for other banks).

HSBC (founded in 1865) has its banking network in 85 countries on all continents. Its shares are listed on stock exchanges in London, Hong Kong, New York, Paris, and Bermuda. Shares of HSBC Holdings plc are held by over 220,000 shareholders in 132 countries. The number of customers of the bank is estimated at 89 million people.[59]

Although HSBC strives to maintain excellent reputation, it recently failed to prevent several scandals. For example, according to the findings of the American Senate subcommittee – HSBC had supposedly laundered money for Mexican drug traffickers using accounts at HSBC branch in the Cayman Islands since 2005.

Barclays Bank (Barclays PLC) is a large British international bank based in London. It was founded in 1690 and is one of the oldest banks in England. Today, the universal bank has more than 4750 offices in more than 50 countries around the world. Around 1,600 banking branches are located in England. The bank is listed on the London Stock Exchange (as one of the largest listed companies, currently 22nd on the list). It is also listed on the New York Stock Exchange. At the end of 2011, its market capitalization amounted to GBP 21.8 trillion. However, this bank was not able to avoid numerous problems either. In terms of recent scandals, the bank breached money laundering regulations by maintaining an account for a son of an African country's president within its Paris branch, with various financial machinations taking place in the account. In 2009, the bank attempted tax evasion; after the given conduct was revealed, the bank had to pay a fine of GBP 500 million in 2012.[60]

However, one of the largest recent financial scandals is the fact that there has been tampering with the LIBOR interbank interest rate on the part of a number of major international banks for several years. The bid rate is calculated as the average of the rates, at which banks in the London interbank market lend money to each other; overall, 18 banks are involved in the compilation thereof. For the time being,

59 HSBC. [online] HSBC Bank [quoted 28 February 2012]. Available from: <http://www.hsbc.com/1/2/about/network>.

60 *Barclays Bank told by Treasury to pay £500m avoided tax*. [online] BBC News. [quoted on 28 February 2012] Available from: <http://www.bbc.co.uk/news/business-17181213>.

investigations relating to the tampering with the aforementioned rate have included Barclays Bank, Deutsche Bank, Société Générale, HSBC, and Credit Agricole. However, the investigations have not been completed so far.[61]

This unpleasant affair documents just how far the actual noncompliance with the fundamental principles of banking may lead. In case large international banks declare their commitment to the compliance with agreements on the fight against financial crime and to various codes of conduct, while also breaching these agreements and codes, it demonstrated both the moral decay and insensible, reckless, and greedy conduct of senior executives of some banks.

Summary

The "Know your customer" banking principle is always applied under certain conditions of time and place; these conditions have been subject to rapid development in the last decade, with the common denominator being the general tendency towards their tightening and strengthening of ties to other "golden rule", such as "due diligence". The process of getting to know a client (in various possible forms) is not just about identifying "individuals", but mainly about proving the origin of their financial assets and, after an account is opened, also about the monitoring of transactions executed from such account.

We believe it is beneficial to deal not only with these rules, but also to examine the broader financial market environment, where bank transactions with various clients (including the so-called invisible clients) take place. The tightening of bank regulation, focusing on narrowing down the field for potential impairment of the financial markets integrity, will be accompanied by efforts to interconnect more closely all parts of the existing system within a single unit and clarify the mutual interrelation of its individual components.

In a sense, this leads to a change of the very concept of banking regulation, which, in a broad sense, will include enhancing the transparency of banking activities (also by amending the concept of banking secrecy, with introduction of certain limit thereto, by stepping away from the anonymity of owners of shares, etc.), promotion of the fight against corruption (associated with changes in the area of banks' management and administration), taking into account the fact that tax fraud or mere tax omissions tend to be an initial step to money laundering (cf. upcoming changes in the FATF regulation in this area), and the inclusion of a number of other elements.

In this paper, we have also pointed out the extremely important role of large international banks, which should also play the role of watch dogs/guardians of the financial markets integrity; however, they have unfortunately not been too successful so far. It turns out that even really complex and rigorous regulations that also contain sanctions are sometimes not sufficient to make the invisible become "visible", that the evil will have to be rigorously punished. In order to attain this objective, two instruments should mainly be used: education and prevention.

61 I.e. until September 2012

3.8 Will the legal entity identifier contribute to safer operation of the global financial markets?[62]

Introduction

The safety of undertakings on the financial markets is one of the ancient problems that each individual addresses based on existing capabilities. "Safety" of the financial markets operations has many possible forms. Presently, the fight against financial crime and drugs tends to be accentuated. However, even if no events of criminal nature took place in the financial markets, the financial markets might not be "safe", as there are always various risks in the financial markets, such as those given by the nature of the market mechanism, number of participants, their behavior, and many other factors including well-established rules that must be followed for the market to operate properly.

To ensure the functioning/operation of modern financial markets, it is necessary to guarantee, among others, that the state is able to provide the participants - clients of financial intermediaries – with effective protection. However, it is also necessary to protect the financial institution, both from incorrect decisions, which are unavoidable, but also from "imperfections of the financial markets", from systemic defects that greatly increase the risk and uncertainty.

In this paper, I wish to focus on these "imperfections", which influence "safety" of the financial markets in a broad sense, i.e. factors that increase associated risks and reduce financial stability.

Some aspects of "safe" operation of the financial markets

The problem of "safe" operation of the financial markets has many different aspects and dimensions; it may be further broken down into the following components, for example:

a) **Technical** aspects of the financial markets operations: reliable functioning of the market mechanism supported by reliable technical equipment - hardware and software - not only in the course of trading, but also during other activities, such as settlement, clearing, central depositary activities, central counterparty operations, etc. In many regards, the proper functioning of the financial markets is subject to proper functioning of their infrastructure. The security of technical equipment of institutions operating in the financial markets can significantly contribute to the reduction of market risks (particularly counterparty risk), operational risk, and systemic risk;

b) **Economic** aspects of the financial markets operations: in this case, the main prerequisite is effective functioning; this assumes identification of cost savings, for example by achieving economies of scale, introducing innovations (technical, economic, and organizational), etc;[63]

c) **Legal** aspects, ensuring the financial markets operations (functioning) by means of first-rate regulations, their maintenance and timely renewal, which assumes their adaptation to the level of technology and requirements for economic efficiency;

---

62 This paper has been prepared under IGA VŠFS entitled "Adequacy of financial markets infrastructure and ways of its further development (with special consideration of the situation in the Czech Republic)", project number 7427.

63 Innovation processes on stock exchanges: PAVLÁT, V. *Globální finanční trhy*. Prague: VŠFS, edition EUPRESS, 2013, pp. 94-98. ISBN 978-80-7408-076-0. (Global financial markets).

d) **Personal** profile (psychological aspects) of the financial markets' participants, ensuring appropriate ("correct") conduct of the financial markets users; it also comprises, among others, the necessary level of financial literacy.

e) **Social** aspects are not only associated with the functioning of trading in the financial markets, but also with the functioning of the broader financial market infrastructure elements (rating, media, research, education). Modern markets cannot operate without effective and efficient financial infrastructure.

As an alternative diagram of the protection of the financial market and its participants, it is possible to present the following simple model, for example:

Table 7: Schematic illustration of the financial markets safety system

Criterion	
Protection object:	WHAT to protect?
Protection subject	WHO to protect?
Protection process:	HOW to protect?
Area:	WHERE to protect?

Source: Author's own elaboration

Note: It is necessary to distinguish national and international safety nets.

The safety of operations of the modern financial markets cannot be assured without adequate financial regulation. In recent years, significant changes have been taking place. Let us present at least two:

a) Former approach was characterized by the micro-prudential nature of regulation, while the current approach also puts emphasis on macro-prudential nature of regulation; this change has had a major importance for the functioning and safety of the financial markets and has already been institutionalized;

b) In the past, considerable emphasis was placed on repression; today, it is prevention that is in the core, with self-governance and advances in the area of management and administration of financial organizations playing a major role.

Roughly since the late 1970s, there have been significant efforts of the financial markets' participants apparent to increase the safe operations of these markets. There was a gradual development of tools, rules, procedures, mechanisms, and systems for the elimination of markets' "imperfections".[64]

These "emergency elements" (referred to as "safety nets")[65] were introduced with a view to ensure benefits for the national economy, in favor of the financial markets' participants and the public as a whole.

64 PAVLÁT, V. *Globální finanční trhy.* Praha: VŠFS, edition EUPRESS, 2013, pp. 58-59. ISBN 978-80-7408-076-0. (Global financial markets).

65 MIKDASHI, Z. *Regulating the Financial Sector in the Era of Globalization. Perspectives from political economy and management.* Palgrave Macmillan, 2003, p. 92. 249 pages. ISBN 1-4039-1638-1.

The set of these measures tends to include the following components:

1. Deposit insurance;
2. Function of central banks, ensuring the necessary liquidity and effective functioning of payment / settlement systems;
3. Investor protection;
4. Compensation to insurance policy holders and beneficiary of pensions;
5. Compensation of some losses caused by natural disasters;
6. Protection of private companies from selected risks;
7. Recapitalization measures aimed at overcoming insolvency of key financial institutions.

International efforts aimed at increasing the safety of the financial markets operations

The recent global crisis has resulted in a considerable pressure on the intensification of efforts for establishing preconditions for national and international financial stability, i.e. efforts for increasing the "safety" of the financial markets operations.

In terms of these efforts, various heads of state meetings under different groups, such as G-8 or G-20, played an important role. The meetings addressed the most pressing problems of international relations and particularly sought consensus in preparing measures to mitigate the impacts of the global financial crisis. Some Summits have played a crucial role for the adoption of many decisions that may positively affect the long-term global development. One of the successfully resolved problems is, for example, the fact that a major breakthrough was achieved with regard to the international agreement Basel III, which is gradually being implemented within the agreed steps. Table no. 8 lists the G-20 Summits, which have apparently had positive effects for further development, even in the financial sector.

Table 8: Chronology of important international Summits

Year	Dates	Country	City	Host leader
2008 – 1st	November 14 – 15	United States	Washington D. C.	George W. Bush
2009 – 2st 3st	April 2 September 24 – 25	United Kingdom United States	Londýn Pittsburgh	Gordon Brown Barack Obama
2010 – 4st 5st	June 26 – 27 November 11 – 12	Canada South Korea	Toronto Soul	Stephen Harper Lee Myung-bak
2011 – 6st	November 3 – 4	France	Cannes	Nicolas Sarkozy
2012 – 7st	June 18 – 19	Mexiko	Los Cabos	Felipe Calderón
2013 – 8st	September 5 – 6	Russia	Strelna, Saint Petersburg	Vladimír Putin
2014 – 9st	TBA	Austrálie	Brisbane	TBA
2015 – 10st	TBA	Turecko	TBA	TBA

Source: Protocols of the respective Summits

The Summits in Cannes and Los Cabos were the most significant in terms of addressing the issues of financial stability, systemic risk, systemically important financial institutions, and introduction of the global legal entity identifier.

Current problems regarding financial stability and global identifier construction

One of the important articles of the final communique from the G-20 Summit in Cannes includes a requirement for the establishment of rules concerning the liquidation of large financial corporations to ensure that taxpayers do not bear the costs of their failure. As of 2016, additional requirements are to be set down for the global SIFIs relating to the absorption of losses. It was agreed during the Summit that the list of systemically important financial institutions would be published each year.[66] The Summit also supported the idea of creating a global financial entity identifier and commissioned the FSB (Financial Stability Board) with the preparation of relevant background materials to be discussed at the next Summit.[67]

The final communique of the Los Cabos Summit reiterated (Articles 42 and 44) the need to regulate the systemically important financial institutions and it was agreed to create global legal entity identifier for financial markets. The task was assigned to the FSB.[68]

Path to financial stability by increasing the regulation of "global" (SIFI) banks

Investigation of factors that affect the financial stability of large banks led, at the end of last millennium already, to important findings about the potential threats that their failure could pose to the national economy. Based on these findings, an opinion emerged that large financial institutions should be subject to better regulation and supervision.

The regulation of large banks, based on the identification of their systemic importance, represents a serious challenge: to find appropriate measures and tools to minimize the potential adverse effects of these giants' failure is not easy.

The system of national regulation and supervision of large financial institutions originally had microeconomic dimension: it consisted in the regulation and supervision of large individual financial units. International regulation and supervision was carried out in the same manner; Basel I and Basel II agreements document this narrow approach. At the end of the 1990s, the situation began to change in favor of a new, systemic approach, which relied on considerations of financial stability: the system of regulation embraced a macroeconomic element. The need for change of the system ultimately resulted in the establishment of new national and international regulatory institutions (Financial Stability Board and others.)

---

66 Cannes Summit Final Declaration – *Building Our Common Future: Renewed Collective Action for the Benefit of All.* Draft of November 4. Cannes, November 4, 2011. Available from: http://www.g20.utoronto.ca/summits/2011cannes.html. (Staženo 31.3.2013.)

67 The final communique stated the following: "We support the creation of a global legal entity identifier (LEI) which uniquely identifies parties to financial transactions. We call on the FSB to take the lead in helping coordinate work among the regulatory community to prepare recommendations for the appropriate governance framework, representing the public interest, for such a global LEI by our next Summit." See: FSB. *A Global Legal Entity Identifier for Financial Markets*. Available from: http://www.financialstabilityboard.org/publications/r_120608.pdf

68 For the full text of the communique, see Telegraph. G20 Leaders Declaration - Los_Cabos_Summit. Available from: http://www.telegraph.co.uk/finance/g20-summit/9343250/G20-Summit-communique-full-text.html (Downloaded on 29 March 2013.)

Many measures relating to SIFIs were implemented on the national level during the global financial crisis already. It mainly concerned the following types of measures:

1. SIFI liquidation in the event of failure;

2. SIFI reorganization;

3. SIFI reduction;

4. Reduction of SIF's scope of activities;

5. Increase in taxes aimed at discouraging further growth of SIFI.

However, these measures were generally not consistently applied – also due to some of their possible controversial impacts.

The construction a comprehensive set of tools, methods, and indicators for the SIFI regulation has continued as part of activities carried out by the FSB's SIB committee.

The objective of these activities is:

1. Reduce the probability of SIFI failure and limit its consequences, if it occurs;

2. Reduce the costs of the public sector of any interventions, if they were to be applied.

Two large groups of systemically important banks are currently distinguished for the purpose of regulation and the selection of suitable economic policy. The first group comprises the so-called G-SIFIs, i.e. global systemically important financial institutions. The second group consists of systemically important banks operating within the territory of individual states – i.e. so-called D-SIFIs or domestic banks.

Since this differentiation respects the heterogeneous nature of "global" and "domestic" systemically important financial institutions, it is possible for the governments of individual states to adopt specific measures for the group of D-SIFIs, arising from the different nature of the banking sectors of individual countries.

A practical conclusion results from the classification of the two groups of banks mentioned above: global SIFIs (G-SIFIs) will be permanently required to ensure higher absorption capacity, efficient procedure for their potential liquidation, intensive supervision and existence of robust financial market infrastructure, which is to allow the reduction of the contamination risk. On the other hand, national regulatory authorities still influence the conduct of "domestic" SIFIs (D-SIFIs), as they are competent to adopt own specific measures for their regulation.

The regulation of global SIFIs includes a number of new measures: 1. obligation of large financial institutions to develop recovery and liquidation plans; obligation to enter into specific cooperation agreements on cross-border liquidation of corporations; 2. Regulation implementation is monitored by a special body (Peer Review Council).

In terms of the practical implementation of the above regulatory measures, the following factors are crucial: identification of systemically important banks (whether global or national) and their classification allowing differentiation of the given regulatory measures. The table below briefly illustrates the development of approaches to the identification and classification of SIFIs.

Table 9: Identification and classification of entities based on the criteria of systemic importance

2009	Group 1: Solely based on the aspect of size and concentration; Group 2: Based on interconnection; Group 3: Based on the exposure to correlation risk; Group 4: Large companies, the failure of which could have significant effects for regional economies, even though they are not systematically important; Group 5: Financial institutions not included in other groups, i.e. local (community) financial institutions.
2012 (FSB)	Systemically important banks (SIB): 1. G-SIB – global systemically important banks; 2. D-SIB – domestic systemically important banks – important for the national economies of individual countries.
Prospectively (FSB)	1. Application of the systemic importance criteria to other types of financial institutions is assumed (ie. securities dealers, insurance companies, etc.); 2. Differentiated regulation of individual types of financial institutions is expected; 3. Introduction of national discretions for the regulation of domestic entities is assumed.

Source: Author's own elaboration

Note: For illustration of the development of criteria for the systemic importance of banks, see Pavlát, V. Cesta ke globálním trhům a její peripetie. In: 6. Mezinárodní konference o finančních trzích, VŠFS, 29 – 30 May 2013. (Path to global markets and its peripety)

he FSB published the first official list of systemically important banks in November 2011 (without differentiating the SIFIs as global or domestic). A year later, in November 2012, another list was published, already containing some new, very important elements.

The list of November 2012 is newly arranged: banks are categorized into 5 groups in terms of the required degree of banks' ability to absorb the loss of registered capital – specified as a percentage of risk-weighted assets for each group of banks. Group 1 remained empty in 2012. The Financial Stability Board intends to issue another list of systemically important banks in November 2013.

Table 10: New list of systemically important banks (G-SIBS)

Group 5 (3.5%)	**Group 2 - (1.5%)**	**Group 1 (1.0%)**
(empty)	Bank of America	Bank of China
	Bank of New York Mellon	BBVA
Group 4 (2.5%)	Credit Suisse	Groupe BPCE
Citigroup	Goldman Sachs	Group Crédit Agricole
Deutsche Bank	Mitsubishi UFJ FG	ING Bank
HSBC	Morgan Stanley	Mizuho FG
JP Morgan Chase	Royal Bank of Scotland	Nordea
	UBS	Santander
Group 3 (2.0%)		Société Générale
Barclays		Standard Chartered
BNP Paribas		State Street
		Sumitomo Mitsui FG
		Unicredit Group
		Wells Fargo

Source: FSB. Update of group of global systemically important banks (G-SIBs). November, 2012. Available from: r_121031ac.

The approach to the identification of SIFIs has gradually changed in the last two or three years: today, they are characterized by a set of specific characters. More indicators have been developed, among others, used for the purpose of regulation and supervision of SIFIs at national and international level. All these measures relating to systemically important financial institutions are part of a complex of measures in the context of Basel III. The regulation of SIFIs should apply not only to the banking sector, but also to other institutions in the financial sector in the near future.

Legal entity identifier as one of the prerequisites for increasing the financial markets safety

One of the important steps of the Financial Stability Board (FSB), the implementation of which may facilitate the monitoring and influencing of the financial stability at national and international level in the near future (as well as the SIFI regulation in this context), is the construction of an identifier of financial organizations that has not existed within the financial sector so far.[69]

The FSB presented the cited report to the Los Cabos Summit, which approved it and made the decision to implement a system of identifiers.

69 FSB. *A Global Legal Entity Identifier for Financial Markets*. Available from: http://www.financialstabilityboard.org/publications/r_120608.pdf

Legal entity identifier

According to the said FSB report, a financial identifier shall mean a system for the recognition of financial transactions counterparties, which are referred to as "legal entities".

The FSB report views a legal "entity" as a "legal entity of structure, organized under the laws of any jurisdiction". Legal entities also include entities that are responsible for executing financial transactions or have the right (by law) to independently enter into legal agreements. The term "legal entity" is interpreted very broadly: it is viewed as a business, company, possession, partnership, or corporation.[70]

Objective of introducing a financial identifier

The system of a general financial identifier should facilitate easier monitoring of objectives associated with the formation of financial stability.

This namely concerns:

1. Improved management of corporate risks;

2. Better management of micro-prudential and macro-prudential risk;

3. Facilitation and proper execution of company liquidations;

4. Limitation of market abuse and financial fraud; and

5. Achieving higher quality and accuracy of financial data.

Furthermore, the system implementation should also contribute to mitigating operational risk and, consequently, to reducing the usually high costs associated with identification of companies.

Historical conditions of emergence of the global identifier

Various attempts aimed at creating a system used to identify financial institutions date back to the second half of the 1990s. However, they were not successful, so, until recently, the "financial industry" lagged behind other sectors. An unambiguous and reliable identification of financial entities has been virtually impossible until recently, for various reasons.[71]

The global financial crisis was the key impulse for addressing the issue of unique identification of financial institutions, as it shifted the matter of identifying financial entities into a considerably macroeconomic level, because: without the ability to identify financial entities, you cannot effectively cope with systemic risk, with systemically important financial institutions as its most important carriers.[72]

The financial crisis exposed the extraordinary complexity of interrelations of various financial entities,

70 Instead of the term "entity" we sometimes use the term "subject", which is not entirely accurate.

71 Yet: "a standard way to uniquely identify one financial entity from another does not currently exist. A Social Security number distinguishes one John Smith from another John Smith, but at present no single identifier distinguishes one First National Bank from another. Several private companies have developed proprietary identifiers created for their own purposes but none of those identifiers are industry-wide, universal, or strictly focused on identifying a specific institution." See: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1723298

72 See above

while also revealing some of their consequences. If one cannot find out who is actually dealing and trading with whom, not even a strong regulator may effectively intervene in support of financial institutions at risk. In situations, when horizontal relations mingle with vertical ones, when one does not know where individual threads lead to within the maze of different relations, and when this cannot even be reliably ensured, it is extremely difficult to find a suitable solution.

It is also suitable to note at this point that, ultimately, the correct application of the "know your customer" principle depends on whether it is actually possible to identify a client. After all, the situation is similar in case of risk management at the micro-prudential level.[73]

The severity of the situation related to the issue of financial stability – and, in this context, to the issue of insufficient identification of financial entities – is also documented by the fact that these problems were discussed in the American Congress in 2010. In 2010, a fundamental study of Bottega – Powell was published, providing a detailed analysis of the situation relating to the identification of financial entities in the United States and also formulating the most important possibilities of practical solutions at the time. The study served as the basis for proposals of later G-20 Summits.

Principles of functioning of the global identifier system

The system elaborated by the FSB relies on 12 principles ("Global LEI System High Level Principles"). We provide the first 6 principles; the remaining 6 principles are of organizational nature. The Principles are also the basis for recommendations, which are followed in the course of the system implementation.

Table 11: Principles of the system functioning

1. The Global LEI system should uniquely identify participants to financial transactions.
2. The LEI system should meet the requirements of the global regulatory community for accurate, consistent and unique entity identification.
3. The LEI system should be designed in a manner that provides benefits to financial market participants.
4. Flexibility must be built into the global LEI system to provide the capability for the system to expand, evolve, and adapt to accommodate innovations in financial markets.
5. The LEI system should not be "locked-in" with a particular service provider for any key system functions or processes. The principles of competition should be ensured on both global and local levels where appropriate.
6. The global LEI system should support a high degree of federation and local implementation under agreed and implemented common standards.

Source: Cited FSB Report, Annex 3

73 BOTTEGA, J., POWELL, L. *Creating a Linchpin for Financial Data: The need for a Legal Entity Identifier,* p. 4. SSRN--id1723298.

Structure of specific bodies formed for the purpose of the system implementation

The global legal entity identifier system relies on three groups of authorities: (1) Regulatory Oversight Committee – ROC; (2) Central Operating Unit – COU; and (3) Local Operating Units.[74]

Table 12: Structure of the global system

Regulatory Oversight Committee – ROC
Central Operating Unit – COU
Local Operating Units – LOU

Source: Based on the cited FSB (simplified by the author)

Regulatory Oversight Committee (ROC) is the supreme body, which is in charge of management and administration of the entire system. The objective of the ROC is to ensure the system complies with 35 adopted principles and operates in the public interest.

Central Operating Unit (COU) is the basic operating body of the entire system; it is responsible for its superior operations on the basis of approved methods and protocols, which are used to connect the Central Operating Unit with Local Operating Units. The Central Operating Unit has a status of public nonprofit company, financed by the entire financial industry.

Local Operating Units (LOUs) ensure onsite implementation of the global system. The Local Operating Units are also required to protect the locally stored data. Additional entities may connect to the global system via the Local Operating Units. The Local Operating Units may be arranged in a differentiated manner, based on the situation in individual countries: in some countries, only one operating unit might be in operation, with several operating units being used in other countries. Since the Local Operating Units emerge gradually in different countries, it is expected that these units will have to be designed in a manner that ensures adaptation to differences in legislation.

Implementation process

The implementation of the financial identifier project currently continues with the formation of organizational units, as described above. The Regulatory Oversight Committee (ROC) was established in January 2013, with representatives from 35 countries as the ROC members.

Conclusion

In order to ensure real security of financial transactions, it is not sufficient to simply find out whether this or that operation is in line with applicable regulations, i.e. whether it is legal. This comparison necessarily takes place ex post, at the time the economic and financial practice has already advanced to a point that the given regulation may already be so outdated that, according to "common sense", it makes it possible to view criminal activities as legal. The real security of financial transactions in today's world of rapid economic and financial fluctuations is subject to timely identification of the need to change the established system and early/timely response to this need.

In case the economic and financial reality has already left the framework of the originally set system,

74 Legal entity identifier: what else do you need to know? http://www.federalreserve.gov/pubs/feds/2011/201131/201131pap.pdf

it is necessary to identify this "deviation" as soon as possible and to repair the situation through the system revision. It is very difficult, for several well-known reasons (such as, for example, resistance of interest groups, bureaucracy, and tendency towards inertia of the state apparatus, insufficient qualification of officials and legislators that often spawns corruption contamination, etc.); however, it is also often impracticable due to concerns over potential high costs of performing meaningful changes or over political and social impacts.

Some examples of failures in terms of systemic issues in the area of "financial security" in a broad sense include: "pseudo-legal" outsourcing, tampering with the consolidation of balance sheet data, hardly prosecutable tunneling of companies with immediate incorporation of new companies by the same individuals, different projects predesigned to provide their executors with a chance of enrichment at the expense of the society, etc.

In order to ensure real security of financial transactions - whether operations and transactions by individuals, companies, or states – it is necessary, since the very beginning of the formation of various financial security elements as well as entire systems, to incorporate various features aimed at facilitating their control, feedback, and flexibility assurance in such elements/system. With proper public support (and not only on the part investigative reporters who are often only after "exposure"), this could contribute to a faster response of the state apparatus to real signs of financial crime and to the repression thereof.

3.9 Selected problems of detecting the legalization of the proceeds from crime in the practice of financial service providers

Introduction

According to Act no. 253/2008 Coll., on Selected measures against legalization of proceeds from crime and financing of terrorism, the legalization of the proceeds from crime shall mean an activity performed to conceal the illicit origin of any economic benefits from crime with the intention to present the illicit proceeds as legal income. To conceal the illicit origin of any economic benefits from crime, the perpetrators use a number of processes and property transactions with a view to prevent or at least impair the disclosure of the source (origin) of the illicit property benefit, which forms the subject matter of such transactions.

Suspicious transaction – fundamental indicator of potential legalization of the proceeds from crime

In case a financial institution, as the liable entity within the meaning of Act no. 253/2008 Coll., enters into a transaction and such transaction is carried out under circumstances that lead to a suspicion over attempted legalization of proceeds from crime, it is required to identify the parties to the transaction. The Act on Selected measures against legalization of proceeds from crime and financing of terrorism specifies certain facts that make it possible for the financial institution to label such transaction (business relation) as suspicious. It concerns the following facts, for example:[75]

75 Section 6 of Act no. 253/2008 Coll., on Selected measures against legalization of proceeds from crime and financing of terrorism.

a) Cash deposits immediately followed by withdrawals or transfers to other accounts;

b) Numerous transactions performed in one day or in consecutive days and not typical for the given customer;

c) Number of various accounts opened by the given customer which are in obvious discrepancy with their business activities and financial situation;

d) Transfers of assets make no obvious economic sense;

e) Assets handled by the customer which are in obvious discrepancy with the nature or scope of their business activities and financial situation;

f) Account which is not used for the purposes for which it has been opened;

g) Customer's actions which seem to aim at concealing their or the beneficial owner's real identity;

h) Customer or the beneficial owner who are nationals of a country which does not enforce, or fails to fully enforce, measures to combat legalization of proceeds from crime and financing of terrorism; or

i) Customer's identification data the correctness of which the obliged entity has reasons to doubt.

In cases, where a client of the obliged entity is a person, against whom the Czech Republic enforces international sanctions under the Act on the Implementation of international sanctions, the subject matter of the transaction is to involve goods or services, against which the Czech Republic enforces sanctions under the Act on the Implementation of international sanctions, or in case a client refuses to undergo inspection or to provide identification details of the person he/she represents, the financial institution must always identify such transaction as suspicious.

Several other attributes of suspicious transactions resulted from the practice of specific financial institutions, and it is up to the given legal entity to determine, which of them (even if it is the only attribute) would be a reason to consider the given transaction suspicious. The following situations may be considered general attributes of a suspicious transaction:[76]

- Client is nervous, refuses identification or only undergoes it reluctantly, provides false information during his/her identification or inspection (e.g. in terms of the origin of funds or line of business);

- Known criminal past of a client or contacts/ties with people linked to criminal groups or with direct lawbreakers;

- Client has contacts/ties in areas that are risky in terms of money laundering (non-cooperating states, tax havens) or in terms of the application of international sanctions;

- Identification documents appear doubtful;

- Client behaves as if acting for or on behalf of someone else, is accompanied or followed by another person or persons, who apparently wish to remain anonymous;

76 TVRDÝ, Jiří a Adriana BÁRTOVÁ. *Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu a předpisy související.* Prague: Nakladatelství C. H. Beck, 2009, pp. 112-114. (Act on Selected measures against legalization of proceeds from crime and financing of terrorism and associated regulations)

- Client requests unusual or unusually executed transactions, rushes the transaction execution more than is customary in similar transactions, forces cash payment etc.;

- Operation of several businesses with the same line of business and transfers between them;

- Operation of such business, where it is safe to assume ties to criminal groups (erotic services, discos and other nightclubs, trade in military equipment and weapons in particular, etc.);

- Intentional execution of transactions that generate losses;

- Requests for unusual transaction settlement, unusual or questionable payment purposes;

- Nonstandard transactions with securities;

- Transactions involving inadequate contractual penalty;

- Conclusion of contracts with high deposit and their subsequent termination;

- Deposits of several "strangers" to the same account; and

- Repeated opening and closing of accounts in a short period of time.

On the one hand, successful identification of a suspicious transaction depends on the presence of signs indicating potential legalization of the proceeds from crime. On the other hand, it also depends on the individual experience of a financial institution employee dealing directly with the customer, quality of the financial institution's information system, availability of customer information and the possibility to verify it.

Selected statistical data on transactions indicating possible legalization of the proceeds from crime

According to Section 18 of Act no. 253/2008 Coll., in case the obliged entity detects a suspicious transaction in the course of its activities, it reports to the Ministry of Finance; such suspicious transaction notification shall specifically be assessed by the Financial Analytical Unit of the MoF ČR. Total numbers of suspicious transaction notifications, most frequent notifying entities and notification reasons are shown in the following tables.[77]

Table 13: Obliged entities' notifications of suspicious transactions (NST) in 2011 and 2012

Year	Number of NST
2011	1970
2012	2191

Source: FAU Annual Reports

77 Data taken from Annual Reports of the Financial Analytical Unit of the MoF CR for 2011 and 2012.

Table 14: Most frequent notifying entities (suspicious transaction notifications)

Notifying entity	2011	2012
Československá obchodní banka, a.s.	278	281
Komerční banka, a.s.	266	268
Raiffeisenbank a.s.	229	213
GE Money Bank, a.s.	161	143
Česká spořitelna, a.s.	125	129
UniCredit Bank Czech Republic, a.s.	116	143
Total	1 175	1 177

Source: FAU

The comparison of selected statistical data shown in Tables 14 and 15 suggests that about three fourths of all notifications of suspicious transactions are those submitted by large banks within the territory of the Czech Republic.

Table 15: Most frequent characteristics of suspicious transactions (based on the FAU classification)

Suspicious transaction characteristics	2011	2012
Nonstandard deposits and withdrawals (frequency, volume)	648	641
Connection with a crime	410	222
Other	389	449
Surfing and phishing	194	107
Suspicious or nonstandard conduct of a client or accompanying parties	188	203
Transactions not in line with the account nature or client's business activity or financial situation	134	96
Transfers between private and company accounts, business payments to private accounts	119	107
No economic sense of the transaction, including transactions executed by foreign entities	105	89

Source: FAU

Table 15 shows that the most common suspicious transactions in both years are unusual deposits and withdrawals. The category "connection with a crime" may be viewed as linked to other criminal activity, which was accompanied by attempted legalization of the proceeds from crime.[78]

78 Note: Any attempt to legalize proceeds from crime is one of the crimes in the meaning of Act no. 40/2009 Coll., Penal Code, not only Section 216 of this Act.

Views of representatives of selected financial service providers in respect of the suspicious transaction identification

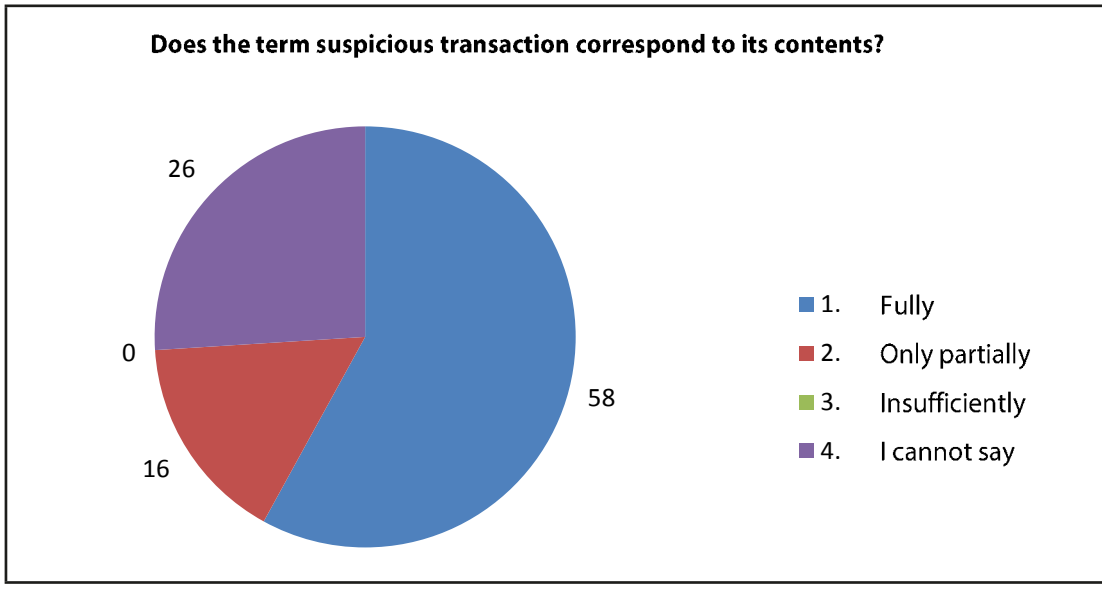
Many financial service providers feature various technical and other system resources that allow the suspicious transaction identification process. However, the final decision on whether a specific business transaction is/is not suspicious is always up to the relevant employee of the financial service provider. To ascertain experience of obliged entities in the area of the suspicious transaction detection, the research team of the project *"Increasing the effectiveness of procedures and measures for detecting legalization of the proceeds from crime and preventing the financing of criminal structures within the sector of the financial service providers"* conducted as a questionnaire survey with selected financial service providers. More than 200 entities were contacted, particularly banks, insurance companies, investment companies, and funds, securities traders, savings and credit cooperatives (unions), as well as the Financial Analytical Unit of the MoF CR.

Definition of the term "suspicious transaction"

The term "suspicious transaction" is defined in Section 6(1) of Act no. 253/2008 Coll., where a suspicious transaction shall mean a transaction the circumstances of which lead to a suspicion of legalization of proceeds from crime or financing of terrorism or any other circumstance supporting such a suspicion. In the questionnaire, we wondered to what extent the term corresponds to its contents.

According to the views, which are shown in Chart no. 1, more than half of surveyed representatives of obliged entities (58%) believe the term suspicious transaction fully correspond to its contents. In their view, this term does not lead to any practical interpretation problems. However, it is surprising that almost one fourth of addressed institutions (i.e. obliged entities) cannot assess the contents of the term suspicious transaction.

Chart no. 1

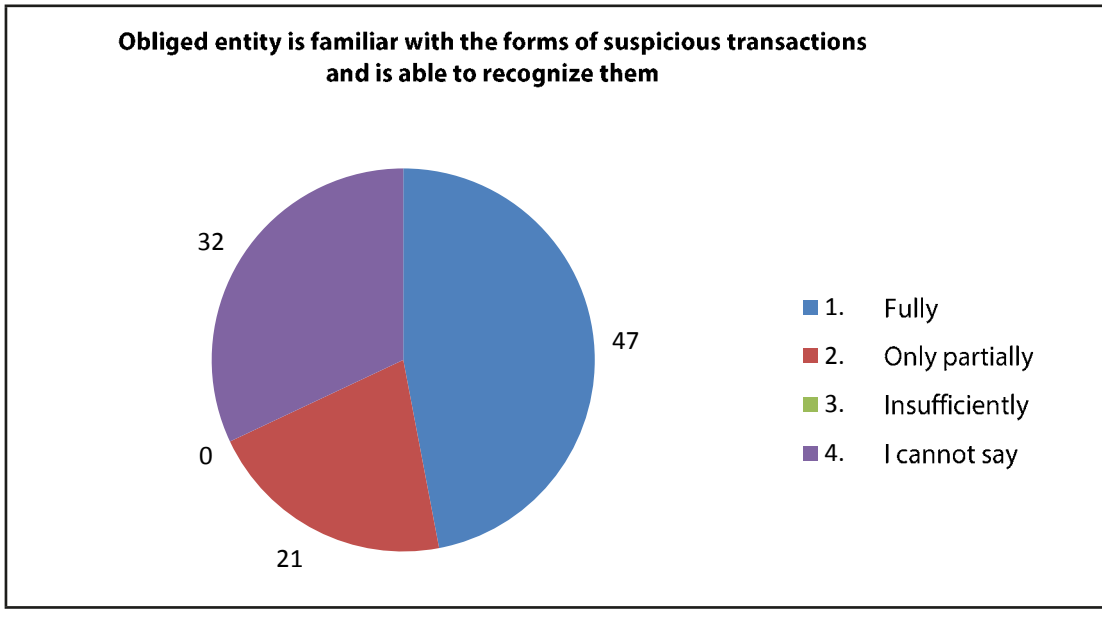


Source: Own research

Forms of suspicious transactions

Nearly one half of surveyed representatives of obliged entities stated that their employees can distinguish specific forms of suspicious transactions, with bank employees being the best. However, almost 32% of respondents were not able to answer this question – i.e. a considerable group (see Chart no. 2).

Chart no. 2



Source: Own research

According to the views of the surveyed representatives of obliged persons, the most common problems in identifying suspicious transactions are caused by different specialization of individual obliged entities (range of obliged entities is very wide). Obliged entities do not have the same lines of business, employee base, capabilities and resources for consistent application of the AML Act. You cannot compare the possibilities and economic interests of big banks in which the application of and compliance with the AML Act provides a separate department in order to eliminate this illegal activity and small currency exchange for two employees.

One cannot compare the potential and economic interests of a large bank, in which the application of and compliance with the AML Act is ensured by a separate department, with a view to eliminate this illegal activity, and a small currency exchange with two employees.

In the event that subjective component – in the form of assessing all circumstances – plays an important role in the decision-making of an obliged entity about suspicious transactions, there is a possibility that one person considers a transaction to be suspicious and another does not. However, the greater "tolerance" arising from such approach subsequently becomes an advantage for high-risk clients, who may prefer financial institutions, where subjective aspects have priority in assessing/identifying suspicious transactions.

With regard to the elimination of the aforementioned, some surveyed respondents mentioned the possibility to also ascertain such generally mandatory data about clients, which could be processed in a way that would maximally eliminate subjective evaluation on the part of obliged entities.

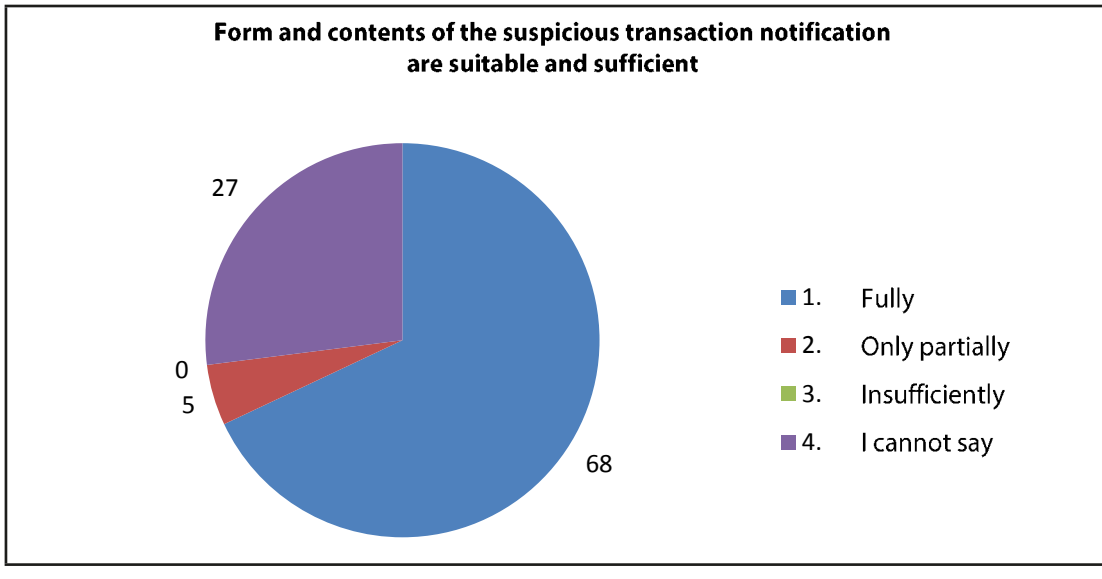
Another way of eliminating more subjectivism in the assessment of suspicious transactions is to insist on required professional qualification of the relevant personnel of obliged entities, e.g. in the form of certification. In particular, it is necessary to motivate obliged entities (e.g. exchange offices, casinos, etc.) to comply with the obligations arising from the AML Act, both through education, lectures or regular training on the part of the body responsible (CNB, FAU, Police) and consistent control application and enforcement of AML for possible use of sanctions.

It is mainly necessary to motivate obliged entities (e.g. exchange offices, casinos, etc.) to comply with the obligations arising from the AML Act, both through education, lectures or regular trainings on the part of the bodies in charge (CNB, FAU, Police of the Czech Republic), and through rigorous monitoring of application of and compliance with AML principles, with possible use of sanctions.

Form and contents of suspicious transaction notifications

More than two thirds of surveyed representatives of obliged entities stated that the form and contents of the suspicious transaction notifications are fully suitable and sufficient.

Chart no. 3



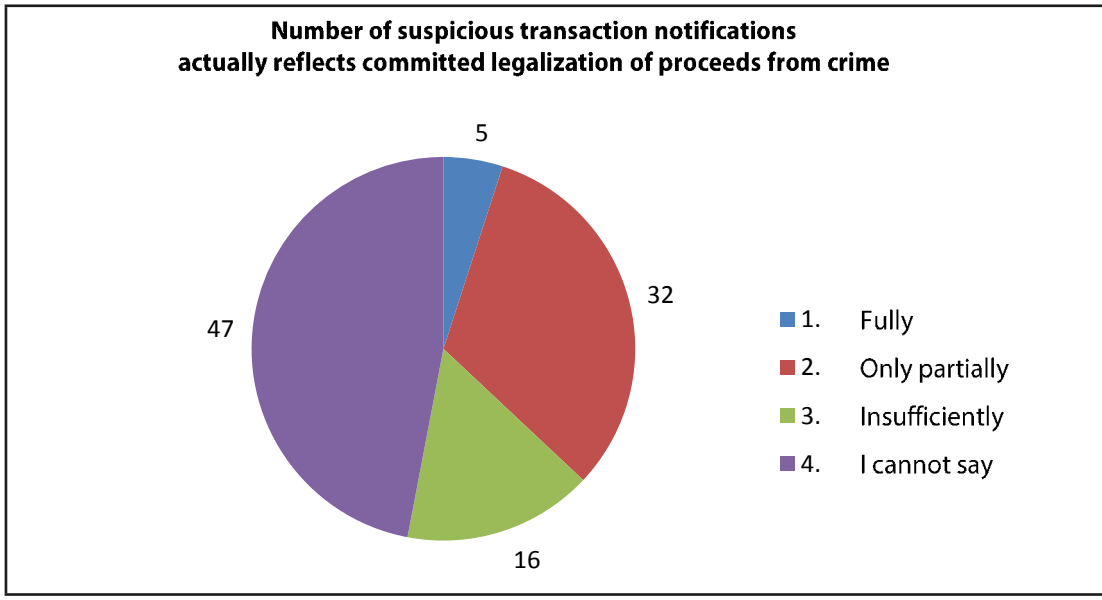
Source: Own research

In cases where the form and contents of the suspicious transaction notifications are insufficient, some surveyed representatives of obliged entities recommend performing full identification of clients and other parties involved in the transaction. Furthermore, they also suggest carrying out identification of accounts, from/to which a transaction is executed, describing all relevant circumstances of a suspicious transaction, which should reflect the seven criminalistics questions,[79] and defining what is viewed as suspicious. The investigation should also feature appropriate attachments, including an account statement in a machine-readable format.

79 **Who** – identification of business transaction parties; **What** – contents of a business transaction; **When** – when does a business transaction take place e.g. payment order is submitted immediately after funds are deposited to an account in cash; **Where** – e.g. a suspicious business transaction takes place at a financial institution's small branch; **How** – e.g. in person or via an intermediary, etc.; **Method** – way of submitting a business transaction, e.g. in writing, via telephone, electronically, etc.; **Why** – motive, reason to execute a suspicious and/or disadvantageous business transaction.

Number of suspicious transaction notifications and actually committed crimes involving the legalization of the proceeds from crime

Chart no. 4

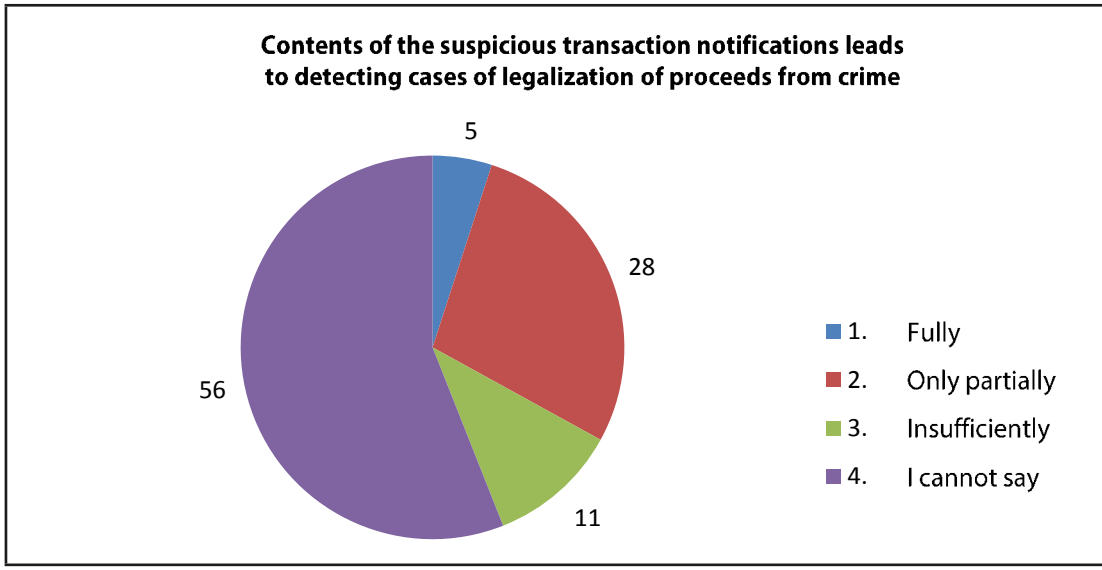


Source: Own research

Only 5% of respondents stated that the number of notified suspicious transactions reflects the real criminal activities involving legalization of the proceeds from crime. However, Chart no. 4 shows one significant fact: almost one half of the surveyed obliged entities cannot assess, whether their notifications in fact reflect the actually committed crimes involving efforts aimed at legalizing the proceeds from crime or financing of terrorism.

About the same number of respondents believes that the contents of notified suspicious transactions fully results in uncovering the cases of legalization of proceeds from crime. This question is illustrated in Chart no. 5.

Chart no. 5



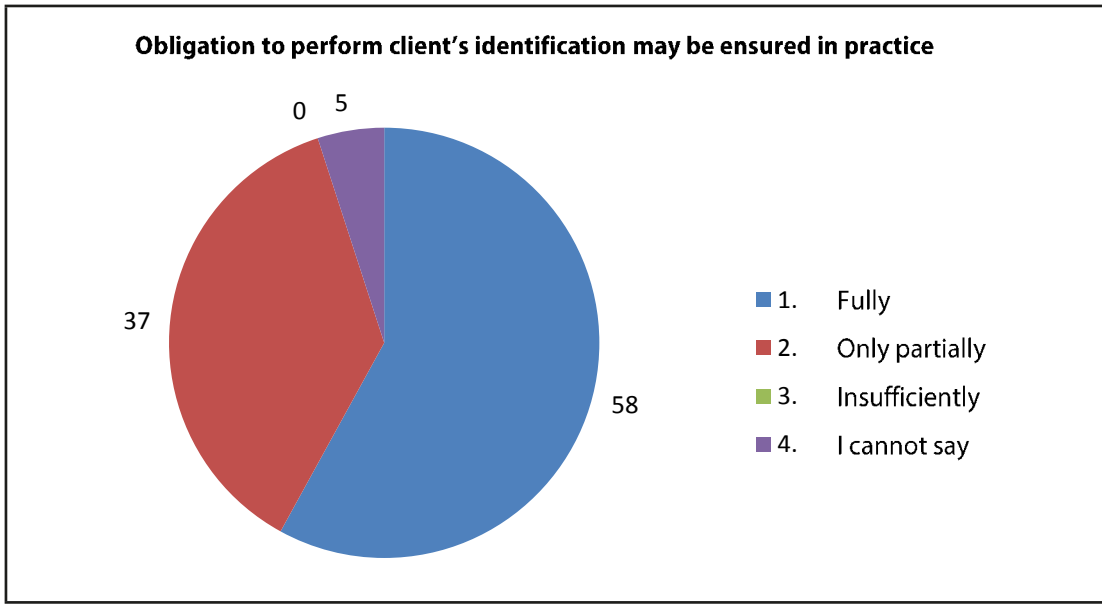
Source: Own research

The given data suggest that employees of obliged entities are apparently not being sufficiently prepared to be able to reveal connection between suspicious transactions and possible legalization of proceeds from crime. Bank employees are most frequently convinced that the contents of the notification of suspicious transactions lead to uncovering the legalization of proceeds from crime; employees of insurance companies are on the other end of the list. Representatives of investment companies are not able to assess this situation at all.

Client identification

In connection with the detection of a suspicious transaction, a financial service provider is also required to identify clients. The analysis of answers provided by surveyed representatives of financial service providers, as shown in Chart no. 6, showed that virtually all respondents agree that it is possible to ensure identification of business partners (clients, customers) in practice.

Chart no. 6

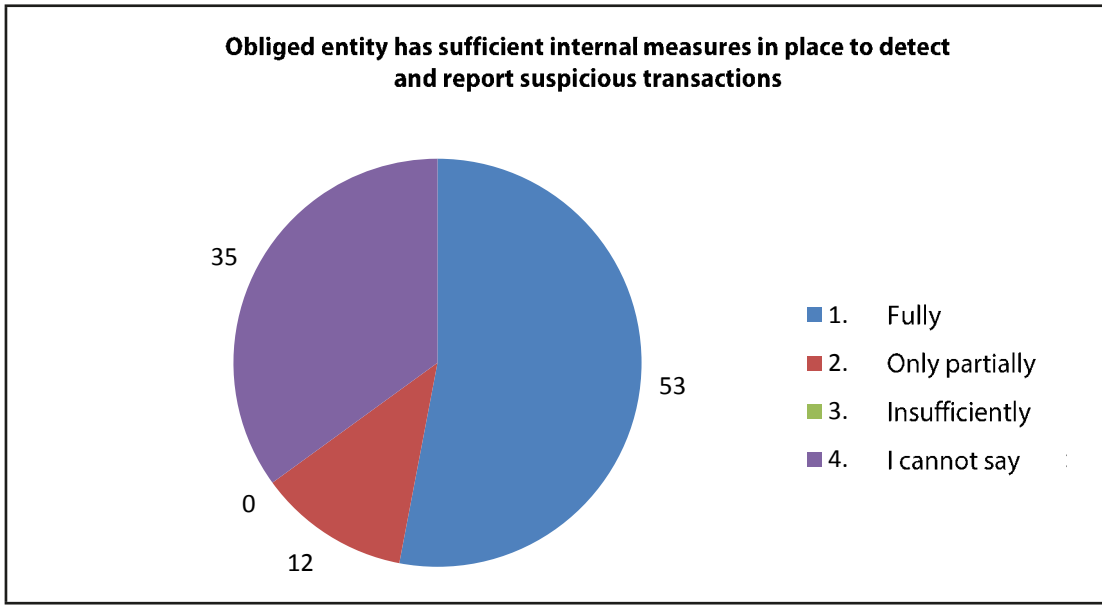


Source: Own research

Internal conditions for identifying and reporting suspicious individuals

Chart no. 7 shows that more than half of surveyed representatives of obliged entities believe their institutions have sufficient internal measures in place for detecting and reporting suspicious entities (i.e. clients). In spite of this; however, nearly a third of respondent cannot assess this. In practice, it may pose some risk in terms of potential money laundering through institutions that are unable to ensure this.

Chart no. 7



Source: Own research

Even though obliged entities have sufficient internal measures in place for detecting and reporting suspicious transactions, only a very small part of these notifications leads to the detection of crimes involving legalization of the proceeds from crime. Out of all received suspicious transaction notifications, only one fifth is submitted to the police in the form of criminal complaints (In 2012, the FAU of the MoF CR received 2,191 notification, only submitting 449 to the police). Various actions of criminal procedure are only initiated in about a half of the submitted suspicious transaction notifications (249). In 2012, only 16 notifications led to criminal prosecution of specific perpetrators.

Conclusion

Overall statistics and results of the survey indicate that suspicious transactions represent a complex phenomenon, which the obliged entities do not absolutely clearly perceive as an indicator of potential legalization of the proceeds from crime. Improvements in this area could be achieved through closer cooperation by financial service providers and the FAU, but also of law enforcement authorities. It is advisable not only to ensure higher popularization of the results achieved by the FAU, but mainly to introduce specialized seminars and trainings on the part of law enforcement authorities for obliged entities, particularly for riskier financial institutions, such as exchange offices and casinos

4. Changes in the process of combating the legalization of the proceeds from crime and terrorism financing

4.1 Introduction

The second chapter discussed existing factors/bases in carrying out activities associated with the prevention of legalization of the proceeds from crime and potential financing of terrorism or criminal structures. The main aspect is both national and especially European legislation. However, very important is the position of the FATF, which – as already mentioned – adopts recommendations (among others) that should be followed by individual countries (and not only member countries) in the form of their incorporation into national legislation.

This section aims to present a brief introduction on national and international legal bases for the area of anti-money laundering and, in particular, to introduce planned legislative changes to the European legal framework in connection to the planned adoption of the new European Directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

The following section will be devoted to risk based approach (hereinafter the "RBA") in the area of fight against money laundering and terrorism financing. This process is based on the newly adopted international recommendations and should be reflected in the applicable legislation of the Czech Republic, but particularly in specific procedures of credit and financial institutions. The RBA should be one of the instruments for effective utilization of resources, both financial and personal, by affected institutions and competent authorities of the Czech Republic (MoF, CNB). Therefore, major resources should be transferred to areas that involve high risk of money laundering (and terrorism financing) or to the area of monitoring of client behavior, trades and transactions that pose high risk, as appropriate.

4.2 Expected legal changes in the AML process

Efforts aimed at preventing the use of the financial system for the legalization of the proceeds from crime or money laundering, if you will, are not new from a legislative point of view. This phenomenon, with destabilizing effects on the legal economy, has been a global threat since the moment money came into existence. Naturally, similarly as other issues, this area has had its own legislative development, which always intermingled with committed crimes and some inventiveness of perpetrators in this case to "clean" illegally generated funds.

Although the first legislative reactions to the problem of money laundering already took place in the United States in 1970s[80], a global normative boom occurred during the late 1980s and early 1990s. As already mentioned in Chapter 2, an important milestone was the year 1989, when G-7 leaders formed a new intergovernmental body at the Paris Summit to combat money laundering, i.e. the "Financial Action Task Force on Money Laundering" (FATF). In 1990, the FATF adopted the so-called "40 FATF recommendations", which are regarded as an international standard in the field of anti-money laundering and are the fundamental pillar for elaboration of individual national legislations around the world, including the European legislation.

80 Bank Secrecy Act (BSA), which introduced an obligation for banks, savings banks, credit and other financial institutions to notify the Internal Revenue Service of any cash transactions over USD 10,000, to identify individuals executing such transactions, and to maintain proper records about them.

The Czech Republic did not adopt corresponding legislative measure until 1996, in connection with the signing of the Strasbourg Convention[81], specifically Act no. 61/1996 Coll., on Selected measures against legalization of proceeds from crime. Following the accession to the EU, it was necessary to implement 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 as well as Commission Directive 2006/70/EC of 1 August 2006, laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of politically exposed person and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis; this took place in 2008, as Act no. 61/1996 Coll. was superseded by Act no. 253/2008 Coll., on Selected measures against legalization of proceeds from crime and financing of terrorism (so-called AML Act). Although subject to several amendments, the Act has been effective to this day.[82]

Expected legislative developments

FATF

To comprehend well other activities in the area of the AML process, it is necessary to briefly remember the significance of the FATF. The Financial Action Task Force on Money Laundering currently comprises 36 countries, two organizations (European Commission and the Council for the Arab States of the Gulf), and 8 affiliated member groups (so-called FATF-Style Regional Body (FSRB)). Furthermore, the FATF cooperates with many international institutions and organizations, thus achieving the commitment to the compliance with the standards in over 180 jurisdictions. The Czech Republic is not a member, although it applied for membership in 1998 already; however, it is bound by these standards, as a member of the Council of Europe Moneyval[83], i.e. one of the FSRB. In order to determine whether individual jurisdictions sufficiently apply all the recommendations, the FATF carries out peer review, i.e. every country is subject to assessment by a team of selected experts from other member States every 4 to 5 years. The given team then prepares an evaluation report, specifying the extent to which the country in question fulfilled individual recommendations and publishes it on its website. In case serious defects are identified, the economically powerful G8 puts pressure on the government of the given state to take the necessary corrective actions; alternatively, it may include the country in question in the group of high-risk countries, whereas other member states are automatically required to adopt such measures that would ensure effective and proportional countermeasures. Consequently, the failure to comply with these standards may cause significant economic impairment for the problematic state.

Since 1997, the Czech Republic has been subject to four evaluations of the Council of Europe Moneyval, with the last one coming in spring of 2010. It should thus undergo another periodical review in 2015.

The FATF Recommendations were last revised in February 2012; there are now 40 recommendations. In addition to the area of money laundering and terrorism financing, they also target weapons of mass destruction, corruption, and tax offenses. The revision also includes several policy changes that each jurisdiction must implement in their national legislation. Member States of the European Union, thus also the Czech Republic, always implement these recommendations through European legislation.

---

81 Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime of 1990, which – among others – required adoption of anti-money laundering legislation.

82 As of 1 January 2014.

83 Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism – formed by the Committee of Ministers of the Council of Europe in September 1997, with a view to ensure that its member states have in place effective mechanisms against money laundering and terrorism financing and comply with the relevant international standards in these areas.

Fourth European Union AML Directive

It took the European Union a relatively long time to react to the FATF Recommendations revision; after all, it is not surprising at all in this area. Almost two years after their effective date, corresponding European legislation is still to be accepted and Member States have no choice but to wait for the outcome of negotiations under way, which is very problematic for the Czech Republic, for example, which is to be evaluated in 2015 in terms of the application of the new recommendations.

In February 2013, the European Commission presented for discussion a draft of the new "Fourth AML Directive", as a reaction to continuous developments in the area of combating money laundering and terrorism financing and to the need for harmonization of the European legal framework with international standards adopted by the FATF. The Directive should supersede the existing Directive 2005/60/EC of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (so-called Third AML Directive), as well as Commission Directive 2006/70/EC, laying down implementing measures for Directive 2005/60/EC. Moreover, it also supplements Council Decision 2000/642/JHA, concerning arrangements for cooperation between financial intelligence units in respect of exchanging information.

The draft contains several policy changes, which extend the Directive scope of application, introduction of a new risk assessment system, both at national and at domestic level, addition of new measures in relation to information about beneficial owners, introduction of measures in respect of domestic politically exposed persons, abolition of equivalence of third country regimes or harmonization of administrative sanctions. Other changes are rather formal, without much impact on existing legal regulation.

Extension of the scope of application

Compared to the original Directive, the draft is more ambitious, particularly as regards the Directive scope of application. The draft applies not only to casinos, but newly to all providers of gambling services in order to cover this risky industry as a whole. This change is a logical response to the detected criminal activity abusing another area of gambling, outside casinos.

The second major change in this area is the reduction of the threshold for dealers in goods of high value, provided they carry out cash payments, from EUR 15,000 to EUR 10,000. Cash transactions have always been and always will be a major problem in terms of combating money laundering, especially due to the fact that such funds cannot be monitored in any way and it is impossible to trace their origin. Therefore, the draft requires stricter regulation by imposing an obligation on the said dealers to carry out identification and inspection of clients, who execute occasional business in case in the amount of at least EUR 10,000. The reduction of the limit, AML measures will apply to a much larger circle of dealers. However, this change is sensitive, considering the fact that cash payments still represent a relatively common form of payments between businesses in the Czech Republic and since cash payments are only subject to national regulation from CZK 350,000 (under the terms and conditions set down in Act no. 254/2004 Coll., on Restriction of cash payments). This type of restriction leads to a question whether supervisory authorities will in fact be able to monitor the compliance with this obligation in practice. It seems that even the European Commission is aware of this problem, as it withdrew the originally proposed limit of EUR 7,500 and increased it to more reasonable EUR 10,000 in the course of discussing the present version of the draft.

Risk assessment system

Perhaps the biggest change compared to the original Directive is the so-called risk based approach – both at the supranational and national levels. Member states and obliged entities are required to identify the risks of money laundering and financing of terrorism that affect them, and to take appropriate measures to mitigate them. In practice, this means that the competent national authorities (i.e. the Financial Analytical Unit of the Ministry of Finance together with the Czech National Bank in the Czech Republic) have to develop so-called national risk assessment, which would be of a general nature and will include both financial and nonfinancial sector. Based on this assessment, stricter legislative measures should be subsequently adopted for those areas that have been identified as high risk areas, whereas corresponding simplified measures may be adopted in lower-risk areas. Following the national risk assessment, even the obliged entities (as defined in the national AML Act) are required to identify their own risks, document and regularly update them.

Although the specification of relevant measures based on the level of real risk seems logical, it also has its latent weaknesses. In case each EU member state defines different measures in the area of combating money laundering based on its own national risk assessment, there is a risk that 27 inconsistent legal solutions might come into existence, which could be particularly problematic for financial services that can be provided on a cross-border basis within the EU, without any establishment of local branches. States that would identify some of those services as risky and apply more stringent measures would be at a disadvantage against those who would not. Moreover, this situation could obviously be beneficial for potential perpetrators. Therefore, the presented draft lacks EU-wide consistence from this perspective.

Beneficial owner information

According to the draft, efforts aimed at ensuring greater clarity and accessibility of information about beneficial ownership should be implemented by making information available about beneficial ownership to the competent authorities and obliged entities based on a requirement imposed on legal entities for the provision of adequate, accurate, and current information about their beneficial owners. It is also contemplated to impose an obligation on member states to establish registers that would explicitly state this information. Similarly, an obligation to establish registers of trust funds containing information about founders, custodians, and beneficiaries is considered. However, it is not clear so far whether these registers would be public on a mandatory basis or only accessible by a limited range of entities. In any case, the introduction of these types of registers would significantly facilitate the performance of AML obligations on the part of obliged entities that presently often have big problems in finding beneficial owners within the meaning of Section 4(4) of Act no. 253/2008 Coll., i.e. specific individuals, who hold more than 25% of voting rights in given legal entities.

Politically exposed persons

The draft newly introduces the term "domestic politically exposed person" (hereinafter the "PEP"); it shall mean an individual, who is or has been assigned a prominent office/function/role by a member state. On the other hand, a "foreign politically exposed person" is an individual, who performs such office/function/role outside the EU. With regard to both types of PEPs, more prudential rules are set down due to clear existence of high risk of money laundering.

According to Act no. 253/2008 Coll., "PEP" shall currently mean an individual, who holds a prominent public office/function/role with a nationwide scope and who has his/her place of residence outside the Czech Republic or carries out such prominent office/function/role outside the Czech Republic. Domestic PEP is currently not defined. In terms of domestic legislation, the main change would be the fact that PEPs would also include Czech citizens holding such office/function/role, which is definitely welcome.

The differentiation between domestic and foreign PEPs, with "domestic" meaning an EU citizen, seems to be an unnecessary administrative burden for obliged entities that does not bring too much added value. PEPs represent risk – irrespective of whether they are from the EU or from other countries; moreover, in case an EU citizen performs this office/function/role outside the EU, he/she would be considered a foreign PEP. Therefore, there is no reason to adopt different measures for individual types of PEPs.

Equivalence of third country regimes

In connection with the introduction of the risk based approach, it is proposed to abolish the requirement for adopting decisions on whether third countries feature systems for combating money laundering/financing of terrorism equivalent to those set in the EU. In practice, this means that the "white list" would no longer be prepared. Geographical factors should be an integral part of the risk assessment process. However, the European Commission is considering an opposite approach, the so-called "black list", i.e. identification of high-risk countries that pose a significant risk to the financial systems of the EU. Nevertheless, it is very difficult to predict the final form of the text relating to this issue, since it is a politically sensitive topic. Although the white list indirectly specified high-risk states, this specification was only general, indirect; explicit identification of specific high-risk countries from the perspective of the EU may undoubtedly have far-reaching political consequences.

Administrative sanctions

Due to the aforementioned objective to harmonize administrative sanctions, the draft includes explicit specification of many sanctions that should be ensured by member states in case of systematic breach of the Directive's key requirements, particularly client identification and due diligence, record keeping and reporting of suspicious transaction. Namely the proposed level of sanctions is problematic. The draft envisages administrative financial sanctions for individuals amounting up to EUR 5,000,000 or about CZK 125,000,000. In case of legal entities, administrative financial sanctions may be imposed in the amount of up to 10% of their total annual turnover in the preceding business year; in case of a subsidiary of a parent undertaking, the relevant total annual turnover shall mean the total annual turnover specified in the consolidated financial statements of the ultimate parent undertaking in the preceding business year.

These sanction amounts represent a significant disproportion to the usual sanctions imposed in the Czech Republic, given that the current wording of Act no. 253/2008 Coll. includes sanctions for the breach of certain measures against money laundering and terrorism financing of up to CZK 10 mil. The sanctions are also clearly disproportional to the penalties that may be imposed during criminal proceeding under applicable laws of the Czech Republic. Moreover, calculation of sanctions based on the turnover of the entire group could even lead to bankruptcies of relatively strong entities.

The transposition deadline for adoption of the relevant implementation regulation is proposed to be up to two years from the Directive adoption. Originally, the Directive should have been adopted by the end of 2013, but this deadline was not met. According to the 2014 legislative plan, the Directive should undergo the first reading in the European Parliament in April 2014; however, the European Parliament elections take place in May 2014, so further developments can hardly be estimated.

In any case, this delayed adoption of the European anti-money laundering regulation is very problematic for the Czech Republic, since it is already certain that the implementation process of the future Directive into national legislation cannot be completed by the end of 2015, when the Czech Republic is to undergo the aforementioned peer review of the implementation of the FATF Recommendations.

Conclusion

The main novelty in the fight against money laundering should be the signaled risk based approach, which will be discussed in more detail below. On the one hand, it may be beneficial in the sense that individual measures would correspond to the real risks involved, on the other hand, it can cause some legal uncertainty, especially for obliged entities, unless legislators define clear boundaries by means of specific measures. Moreover, considering the pace of the legislative process in the Czech Republic, there are reasonable concerns, whether such measures would actually correspond to the current risks involved.

The legislators will also have to deal with the set disproportionate amount of administrative sanctions, requirements for registers containing information about beneficial owners of legal entities, and most likely also registers containing information about trust funds that are emerging in the Czech Republic.

The upcoming changes that are being prepared in the EU should most likely be reflected in the national legal system by the end of 2016 or as of 1 January 2017, as appropriate. However, a question remains whether international anti-money laundering standards are not revised again by then.

4.3 Assessing client's risk

As already mentioned above, February 2014 marked a 2-year anniversary from the fundamental revision of the so-called Recommendations of the Financial Action Task Force on Money Laundering (hereinafter the "FATF Recommendations"). In its Recommendation no. 1, the FATF explicitly stated that it is necessary to apply the so-called risk based approach to clients of financial and non-financial professions. The given recommendations should be incorporated in the new (i.e. Fourth) European Directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, which was already specified in a report of the European Commission of April 2012. However, a final draft of the new European Directive has not been completed on a European level by the end of 2013 and, due to commenced negotiations and the 2014 European Parliament elections, we cannot assume its quick adoption.

It is therefore necessary that the Czech Republic reflects the FATF Recommendations independently for the time being, as the Recommendations represent the most important internationally recognized standards in the area of combating money laundering, terrorism financing, and newly also in the area of prevention of proliferation of weapons of mass destruction.

This part of the chapter is divided into three subsections; the first one presents the current risk assessment legislation in the area of combating money laundering and terrorism financing and it will also explain the risk based approach. The next subsection is devoted to practical implications relating to the application of the given approach, while the final subsection outlines possible future steps, the adoption of which would be appropriate in this area.

Risk assessment – existing legal regulation

RBA

Certain activities of credit and financial institutions involve client risk assessments in some cases. In many cases, the said institutions had established their own categorization of clients, for example, to reduce the risk of fraud, attacks on themselves, and commission of property crimes. It is also necessary to categorize clients from the perspective of the fight against money laundering and terrorism financing.

However, who is a client of credit or financial institutions? In case we operate solely in the area of combating money laundering and terrorism financing (hereinafter the "AML/CFT"), then the AML Act[84] talks about the terms "transaction", "business relation", and "client's order"[85], although it does not include a specific definition. It is apparent from the above definitions that it is generally a person, who uses the services of credit or financial institutions or whose assets are disposed of by credit or financial institutions, as appropriate.

In case we go back to the RBA, then it by definition implies that obliged entities[86] (i.e. credit and financial institutions, among others) categorize their clients in terms of the risk of money laundering or terrorism financing, as appropriate. The AML Act namely addresses the issue of client's risks in the provisions on the identification and due diligence of clients or on exceptions to those obligations, as appropriate. For example, Section 9(2)(c) specifies that *"customer due diligence process entails the collection of information necessary for on-going monitoring of the business relationship, including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions are consistent with the institution's knowledge of the customer, its business and risk profile". Section 9(3) states that "the obliged entity shall perform customer due diligence to the extent necessary to determine the potential risk of legalization of the proceeds from crime and financing of terrorism depending on the type of customer, business relationship, product, or transaction"*. In the context of application of legal exceptions,[87] the AML Act states that the obliged entity is required to verify whether the conditions for applying such exception are met and whether some of the customers, products, or transactions represent increased risk of abuse in terms of money laundering or terrorism financing based on the information available to such obliged entity. In case of any doubt, such exceptions shall not be applied.

The area of risk assessment is also addressed in the section of the AML Act relating to the system of internal rules[88]. Credit and financial institutions are required to introduce and implement adequate procedures of internal control and communication in order to fulfill the obligations set down by the AML Act. It is clear that these obligations will vary for individual institutions, given the extent to which such institutions carry out activities that are subject to the AML Act, given their size, number of clients, portfolio of products and services, etc.[89] Each system of internal rules, i.e. a written document, which is generally followed by any employee of the institution, who may come across suspicious transactions, must include, among others:

- Procedures for performing the customer due diligence and determining the extent of such due diligence corresponding to ML/TF[90] risk depending on the customer type, business relationship, product, or transaction;

- Adequate and appropriate policies and procedures for risk assessment, risk management, internal control and ensuring control over compliance with obligations set down by the AML Act;

- In some cases (e.g.at subsidiaries of credit or financial institutions, which are located in countries that are not member states of the EU or the EEC), description of additional measures for effective ML/TF risk management.

---

84 Act no. 253/2008 Coll., on Selected measures against legalization of proceeds from crime and financing of terrorism.

85 Sections 4(1) through (3) of Act no. 253/2008 Coll.

86 Section 2 of Act no. 253/2008 Coll.

87 Section 13 of Act no. 253/2008 Coll.

88 Section 21 of Act no. 253/2008 Coll.

89 For example, also based on the method a customer is contacted. Some banks currently prefer remote business relations, i.e. not "face to face".

90 ML/TF = money laundering and terrorism financing

The risk assessment is also addressed in CNB Decree no. 281/2008 Coll., on certain requirements for the system of internal rules, procedures and control measures against the legitimization of the proceeds of crime and financing of terrorism (hereinafter the "CNB Decree")[91]. It is apparent from the very subject matter of the regulation that this topic is crucial within the Decree, as it states that it *regulates the requirements for introducing and applying procedures for performing the customer due diligence process and determining the scope of the customer due diligence corresponding to the risk of legalization of the proceeds from crime and terrorism financing depending on the type of customer, business relationship, product, or transaction; and methods of procedures for risk assessment, risk management, internal control and ensuring control over compliance with obligations set down by the AML Act, applied within the system of internal rules, procedures, and control measures by obliged entities, which are supervised by the Czech National Bank*. In its Section 4, the CNB Decree directly states that "*in the course of the risk management, institutions apply approach based on the assessment of risk of legalization of the proceeds from crime and terrorism financing"*. Other provisions of the Decree state that credit and financial institutions should consider recognized and proven principles and procedures in the area of AML/CFT. These standards are published by the CNB, specifically by means of Official Communication of the CNB of 26 May 2009 on certain requirements for the system of internal rules, procedures and control measures against the legitimization of the proceeds of crime and financing of terrorism. It comprises proven principles and practices, standards, recommendations, analyses of methods and trends reflecting developments in the area of /CFT, and similar documents (e.g. guidance documents) intended to prevent ML/TF and prepared by the intergovernmental organization FATF[92], as well as documents published for the purpose of directing best practice in the area of AML/CFT in specific financial sectors by internationally recognized authors of standards, such as the Joint Forum, Basel Committee on Banking Supervision, International Organization of Securities Commissions[93] or the International Association of Insurance Supervisors[94].

Implementing CNB Decree to the AML Act regulates the client acceptability rules in its Section 5. Institutions shall *"introduce and apply client acceptability rules, according to which and with regard to the client's risk profile: they shall categorize clients; define conditions, upon fulfilment of which they shall not enter into a business relation with a client or shall terminate an existing business relation with a client; define procedures to identify the risk factors in the case of new clients and to identify risk factors during a business relation with a client; and define procedures to be applied in respect of clients in whose case a risk factor was identified".*

Today, it is necessary to categorize not only clients, but namely clients in relation to the products or services they use, transactions they carry out, while monitoring their business relationship to the institution whose products or services they use.

International recommendations – FATF

Although the risk based approach (RBA) has been used in practice for many years, particularly in activities of credit and financial institutions, it was not officially included in the so-called FATF Recommendations until February 2012.

---

91 An amendment to CNB Decree no. 281/2008 Coll. is currently prepared (January 2014), based on the recommendations arising from the evaluation reports of the MONEYVAL Committee; furthermore, it should amend, supplement or specify some problematic formulations and coverage of certain ML/TF risks that have not been addressed by the Decree so far (e.g. amendment to the specification of risk factors, client's risky line of business, expansion of the list of situations, which must be given more attention by an institution, specification of the term nontransparent ownership structure, etc.). Current information is available at: http://www.cnb.cz/cs/dohled_financni_trh/legislativni_zakladna/legalizace_vynosu/konzultacni_materialy.html

92 www.fatf-gafi.org

93 www.iosco.org

94 www.iais.org

In February 2012, the FATF revised its recommendations, which were drawn up in 1990 (as an initiative to combat the misuse of the financial system for laundering money from drug trafficking). According to their Introduction, the FATF Recommendations were also revised to *"strengthen the requirements for higher risk situations, and to allow countries to take a more focused approach in areas where high risks remain or implementation could be enhanced. Countries should first identify, assess and understand the risks of money laundering and terrorist finance that they face, and then adopt appropriate measures to mitigate the risk. The risk-based approach allows countries, within the framework of the FATF requirements, to adopt a more flexible set of measures, in order to target their resources more effectively and apply preventive measures that are commensurate to the nature of risks, in order to focus their efforts in the most effective way."*

The FATF thus targets focused utilization of resources (personal and financial) by states and financial institutions, while also providing some freedom of decision-making to such entities as to the method of addressing the ML/TF threats and risks.

The general principle of the RBA is as follows: where higher risks exist, the state should require credit and financial institutions to use enhanced measures for managing and mitigating such risks (e.g. requirement for increased client monitoring, ban on exceptions for certain products or obliged entities); however, in case of lower risks, it may be possible to use simplified measures (such as the application of statutory exceptions). The Recommendation relating to the RBA is now the FATF Recommendation no. 1. It is clear from the interpretive note[95] to the Recommendation that I tis a general principle that applies to other individual FATF requirements and recommendations. Therefore, other recommendations must also be interpreted in the light of the RBA.

In its interpretive note to the RBA, the FATF divides tasks that must be fulfilled: obligations of countries and obligations of financial institutions. Financial institutions should adopt suitable measures for identification and assessment of ML/FT risks – for clients, countries, or geographic areas, products, services, transactions, or delivery/distribution channels. The FATF also accentuates possible reconstruction of assessments, as the given institutions are required to maintain documentation in order to demonstrate their basis and serve for the provision of information about the risk assessment to competent authorities. Furthermore, financial and credit institutions should implement strategies, control mechanisms, and procedures that would allow them to efficiently manage and mitigate identified risks; these measures should comply not only with national requirements, but also with instructions of competent authorities (in the context of the Czech Republic, we can assume instructions of the Ministry of Finance or Czech National Bank).

Due to obligations arising for the Czech Republic from the membership in the European Union, the rules adopted at the European level will be binding on the Czech Republic. The FATF states that, in determining the risks, it is necessary to take into account assessment of ML/FT risk performed at the supranational level.

European Union

According to the draft of the new European AML Directive, the competent authorities should be required to concentrate on the way of identifying and particularly mitigating AML/CFT risks. Europe thus targets savings of financial resources. Based on the regulation draft, one can assume that financial institutions can generate savings as a result of the new regulation, also by applying less stringent measures for low-risk customers, products and services. But will this really be the case?

95 So-called Interpretative Notes.

According to the explanatory memorandum to the draft of the new EU Directive, new rules are largely based on international standards adopted by the FATF. Given the fact that the Directive is based on the concept of minimum harmonization, the framework should be supplemented by rules adopted at national level. The memorandum further states that the Directive takes into account the need to increase the effectiveness of measures against money laundering activities by adapting the legal framework to ensure that the risk assessment is carried out at the appropriate level and with the necessary degree of flexibility to allow adaptation to different situations and actors. Consequently, the Directive requires Member States, supervisory authorities, and obliged entities to assess risks and take adequate mitigation measures adequate to those risks, while setting down high level of common standards. This results in a Directive that less specifies individual measures to be adopted.

It is apparent from the aforementioned that the final requirements of the Directive for EU Member States and obliged entities operating here will only be of general nature, whereas the mechanisms that will have to be adopted and applied in practice will have to be set down by competent Czech authorities, at least to a minimum extent.[96]

Practical impact of the RBA

Competent authorities

The competent authorities in the Czech Republic are: the FAU and ČNB, Supervision and Regulation sections. In compliance with the AML Act, which is sponsored by the FAU, they investigate suspicious transactions notified by obliged entities and other submissions, carry out control activities and legal agenda associated with the preparation of regulations in the area of AML/CFT and area of coordination of the application of international sanctions, and with conducting proceedings on offences and administrative torts, and cooperates with foreign authorities with the same scope of powers.

We can thus assume that the FAU will be responsible for preparing an amendment to the AML Act, which should follow the adoption of the new European Directive. It is currently very difficult to predict what the final draft of the Directive would look like; consequently, we cannot anticipate the scope of necessary changes to the AML Act. However, one thing is more than obvious: given the need to update the strategies and national risk assessment, it will also be necessary to prepare regulations with lower legal force or methodologies relating to the RBA, which will be intended for credit and financial institutions.

Risk settings

Client's risk profile plays an important role in the area of AML/CFT. According to the CNB Decree, credit or financial institutions shall compile a client's risk profile[97], always assessing it with regard to the following risk factors:

- the fact that one or more of the client's countries of origin or countries of origin of the client's beneficial owner are states that apply insufficiently or not at all AML/CFT measures or states that the institution, by its own assessment, regards as risk states;

- the fact that one or more of the countries of origin of a person with which the client executes a transaction are states that apply insufficiently or not at all AML/CFT measures or states that the institution, by its own assessment, regards as risk states;

96 The draft of the new AML Regulation is still being discussed. Considering the European Parliament elections, scheduled for May 2014, we cannot assume that the draft would be approved by the existing membership. Therefore, the author estimates that the given European legislation will be adopted in early 2015.

97 Section 5(2) of CNB Decree no. 281/2008 Coll.

- Client, client's beneficial owner or a person with which the client executes a transaction is entered on a list of persons and movements against which sanction measures are applied in accordance with legal regulations on the implementation of international sanctions[98];

- Client's nontransparent ownership structure[99];

- Unclear origin of the client's finances;

- Circumstances leading to suspicion that the client does not act on its own behalf or seeks to conceal the fact that it acts under the instructions of a third party;

- Unusual manner of execution of a transaction, with particular regard to the type of client, subject, size and manner of settlement of the transaction, the purpose of opening an account and the subject of the client's business; and

- Circumstances suggesting that the client is executing a suspicious transaction[100].

When determining the given risks, the country of origin[101] of a client or beneficial owner (in case of legal entities) plays an important role. The FATF issues public statements in respect of the so-called high--risk countries. In October 2013, the FATF issued a new public statement ("Public Statement"), in which it again urges its members and other jurisdictions to adopt countermeasures against Iran and North Korea[102], with a view to protect financial systems against the risks of money laundering and terrorist financing, which the two countries pose for the global financial system. In the said public statement, the FATF lists countries, whose AML/CFT system has strategic deficiencies and which have not made sufficient progress in eliminating these deficiencies or have failed to comply with action plans drawn up in cooperation with the FATF to remedy these deficiencies. It concerns the following countries: Burma / Myanmar, Ecuador, Ethiopia, Indonesia, Yemen, Kenya, Nigeria, Pakistan, Syria, Tanzania, and Turkey. This information is always published by the FAU, among others, on its website, together with recommendations for all obliged entities within the meaning of the AML Act to pay *"maximum attention when entering into business relations and executing payments with entities and financial institutions in these jurisdictions; as a minimum, it is necessary to require sufficient information about the client, source of their funds, and the nature and purpose of the transaction"*.[103]

---

98 For example, Act no. 69/2006 Coll., on Implementation of international sanctions

99 Section 3(a) of CNB Decree no. 281/2008 Coll. defines non-transparent ownership structure as: "a state whereby it cannot be ascertained who a client's actual owner is:

1. from an extract of the Commercial Register, other equivalent record of the country of registered address of a person who is not entered in the commercial register in the Czech Republic and, if such record does not exist in the country of such foreign person's registered address, from legalized articles of association; or
2. from another document by which the foreign person was established and which contains all changes thereto; or
3. from a credible source on which an institution relies for good reason;"

100 Section 6 of Act no. 253/2008 Coll.

101 According to Section 3(b) of CNB Decree no. 281/2008 Coll., a country of origin shall mean "a state of which an individual is a national; in which an individual is registered for long-term or permanent residence; or in which a legal entity has its registered address, branch, organizational unit or place of business."

102 Iran mainly represents risk in terms of terrorism financing; North Korea shows permanent defects within the entire system of combating money laundering and terrorism financing.

103 Source: http://www.mfcr.cz/cs/verejny-sektor/regulace/boj-proti-prani-penez-a-financovani-tero/novinky-fau/2013/rizikove-jurisdikce--aktualni-prohlaseni-15071

Another document published by the FATF is the "Improving Global AML / CFT Compliance: On-going Process". It specifies jurisdictions, whose AML / CFT systems show strategic deficiencies; however, these countries have committed to an action plan that has been developed with the FATF to address shortcomings and this plan is followed, at least to a satisfactory extent. It concerns the following countries: Afghanistan, Albania, Angola, Antigua and Barbuda, Argentina, Bangladesh, Iraq, Cambodia, Cuba, Kuwait, Kyrgyzstan, Laos, Namibia, Nepal, Nicaragua, Sudan, Tajikistan, Vietnam, and Zimbabwe. Once again, the FAU publishes recommendations for obliged entities in the meaning of the AML Act on its website, specifically to *"take into account higher risks associated with identified deficiencies when entering into business relations and executing payments with entities and financial institutions in these jurisdictions".*[104]

The country of origin plays a really important role; on the other hand, it is quite simple to include such risk factor in the monitoring systems of credit or financial institutions. It will be important to focus on specific procedures within the identification and due diligence of clients[105]. Interpretive note to FATF Recommendation no. 10 (Customer due diligence) states, among others, the procedure for applying the risk based approach. It lists the following risk parameters: account/business relationship purpose, volume of funds the customer intends to deposit to an account or volume of executed transactions, regularity or duration of the business relationship; it states that these parameters can - either alone or in combination - increase or decrease the potential ML/TF risk and thus also affect the appropriate degree of customer's due diligence. In general, it lists the following situations as potential high-risk situation:

a) Customer risk factors

- The business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the financial institution and the customer);
- Non-resident customers;
- Companies that have nominee shareholders or shares in bearer form;
- Business that are cash-intensive;
- The ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

b) Country or geographic risk factors

- Countries identified by credible sources as not having adequate AML/CFT systems;
- Countries subject to international sanctions;
- Countries identified by credible sources as having significant levels of corruption or other criminal activity;
- Countries identified by credible sources as providing funding or support for terrorist activities.

104 Source: http://www.mfcr.cz/cs/verejny-sektor/regulace/boj-proti-prani-penez-a-financovani-tero/novinky-fau/2013/rizikove-jurisdikce--aktualni-prohlaseni-15071

105 Sections 7 – 13 of Act no. 253/2008 Coll.

c) Product, service, transaction or delivery channel risk factors:

- Private banking;
- Anonymous transactions;
- Non-face-to-face business relationships or transactions;
- Payment received from unknown or unassociated third parties.

On the other hand, it is possible to draw up a list of situations with potentially low ML/TF risk (and the FATF also provides it). However, the FATF further states in this given interpretative note that *"Having a lower money laundering and terrorist financing risk for identification and verification purposes does not automatically mean that the same customer is lower risk for all types of CDD measures, in particular for ongoing monitoring of transactions."*

It is clear from the above mentioned that that credit and financial institutions are required to draw up appropriate risk assessment scenarios and update them based on available information. Each institution determines the risk profile individually - especially by their client portfolio and offered products and services. It is also important to note that the legal requirements form a generally recognized standard enforceable by the state; however, it is possible to deviate from it and impose stricter criteria. This is particularly important in terms of institution's reputation, advertising, and "goodwill".

Steps to be taken…

The primary solution for determining risks in terms of the RBA in the area of AML/CFT is to start with the evaluation of country risks (i.e. of the Czech Republic or its position in the region of Central Europe region) – i.e. to focus on the threat of criminal activities that are present and characteristic for the given region, further concentrating on current information (statistics, national strategies, annual reports, et..) on crimes in the region (i.e. information on predicative crimes).

The above mentioned factors should be assessed by a competent authority (such as the FAU in the author's view), which has access to this information or may request them from concerned authorities, as appropriate. As part of this assessment, it seems beneficial to use information specified in the document FATF Guidance: National Money Laundering and Terrorist Financing Risk Assessment of February 2013. Annexes to the aforementioned documents provide lists of categories of crimes that pose ML/TF risks for individual countries, as well as examples of factors leading to the assessment of ML / TF risks[106].

There are many international documents that can help you create a risk assessment strategy. Such sources are listed in, for example, annexes to Guidance on the Risk Based Approach to Combating Money Laundering and Terrorist Financing (High Level Principles and Procedures) of June 2007. Although it is not the most current document, it contains a lot of information for determining a risk rate.

In terms of other activities and tasks – in case we refrain from new statutory requirements that will have to be implemented after the implementation of the Fourth European AML Directive in the Czech laws

106 Annex II to the FATF Guidance: National Money Laundering and Terrorist Financing Risk Assessment refers to the risk factors using the term "PESTEL" based on the first letters of the key assessment categories: political, economic, social, technological, environmental, and legislative.

- it will be necessary to develop a methodology intended for the private sector. The preparation of methodologies appears to be practical as well as welcome and practicable for the private sector. To do this; however, it is necessary to ensure intensive dialogue with the private sector and other stakeholders - such as the Czech Banking Association[107]. The methodology[108] should set up some fixed processes and also provide specific examples for the ML/TF risk assessment. The scope of the methodology may seem problematic, due to the number and diversity of entities engaged in activities regulated by the AML Act. Therefore, it will first be necessary to properly think through the scope and content requirements of the methodologies or modify the number thereof (division by sector based on their activity, based on the entity type, individual AML/CFT obligations, etc.).

Conclusion

The given excursion into the area of the RBA tried to outline the main aspects of the risk based approach. It could not; however, cover all of its aspects. To identify and, in particular, to mitigate the ML/TF risks well, it is also necessary to ensure personal (staff-related) prerequisites. It is thus important to ensure awareness activities, staff trainings (irrespective of whether within obliged entities or competent authorities of the Czech Republic), or sufficient staffing.

It is safe to say that the RBA brings a slightly reverse view of the anti-money laundering activities, as the objective of the RBA is to individualize and structure the approach of credit and financial institutions to their clients and to provided products and services, and not only to impose fixed statutory requirements that would generally apply to all situations, to all types of clients, and to all activities of these institutions that are subject to regulation under the AML Act. It concerns a really effective targeting of high-risk entities. However, it is important to note that the initial transition to this approach is not cheap and can be quite challenging. From this perspective, it is good to start preparations for this "transition" in advance and also remember it when preparing budgets of the concerned institutions.

It will be necessary to ensure information exchange between the private and the public sectors. The state will need information from the market - i.e. from credit and financial institutions, whereas these institutions will require clearly defined "rules" by the state, as they are constantly at risk of sanctions from the state. Consequently, it will be necessary to balance this relationship correctly. It is beneficial to commit the relevant private entities in relation to the RBA to regular reporting obligations, under which they would be evaluated (rating system), providing the state with valuable information from the market.

Finally, we must note that it is important to ensure that the new statutory requirements for credit and financial institutions actually correspond to the minimum European standard, thereby not excluding businesses operating in the Czech market from the provision of services as competitive entities at the European and global level, as appropriate.

---

107 BEEKARY, N. Combating Money Laundering and terrorism finance: Past and Current Challenges, Edward Elgar Publishing Limited, 2013, p. 5: Authors Lucia Dalla Pellegrina and Donato Masciandaro state that the interrelation of supervisory authorities and financial institutions in establishing the RBA is even more important for achieving effectiveness and efficiency in regulation. On the other hand, the RBA increases flexibility of regulation, which in turn imposes requirements on the responsibility of financial institutions.

108 FAU also publishes "methodological instructions".

5. Do you know your customer?

The area of anti-money laundering and financing of terrorism affects all areas of life of an economically active society. The financial sector is particularly sensitive in this regard. Therefore, the aim of all democratic nations of the world is to "fight", through available means and particularly through legal means, against efforts aimed at legalizing the proceeds from crime.

The authors of this publication focused on the analysis of the entire AML area from different perspectives, looking for ways and opportunities to increase the efficiency of processes and tools in detecting criminal activities consisting in the legalization of funds (in particular) that "flow" through financial institutions. The authors believe that the "know your customer" principle is the key to timely identification of suspicious transactions of financial institutions' clients. This process is very complex and it is certainly not possible to set down uniform procedures for each type of financial institutions, given their diverse operations. Banks, insurance companies, or securities dealers all offer different products. However, all financial institutions are obliged entities within the meaning of the AML Act and, consequently, they must apply procedures aimed at disclosing such activities.

In order to facilitate the entire process of detecting efforts aimed at legalizing the proceeds from crime, we can inevitably apply the "Know your customer" principle. And this leads to a question: Do we really know our clients? Do we know what they do, what products and services they use? Are we able to monitor their activities and register potential risky transactions? We should be able to answer all of these and other questions. Therefore, it is necessary to apply the obligations imposed on financial institutions in Decree no. 281/2008 Coll., on certain requirements for the system of internal rules, procedures and control measures against the legitimization of the proceeds of crime and financing of terrorism.

Risk profile

To get to know clients, financial institutions must determine a risk profile of their clients. As part of composing and assessing the client's risk profile, it is necessary to find out or rule out the existence (as appropriate) of the following facts:[109]

a) Client's country of origin in terms of Section 3(b) of the CNB Decree (with regard to legal entities, a country of origin for the client's beneficial owner in terms of Section 4(4) of the AML Act), country of origin for the person, with which a client carries out the given transaction;

- So-called high-risk jurisdiction are published by the FATF several times ayear in the "Public Statement"[110] and "Improving Global AML/CFT Compliance: On-going Process"[111]

109 See Section 5(2) of Decree no. 281/2008 Coll., on certain requirements for the system of internal rules, procedures and control measures against the legitimization of the proceeds of crime and financing of terrorism.

110 Current information available at: http://www.fatf-gafi.org/documents/documents/fatf-public-statement-oct-2013.html or www.mfcr.cz/cs/verejny-sektor/regulace/boj-proti-prani-penez-a-financovani-tero/novinky-fau/2013/rizikove-jurisdikce--aktualni-prohlaseni-15071

111 www.fatf-gafi.org/documents/documents/fatf-compliance-oct-2013.html or www.mfcr.cz/cs/verejny-sektor/regulace/boj-proti-prani-penez-a-financovani-tero/novinky-fau/2013/rizikove-jurisdikce--aktualni-prohlaseni-15071

b) Client (client's beneficial owner in case of a legal entity) or a person, with which the client executes a transaction is entered on a list of persons and movements against which sanction measures are applied in accordance with Act no. 69/2006 Coll., on the Implementation of international sanctions;[112]

c) In case of legal entities, nontransparent ownership structure of a client[113];

d) Unclear origin of the client's funds;

e) Suspicion that the client does not act on its own behalf or seeks to conceal the fact that it acts under the instructions of a third party;

f) Unusual manner of execution of a transaction, with particular regard to the type of client and client's line of business;

g) Other circumstances suggesting that the client is executing a suspicious transaction.

It is apparent from the provisions of the AML Act on the customer identification and due diligence that the obliged entity must always find out whether or not clients are PEPs. It is possible to differentiate domestic and foreign PEPs[114].

Furthermore, it is suggested to ascertain the following information:

a) Whether a client is included in any of the supporting "sanction" lists, which are not binding on the Czech Republic (e.g. OFAC list, Bank of England list);
b) For legal entities: whether or not the company's registered office is registered in an off-shore center[115];
c) Client's business activities and profession:
   - Higher-risk activities include, for example, exchange offices, betting shops, game room, casinos, alcohol/tobacco wholesale, retail trade in precious stones/metals, pawnshops, night clubs, transactions with strategic raw materials, military materials, etc.
d) Client from a country (registered office in a country) that is characterized by high level of corruption, organized crime (prostitution, manufacture and distribution of drugs, manufacture of arms, including weapons of mass destruction, etc.);
e) Company type (incl. domestic/foreign);
f) Entry of the client in the so-called insolvency register;[116]
g) Method a business relationship is established (identification without the client's physical presence);
h) Type of ID card presented for the purpose of the client's identification, etc.

It is beneficial to register these additional measures in an institution's own system of internal rules; however, the list cannot be exhaustive. For the purpose of these additional factors, it is also possible to use publicly available database of public administration that allow remote access.

112 Overview of applicable sanctions is available at: http://www.mfcr.cz/cs/legislativa/mezinarodni-sankce/prehled-sankci/informace-k-aktualne-ucinnym-predpisum-14100

113 Section 3(a) of the CNB Decree

114 The category of the so-called "domestic" PEPs includes individuals who are or have been assigned a prominent public office/function in the Czech Republic.

115 Use, for example: http://www.taxhavensguide.com/list-of-offshore-financial-centres.php

116 http://www.rejstrik-insolvencni.cz/

Risk levels

To ensure correct setup of the client's risk profile, it is useful to set down different risk levels (risk scale) that would be applied by the specific financial institution. The institution will then use this scale for the purpose of assessing the risk of its clients, with each client being included in one of the predefined categories. The risk level scale should correspond to the institution size, portfolio of its clients, and the nature of involved business relationships. However, it is recommended to introduce at least three levels of risk - low, standard, and high risk.[117] Each institution shall also define the so-called **unacceptable risk**, where no business relationship is established with the client, no transaction is executed or existing business relationship is terminated (e.g. the client is in a sanction list binding on the Czech Republic). At the same time, the system must be configured in a manner that allows quick transfer of clients between groups.

For example, the risk levels may be as follows:

- **Low risk:** central public administration authorities of the Czech Republic, CNB, higher self-governing units, credit or financial institution, companies, the securities of which are admitted for trading on a regulated market and which are subject to disclosure requirements equivalent to the requirements of the EC law, etc.

- **Standard risk:** standard client

- **High risk:** clients that receive customized services (private banking), PEPs, correspondent banks, clients residing in offshore centers, clients from countries with widespread crime, corruption, clients with nontransparent ownership structure, etc.

Handling identified risks

When applying the risk based approach, it is necessary to evaluate each client according to various criteria, analyze it, and – based on the client's risk profile/categorization – implement appropriate mechanisms to carry out client identification and due diligence, apply statutory exceptions, or abolish the transaction, as appropriate (business relationship is not established/is terminated). Each risk level should be linked with the given requirement for the management or mitigation (as appropriate) of such risk.

The following procedures are considered to be effective:

a) Requirement for additional information about the client (including the scope and verification method for information ascertained about or provided by the client) as part of the client's due diligence within the meaning of Section 9 of the AML Act;
b) Continuous client monitoring, its periodicity (including standard/enhanced/simplified client monitoring);
c) Approval powers for approving a new client (i.e. establishment/termination of a business relation, execution of transaction with a client, transaction not executed pursuant to Section 15 of the AML Act),
d) Statutory exceptions pursuant to Section 13 of the AML Act will not be applied; identification will not be accepted pursuant to Section 11 of the AML Act;
e) Assessment of suspicious transaction.

117 Multilevel spectrum is recommended for all credit institutions (5 or more levels).

The above mentioned information may be used to prepare an overview based on the criteria set down, with ties to the risk level:

Table 16

Criterion / Risk level	Low risk	Standard risk	High risk
Client type	Client pursuant to Section 13(1) of the AML Act	Standard client	Private banking, PEPs, correspondent bank, registered office in an offshore center
Business relation establishment method	Acceptable exception to "face to face" identification	"Face to face" identification	Identification without the client's physical presence should not be permitted (accepted identification); if so, additional measures imposed
Client acceptance	Business relation is/will be established	Business relation is/will be established	Business relation is/will – will not be established, or will be terminated, as appropriate*
Client monitoring	Simplified monitoring	Standard monitoring	Enhanced monitoring
Exceptions	Application of statutory exceptions	Application of statutory exceptions based on specific assessment of the institution	Statutory exceptions not applied; additional measures for client identification and due diligence
Client information	Client's declaration, public sources, documents presented for client identification and due diligence	Client's declaration, public sources, documents presented for client identification and due diligence	Client's declaration, public sources, documents presented for client identification and due diligence, additional information, independent verification of documents
Products and services	Products and services pursuant to Section 13(2) of the AML Act	Standard services (current account, savings account)	Investment banking, over limit cash payments, exchange office services, general loans, virtual currency trading, etc.

Source: Authors' own elaboration

** Approval powers settings – e.g. client acceptance subject to approval of a Compliance Department employee, approval by a higher ranking employee, approval by a statutory body, etc.*

Other risk factors

Client's risk profile must be supplemented with other risk factors in specific situations. Other possible risk factors are listed below:

- **Personal risk** – individuals (also as statutory representatives or beneficial owners of legal entities) with criminal or otherwise questionable (unclear) past or associated with such persons, persons with assets of dubious/unknown origin, persons associated with PEPs, "godfathers", lobbyists, people from high-risk territories, persons involved in a large number of business entities, chronic "bankrupt persons", etc.

- **Payment risk** – intensive cash payments, over limit payments in cash, frequent payments that do not match the type of client or client's business activities, transfers to/from high-risk jurisdictions or areas that are subject to international sanctions, etc.

- **Distribution risk** – settlement of foreign checks, application of the so-called new methods of payment (payments via mobile phones, remote payments, digital wallets in excess of the given limits), etc.

- **Commodity risk** – transactions involve weapons or their (potential) carrier, military equipment, dual-use goods or advanced technology, precious metals or stones, strategic raw materials, precursors, etc.

- **Product risk** - investments in mutual funds, flexible investment life insurance with the option of surrender value, virtual or electronic currency (BitCoin, etc.), transactions with strategic commodities or involving territorial, volume or other risks, etc.

The risk may also go up due to subjective evaluation by an organization's employee, who is present upon the establishment of a business relationship or conclusion of the transaction, as appropriate (e.g. local and personal knowledge, lack of confidence in the information provided, doubts about the authenticity of documents submitted for client identification and due diligence).

Possible reconstruction and updates

Institutions maintain documentation for individual assessments so that it is possible to corroborate it and introduce appropriate mechanisms for the provision of information on the risk assessment to competent authorities (FAU of the MoF CR, CNB). The requirement for possible reconstruction is imposed for client due diligence, transaction revisions, correspondence, all processes of an institution in relation to the detection of client's risk profile, and suspicious transaction notifications, as appropriate. The risk based approach must be applied not only prior to the establishment of a business relationship (prior to the conclusion of an individual transaction), but also throughout the existence of such business relationship.

Institutions shall regularly update the given risks, IT tools settings (incl. testing), and inspection of risk assessment and management. However, it shall always perform these processes when the portfolio of products and services changes, in case of amendments to legislation in the area of anti-money laundering or terrorist financing, upon takeover of client portfolio – e.g. during corporate mergers and/or acquisitions.

Institutions must always evaluate all conceivable risks and verify the fulfillment of obligations set down by the AML Act and related regulations - for individual clients, transactions, types of business relationships, and products. Institutions may apply measures to varying extent, depending on the nature and extent of risks for different risk factors. However, if higher risks are identified, financial institutions shall apply enhanced measures for risk management and mitigation.

Conclusion

In case financial institutions consistently apply the principles and recommendations relating to the determination of client's risk factors, thereby getting to know their clients in more detail, it can be said that it is impossible to legalize any proceeds from crime through such financial institutions. Effective, but not excessive and/paralyzing supervision by public administration authorities, which are competent in this area, will further contribute to the application of procedures of each individual financial institution in the area of "anti-money laundering".

Executive Summary

This book has been prepared as part of the scientific research project of the Ministry of the Interior of the Czech Republic implemented by Vysoká škola finanční a správní, o.p.s. (University of Finance and Administration), Department of Finance, entitled "***Increasing the effectiveness of procedures and measures for detecting legalization of the proceeds from crime and preventing the financing of criminal structures within the sector of the financial service providers***" (project identification code VG 20122014087, with total support of CZK 2,238 thousand). The book represents one of the project outputs.

The monograph focuses on increasing the effectiveness of the fight against money laundering, with particular emphasis on the area of financial institutions. The research team mainly targeted the analysis of the actual situation, which relies on the analysis of the legal support for the prevention of money laundering and financing of terrorism.

Following a short introduction to the given issue, the first chapter characterizes the legal bases of the AML process using the descriptive method of the research work. This part also deals with the legal implications of the breach of the AML process rules by financial institution employees, and with the issue of identification. The first two sections of the chapter are devoted to the identification process; they analyze the so-called remote identification process and simplified identification process. As part of the research, recommendations are given that could, on the one hand, significantly improve the AML process and, on the other hand, simplify the identification process in cases that only involve low counterparty risk.

The second part of the monograph analyzes selected areas of prevention and suppression of money laundering. This concerns, for example, the area of reporting and its assistance in the course of the AML process, virtual environment and its effect on potential money laundering, or the analysis of the financial institution identifiers implementation. Another important area also addressed by this section is the role of the so-called politically exposed persons within the AML process and the link of such persons to public administration. Furthermore, the chapter comprises the view of an expert witness of AML.

At the end of the chapter, selected problems associated with the practical detection of money laundering as well as findings made in the course of a survey (questionnaire) with selected financial service providers in the Czech Republic, carried out by the research team, are discussed. Moreover, this section also provides basic statistical data on the number of notifications of suspicious transactions in recent years.

The next chapter addresses new possibilities of the AML process that should rely on the Risk Based Approach – assessing clients by determining their risk factors. This approach relies on the recommendations of the inter-governmental body FATF, as adopted in February 2012. The determination of clients' risk factors represents a very important step in the subjective assessment of the clients' risk and the risk associated with their transactions carried out within specific financial institutions. The chapter comprises some proposals and measures, the practical application of which would be useful.

The fifth and final chapter then analyzes the entire AML process and the measures aimed at increasing its effectiveness, with special emphasis on financial institutions. It mainly accentuates the client identification process and its potential modifications, and underlines the RBA, with selected implementation methods.

References (literature and other sources)

Literature

BALOUN, V. *Finanční kriminalita v České republice.* Praha: 2004. Institut pro kriminogoii a sociální prevenci. Dílčí studie úkolu „Výzkum ekonomické kriminality". (Financial crime in the Czech Republic. Institute of Criminology and Social Prevention, Partial study under the project "Research of economic crime").

BEEKARRY, N. *Combating Money Laundering and terrorism finance: Past and Current Challenges.* Edward Elgar Publishing Limited, 2013. ISBN 978-18-49807-517.

BLAHOVÁ, N. Změny regulačního a dohledového rámce finančních trhů v Evropské unii. *Český finanční a účetní časopis*, 2010, Vol. 5, No. 2, p. 42–51. ISSN 1802-2200. (Changes to the regulatory and supervision framework of financial markets in the European Union).

BOTTEGA, J. POWELL, L. *Creating a Linchpin for Financial Data: The need for a Legal Entity Identifier*, p. 4. SSRN-id1723298.

BRADA, J. Hodnocení úvěrové bonity obchodní společnosti. In: *Zadlužení – fenomén současnosti.* Praha: Soukromá vysoká škola ekonomických studií, s.r.o., 2012. P.108-116, 8 p. ISBN 978-80-86744-92-6. (Assessing creditworthiness of a company).

BUUS, T. a J. BRADA. Economics of Transfer Pricing Reviewed, 2010, (dostupné on-line http://papers.ssrn.com/sol3/papers.cfm?abstract_id=954333)

CEJP, M. *Organizovaný zločin v České republice III*, Institut pro kriminogogii a sociální prevenci, Praha: Institut pro kriminologii a sociální prevenci, 2004. (Organized crime in the Czech Republic III, Institute of Criminology and Social Prevention, 2004, Prague, Institute of Criminology and Social Prevention).

Doporučení FATF: Mezinárodní standardy v boji proti praní peněz, financování terorismu a šíření zbraní hromadného ničení, únor 2012. (Financial criminals).

DVOŘÁK, V., J. ŠUGÁR, P. MÁLEK a P. HORÁČEK. V*ýnosy z trestné činnosti.* Praha: Scientia, spol. r.o., 2010. 236 p. ISBN 978-80-86960-67-8. (Proceeds from crime).

EIGEN, P. et al. *Kniha protikorupčních strategií.* Prague: Transparency International, 2000. 117 pages. p. 99 (Book of anticorruption strategies).

FATF Guidance: National Money Laundering and Terrorist Financing Risk Assessment, February 2013.

FATF Recommendations: International standards on combating money laundering and the financing of terrorism financing, and proliferation of weapons of mass destruction, February 2012.

FRYŠTÁK, M. *Hospodářská kriminalita z pohledu teorie a praxe.* Prague: KEY Publishing, 2007. 208 pages. ISBN 978-80-87071-18-2. p. 10 et seq., 200 et seq. (Economic crime from the perspective of theory and practice).

GILMORE, W. *Dirty Money. The Evolution Of Money-Laundering Counter- Measures.* 2nd ed. Strasbourg: Council of Europe Press, 1999.

HARVEY, J. *Journal of Money Laundering Control:* An Evaluation of Money Laundering Policies. London: Henry Stewart Publications, 2005, Vol. 8, No. 4.

CHMELÍK, J. et al. *Úvod do hospodářské kriminality.* 1st Edition. Prague: Vydavatelství a naklad. Aleš Čeněk, s.r.o., 2005. 167 pages. ISBN 80-86898-13-X (Introduction to economic crime).

JÍROVSKÝ, V. *Kybernetická kriminalita – nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* 1st Edition. Prague 2007. ISBN 978-80-247-1561-2. p. 91 et seq. (Cybercrime – not only about hacking, cracking, viruses, and Trojan horses without any secrets).

KLIMIKOVÁ, M. a kol. *Bankový manažement a marketing I.* Bratislava: IRIS, Vydavateľstvo a tlač, s. r. o., 2012. ISBN 978-80-89238-63-7. (Bank management and marketing).

KYNCL, L. et al. *Poznej svého klienta – základní zásady finančního práva.* 1st Edition, Brno: ACTA UNIVERSITATIS BRUNENSIS, IURIDICA, 2012. No 433. 165 pages. ISBN 978-80-210-6085-2. (Know your customer – basic principles of financial law).

LEVI, M. *Fraud: Organization, Motivation And Control.* Ashgate, 1999. 1036 s. ISBN 978-18-552-1716-4.

MAZÁNEK, J. Specifika dokazování hospodářské trestné činnosti. In: *Trestní právo*, 2008, Vol. 13, No. 2, p. 5 - 13. (Specificities of proving economic crime).

MIKDASHI, Z. *Regulating the Financial Sector in the Era of Globalization. Perspectives from political economy and management.* Palgrave Macmillan, 2003, p. 92. 249 p. ISBN 1-4039-1638-1.

PAVLÁT, V. *Globální finanční trhy.* Praha: VŠFS, 2013. Edice EUPRESS. P. 58-59. ISBN 978-80-7408-076-0. (Global financial markets).

POLOUČEK, S. a kol. *Bankovnictví.* 2st Edition. Praha: C. H. Beck, 2013. ISBN 978-80-7400-491-9. (Banking).

Reports and Publications. [online] Federal Bureau of Investigation. Available from: <http://fbi.gov/stats--service/publications/>.

ROBINSON, J. *Pánové z prádelny špinavých peněz.* 1nd Edition. Praha: Columbus, 1995. ISBN 80-85928-06-X. (Gentlemen from the money launderette).

SCHLOSSBERGER, O. AML procedures in financial institutions - suggestions for changes. In: *Platební služby on-line v EU, praktické aplikační problémy elektronických platebních prostředků.* 2012.

SCHLOSSBERGER, O. *Platební služby.* 1nd Edition. Praha: Management Press, 2012, 325 p. ISBN 978-80-7261-238-3. (Payment services).

SCHNEIDER, F., BUEHN, A. and C. E. MONTENEGRO. *Shadow Economies All over the World. New Estimates for 162 Countries from 1999 to 2007.* [online] The World Bank Development Research Group. July 2010. WPS5356.

Statistical overviews of crime for 2011. [online] Police of the Czech Republic. Updated in 2012 Available from: <http://www.policie.cz/clanek/statisticke-prehledy-kriminality-za-rok-2011.aspx>.

ŠÁMAL, P. et al. *Podnikání a ekonomická kriminalita v České republice*. 1st Edition. Prague: C. H. BECK, 2001. 776 pages. ISBN 80-71794-93-7. pp. 438 – 475. (Business activities and economic crime in the Czech Republic).

ŠUGÁR, J. et al. *Odčerpávání výnosů z trestné činnosti v praxi policejního orgánu, státního zástupce a soudce*. Prague: Police Academy of the Czech Republic in Prague, 2009. (Outflow of the proceeds from crime in the practice of policy authorities, public prosecutors, and judges).

TOMÁŠEK, J. *Úvod do kriminologie*. 1st Edition. Prague: Grada Publishing, a. s., 2010. 214 pages, ISBN 978-80-247-2982-4, p. 68 (Introduction to criminology).

TVRDÝ, J. a A. BÁRTOVÁ. *Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu a předpisy související*. Prague: Nakladatelství C.H. Beck, 2009, 502 pages. ISBN 978-80-7400-099-7 (Act on Selected measures against legalization of proceeds from crime and financing of terrorism and associated regulations).

Legal norms

Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community;

Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006, on information on the payer accompanying transfers of funds.

Commission Directive 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council.

Decision of the Supreme Court of the Czech Republic of 12 April 2001, file no. 21 Cdo 3019/2000.

Decision of the Supreme Court of the Czech Republic of 14 June 2012, file no. 21 Cdo 977/2011.

Decision of the Supreme Court of the Czech Republic of 19 January 2000, file no. 21 Cdo 1228/9.

Decision of the High Court in Prague of 28 June 1995, file no. 6 Cdo 53/94.

Directive 2005/60/EC of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing.

Decree no. 123/2007 Coll., stipulating the prudential rules for banks, credit unions and investment firms.

Decree no. 281/2008 Coll., on certain requirements for the system of internal rules, procedures and control measures against the legitimization of the proceeds of crime and financing of terrorism.

Decree no. 23/2014 Coll., on the performance of the activities of banks, credit unions and investment firms.

Act no. 89/2012/ Coll., Civil Code.

Act no. 284/2009 Coll., on the Payment system.

Act no. 253/2008 Coll. on Selected measures against legalization of proceeds from crime and financing of terrorism.

Act no. 69/2006 Coll., on the Implementation of international sanctions.

Act no. 262/2006 Coll., Labor Code.

Act no. 21/1992 Coll., on Banks.

Act no. 513/1991 Coll., Commercial Code (effective until 31 December 2013).

Act no. 455/1991 Coll., on Licensed trades (Trade Licensing Act).

Final report to the issue of proceeds and money laundering for 2012. Prague: Police of the Czech Republic, Agency for Detecting Corruption and Financial Crime of the Service of Criminal Police and Investigation, 2013.

Internet (online) sources

Anti-Money Laundering. Understanding global KYC differences. London. January 2013. Available from: http://www.pwc.com/gx/en/financial-services/publications/anti-money-laundering-know-your-customer-quick-reference-guide.jhtml.

Barclays Bank told by Treasury to pay £500m avoided tax. [online] BBC News. Available from: <http://www.bbc.co.uk/news/business-17181213>.

Cannes Summit Final Declaration – Building Our Common Future: Renewed Collective Action for the Benefit of All. Draft of November 4. Cannes, November 4, 2011. Available from: http://www.g20.utoronto.ca/summits/2011cannes.html. (Downloaded on 31 March 2013).

FSB. A Global Legal Entity Identifier for Financial Markets. June 2012. Available from: http://www.financialstabilityboard.org/publications/r_120608.pdf.

Hospodářské noviny no. 088, of 4 – 6 June 2012, p. 1. Article Czech Republic affected by identity thefts. Frauds will open an account in your name. [online] MAFRA, a. s. Updated on 4 May 2012. Available from: http://ekonomika.idnes.cz/cesko-zasahly-kradeze-identit-dkl-/ekonomika.aspx?c=A120504_085107_ekonomika-.

HSBC. [online] HSBC Bank [quoted on 28 February 2012]. Available from: http://www.hsbc.com/1/2/about/network>.

http://www.mfcr.cz/cs/verejny-sektor/regulace/boj-proti-prani-penez-a-financovani-tero/zprostredkovana-identifikace.

http://www.mfcr.cz/cs/verejny-sektor/regulace/boj-proti-prani-penez-a-financovani-tero/novinky-fau/2013/rizikove-jurisdikce--aktualni-prohlaseni-15071.

http://www.mfcr.cz/cs/legislativa/mezinarodni-sankce/prehled-sankci/informace-k-aktualne-ucinnym-predpisum-14100.

http://portal.justice.cz/Justice2/Uvod/uvod.aspx, Public Register section.

http://www.rzp.cz/cgi-bin/aps_cacheWEB.sh?VSS_SERV=ZVWSBJFND.

http://www.fatfgafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%20approved%20February%202012%20reprint%20March%202012.pdf.

http://bankovnictvi.ihned.cz/c1-55893980-fatca-v-boji-proti-danovym-unikum.

http://www.epravo.cz/top/soudni-rozhodnuti/uzavirani-smlouvy-89710.html.

http://www.taxhavensguide.com/list-of-offshore-financial-centres.php.

http://cs.wikiquote.org/wiki/Václav_Klaus.)

http://ec.europa.eu/public_opinion/archives/ebs/ebs_325_sum_en.pdf dostupný online dne 27.12.2013

http://www.strukturalni-fondy.cz/cs/dostupný on-line dne 20. 9. 2010.

http://www.telegraph.co.uk/finance/g20-summit/9343250/G20-Summit-communique-full-text.htm.

http://www.uoou.cz/uoou.aspx?menu=14&loc=328 .

2011 and 2012 Annual Reports of the Financial Analytical Unit of the Ministry of Finance of the Czech Republic. Available from: http://www.mfcr.cz/cs/verejny-sektor/regulace/boj-proti-prani-penez-a-financovani-tero/vysledky-cinnosti-financniho-analytickeh/2011(2012).

http://www.fatf-gafi.org.

http://www.iosco.org.

http://www.iais.org.

http://www.rejstrik-insolvencni.cz./

Wolfsberg Anti-Corruption Guidance Paper August-2011 (published).pdf. [online] Wolfsberg Group Available from: <http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg%20Anti%20Corruption%20Guidance%20Paper%20August%2018-2011%20%28Published%29.pdf>.

Index

About the authors

Assoc. Prof. Ing. Jaroslav Brada, Ph.D.
He graduated from VŠE in Prague and the scientific and academic degree in the field of Finance was awarded to him at the same university. At present, he works as a university pedagogue at VŠE and VŠFS in Prague, specializing in financial investment pricing. He is an authorized expert in the area of banking industry, trading and dealing in stocks. He has experience in submitting expert opinions in the area of the so-called financial criminality.

Ing. Naděžda Blahová, Ph.D.
After graduating from VŠE in Prague, where she obtained the Doctoral Degree in Finance, she held superior positions e.g. in the banking industry. For the past 15 years she has worked as a pedagogue at the Department of Monetary Theory and Policy of VŠE in Prague. She also worked for the Bank Institute and VŠFS in Prague.

Ing. Josef Budík, CSc.
He graduated from ČVUT in Prague and afterwards he focused on economic research. Early 90´s he worked for the Central Bank in positions related to bank trading. After 2000 he worked on the stock market as a development specialist. At present, he is involved in pedagogical and scientific-research work at VŠFS in Prague.

Ing. Petra Korbasová
After graduating from VŠFS and obtaining the Master´s Degree, she joined a Doctorate Study Programme, Field of Finance, at VŠFS. She is employed as a specialist in the field of the financial market supervision at ČNB.

Assoc. Prof. Ing. Vladislav Pavlát, CSc.
After graduation he obtained scientific degree CSc. at VŠE in Prague. He is a college lecturer in economics, especially in the field of financial market at VŠFS in Prague. He was one of the founders of the Stock Exchange in Prague but he also pursued a scientific-research career, where he focused on management and management organization for many years. He is the author of many important publications.

PhDr. Bc. Ján Šugár, CSc.
He graduated from psychology and sociology, in which he also obtained scientific degree CSc. His professional experience includes his work as a soldier, but especially – after 1989 as a researcher focusing on sociological studies in the army. He currently works for the Police Academy of CR as a researcher, specializing in exposing the legalization of profits from criminal activity.

JUDr. Ing. Otakar Schlossberger, Ph.D.
After graduating in economy, Field of Banking Industry at VŠE Praha and Field of Law at Charles University, he had pursued a career in the field of banking industry and financial markets till 2011 (SBČS, sphere of commercial banking industry and banking cooperative system). In 2007, he obtained the doctoral degree in the field of finance at VŠE Praha. In 2003, after the election by the Chamber of Deputies of the Czech Parliament, he acted as the historically first financial arbitrator of the Czech Republic in the first term of office (till 2007 incl.). Since 1996 he has worked as a pedagogue, first at VŠE in Prague, then at the Bank Institute. Since 2010, he has been working as the chief of Finance Department at the University of Finance and Administration; he also cooperates externally with the Department of Banking and Insurance of VŠE in Prague.

JUDr. Michaela Katolická (born Kolářová)
She graduated from the Faculty of Law of ZČU in Pilsen; during her study at University Toulouse 1 Sciences Sociales in France she obtained the college degree in EU Law and the doctoral degree at Charles University in Prague. Since 2010 Michaela Katolická has been working for the Financial Analytical Unit of the Ministry of Finance, specializing in legislative matters related to the fight against the legalization of profits from criminal activity and terrorism financing.

JUDr. Adriana Vavrušková
After her Master Study Programme completed in 2006 at the Faculty of Law of Charles University in Prague, she obtained degree JUDr. in Financial Law at the same faculty in 2009. Since 2006, she has been professionally involved in the fight against the legalization of profits from criminal activity and terrorism financing and in the implementation of international sanctions. She was also a member of problem-solving teams for several projects related to the fight against money laundering. She is the co-author of the commentary to the Act on some measures against the legalization of profits from criminal activity and terrorism financing and related regulations (Tvrdý/Bártová, C.H. Beck 2009) and a regular lecturer at expert seminars and conferences focusing on the fight against money laundering and terrorism financing.

Otakar Schlossberger et al.

Anti-Money Laundering

Editor: Assoc. prof. Ing. Milan Kašík, CSc.
Publisher Vysoká škola finanční a správní, o.p.s. / University of Finance and Administration,
Estonská 500, 101 00 Praha 10,
www.vsfs.cz
Edition EUPRESS, number 195

Issue the monograph was approved by editors of scientific publishing.

First edition, Prague 2014
Prepress and production: Educo Uni Group, a. s., Estonská 500, 101 00 Praha 10
[CD-R]

© 2014 Otakar Schlossberger et al.
© 2014 Vysoká škola finanční a správní, o.p.s.

ISBN 978-80-7408-094-4

ISBN 978-80-7408-094-4