International Journal in Economics and Business Administration
Volume III, Issue 2, 2015

pp. 22 - 31

Processes and Technologies for Identifying Illegal Financial Operations

Josef Budik[1], Otakar Schlossberger[2], *[3]

Abstract:

The aim of the paper is to discuss law requirements and computer technology related to the processes carried out at identifying clients of banks and other financial institutions. Customer identification is an essential element of an effective customer due diligence programme which banks need to put in place to guard against reputational, operational, legal and other risks. There are mentioned in the paper the law requires that identification must be carried out inside any financial institution which negotiates the new account with the client.

The paper describes several approaches to identification. Various scientific and research results are available in printed information. It shows that the illegal operations of clients in these days usually identify bank employees. Communication technologies and computer equipment however has developed so much, and therefore computers could play a new role in money laundering. Illegal operations could currently be detected by a computer. Rapid development of banking technology has changed the way banking activities are dealt with. In conclusion, the present text identifies some problems that lie ahead of financial market in connection with a huge flow of money from black market economies.

The paper has been prepared within the project "Current trends in development of financial markets", supported by the Institutional support for long-term strategic development of research organization University of Finance and Administration in 2016.

Key Words: *crime, illegal behavior, banks, checking, risk*

JEL Classification: *K42, G21*

[1] Assistant Professor, University of Finance and Administration, Estonská 500, Prague, Czech Republic.
[2] Assistant Professor, University of Finance and Administration, Estonská 500, Prague, Czech Republic.
[3] * Acknowledgements: The paper has been prepared within the project "Current trends in development of financial markets", supported by the Institutional support for long-term strategic development of research organization, University of Finance and Administration in 2016.

Introduction

The topic of preventing a misuse of the financial system for money laundering was published as a Directive of the European Parliament and of the Council in 2005. In the Czech Republic, the topic of money laundering is addressed by a law from 2008. It prescribes financial institutions to verify the identity of clients and simultaneously gives them an opportunity of identification at a distance. Further, the law contains provisions on when the client's identification needs not to be done. In parallel with the development of the legislative environment, rapid developments can be seen in technologies and computer capacity. A technological point of view on the possibility to identify a client correctly also deserves our attention (Thalassinos *et al.,* 2013; Thalassinos *et al.,* 2014; Thalassinos and Liapis 2014).

The purpose of the paper is to analyse the current legal regulations and amendments to the "Fourth Directive" as regards anti-money-laundering measures. Another aspect that is discussed in the paper is banks' technological possibilities in relation to client identification.

1. Methodology

There exists an interest in using computers in processes oriented at anti-money-laundering measures; however, it is not significantly growing among theoreticians and their publications. The ProQuest database displayed only 65 results concerning the "financing and (money laundering)" entry in 2000–2015, of which only 26 were reviewed works and all of them were published in scholarly journals. Territorially, they were focusing on America and the EU, Jamaica, but also e.g. on Hong Kong.

1.1 Analyses of legal and supranationally adopted documents

One of the methodical approaches used by De Koker (2009) analysed the Recommendations of FATF (Financial Action Task Force) in detail. In another text, Clunan (2007) emphasized that combatting financing of terrorism is comprehensive and requires measures both international among individual countries and internal among agencies controlled by individual governments. She sees the source of money for subsequent "laundering" in thefts, drug sales or human trafficking. Nevertheless, she also mentions the fact that money can come from humanitarian organisations and charity activities. And donors are often totally unaware that their money finances terrorism.

1.2 Computers and computer models in the AML process

Suspicious transactions on accounts can be indicated by computer systems. According to Tang, Jun and Lishan Ai. (2013), it is possible to design integration of a customer relation management system and a system of registering suspicious data reported in commercial banks. The designed system consists of several layers and

can be used for the purpose of client identification and reduction of error messages about money laundering. The most important layer can be considered the analytical one which provides an in-depth analysis of client information – transaction history – and categorises customers by income, analyses risks and other connections. It uses a data storage for analyses and can conduct analyses from different points of view.

2. Discussion

The discussion in the presented paper is divided into the legislation-related topic and technological issues.

2.1 Legislation

Misuse of financial institutions for money laundering mostly occurs due to cooperation of entities that need to legalise funds with natural persons who, for a certain payment, conclude contracts with banks, open accounts, acquire other banking products that are subsequently used for legalisation of proceeds of crime activity.

Banks have to defend themselves against such misuse, as prescribed to them in the Czech Republic by the Act No. 253/2008 on some measures against legalisation of proceeds of crime activity and financing of terrorism. The basis for implementing the process of combatting money laundering and combatting financing of terrorism is a proper identification of clients. In the context of the Czech Republic, it is the Act No. 253/2007 on some measures against legalisation of proceeds of crime activity and financing of terrorism that deals with the client identification most comprehensively. It specifies the basic duties that must be performed at identifying the client as a party to a banking transaction.

2.2 Identification in connection with the type of transaction

The law provides for a general obligation to identify the party to a transaction if the transaction exceeds EUR 1,000, always before it is carried out. Then, following provisions of the law specify the method how the client identification is carried out. The identification attributes for natural persons are as follows:

- All the names and surname
- Birth certificate number (if not assigned, then the date of birth),
- Place of birth
- Gender
- Permanent or other residence
- Citizenship

For entrepreneurs, it is necessary, in addition to the above attributes, to verify their company name, place of business and the company registration number.

These facts must be checked against an identifying document if stated there. Moreover, in the information system or records financial institutions are obliged to enter the number of the identifying document, the country and the authority that has issued it and the period of its validity. The employee that carries out this identity verification is obliged to check sameness of the person's appearance with the photo in the identifying document. Various questions are raised because of these obligations already. One of them can be e.g. what to do when not all the data are included in the identifying document. For example, the identifying document of persons born outside the Czech Republic includes the country of birth instead of the place of it. Passports, being the basic identifying document for nationals from non-EEA countries, do not show permanent residence or domicile, etc. In practise, the missing data are thus replaced by the requirement of the person's statutory declaration on e.g. where he or she was born or what is his or her place of permanent residence.

In case of a stricter approach, it would be possible to require a production of the birth certificate, which is, however, omitted in practice. Nevertheless, the law at last does not provide for an obligation to require a statutory declaration or other actions by the identifying entity. It is thus an action that the law does not require, but it does not ban it either.

2.3 Taken-over identification

The bank must identify the client, but it is not necessary for the bank to verify the client's identity by itself. It may work with a taken-over identification. According to Schlossberger (2013) it basically means that another obliged person verified the client's identity and the third party thus supposes in a good faith that its client has already undergone a proper identification process. Which obliged persons can use the taken-over identification is clearly specified by law. It concerns e.g. persons with a certificate to provide investment services except for investment intermediaries, investment companies, investment funds, pension companies, pension funds, payment institutions, small-scale payment service providers, electronic money institutions, small-scale electronic money issuers, persons certified to provide leasing, guarantees, credits or money loans and so on. Of the above-mentioned it is evident that it concerns a wide range of persons who can use the taken-over identification. With regard to the above-mentioned facts, the authors will regard all the above-mentioned entities as "financial institutions" in the following text of this section.

At first sight it may seem that taking over clients' identification for the needs of a financial institution is highly advantageous for clients themselves. They need not undergo the entire identity verification procedure although it is not demanding for clients. Proof of identification attributes can be done very easily, as already mentioned above, i.e. for natural persons by showing an identifying document which is the ID card for citizens of the Czech Republic and the passport for foreign

nationals and possibly another official document recognised by the state (e.g. driving licence, birth certificate, etc.) from which all the necessary identification attributes will be evident.

Nevertheless, the law also takes into consideration the situation when the requesting entity is not sure whether the information received from the other entity is relevant. In such case the obligation is basically not to take over the data and not to use this method of client identification.

An even more risky situation can be seen when a financial institution is in the position that it is requested to provide data about its client. This institution "runs a risk" of giving information about its client to someone who is not entitled to it. It is mainly the situation when communication can run also by e-mail.

Telephone inquiries or requests to provide client information should not be responded to. A provable and objective communication should always take place, while the risk of the adverse party is always to be eliminated. Basically it means that the requested financial entity has to be a hundred per cent sure that the requesting party falls into the category of entities that are entitled to work with the taken-over identification data and that this entity really exists.

For the purposes of use of the taken-over identification data and mutual positive communication between two financial entities it would be ideal if representatives of both parties knew each other from previous cooperation, from business contacts, which would essentially eliminate the risk of the adverse party.

Taken-over identification data are also connected with another fact that a financial institution takes over identification data and subsequently finds out that the data are spurious, false or related to a completely different person (e.g. misused personal data of another natural person). Then there is a question who would be liable e.g. for damage that could be caused to the financial institution that took over such data from another institution in a good faith that they are correct. At this point it is impossible to foresee what court judgement would be in case of disputes between these two institutions; however, it is evident from the above-mentioned that it is impossible to rely on the taken-over identification data, especially if an active (e.g. credit) deal is to be made. How to prevent this situation? Simply by not using the possibility of taken-over identification data. Financial institutions can be fully recommended to verify clients' identity by themselves and use the taken-over identification data as little as possible, since in the presence of the client, being a natural person, or the statutory representative or the authorised agent in case of a legal person, the client identification process is not that complicated and lengthy.

2.4 Regarding identification carried out at a distance

The final section of this text deals with client identification carried out at a distance. It is basically a method when the client who wants to become a client of a financial institution can, if permitted by the financial institution, use the offer to carry out his or her identification in a remote way. In the Czech Republic, the law terms it identification carried out at a distance. The law specifies the obligations which a given financial institution has to meet and for which it has to prove that its potential client has performed them. To summarise it briefly, it is the client's obligation to make a true copy of his or her ID and to send this copy to the new financial institution and subsequently to make the first payment towards the newly opened payment or equated account with this financial institution from any credit institution (i.e. only from a bank or savings and credit cooperative, not from an account of a payment institution) and to make copies of documents about this account which again he or she sends to a given financial institution.

This fact can be assessed as a high risk, especially if it is a natural person whose literacy is not sufficient. Here, the risk of adverse party is so high for the client that a general recommendation can be given not to use it expect for a highly reputable financial institutions. Possible frauds and subsequent misuse of personal data were dealt with in the book by Kyncl (2012) "Poznej svého klienta" ("Get to know your client"). Therefore, it is possible to state also here that the method of identification at a distance has to be approached even more carefully than the taken-over identification. The reason is that in case of taken-over identification two professional and financially erudite entities are involved, whereas in case of identification at a distance there is a completely non-professional party on one part and a professional party to the deal – a financial institution – on the other part. If the part of the professionals is taken by institutions at least registered with the Czech National Bank, "instinct of self-preservation" can be expected and therefore these institutions, or more precisely their employees will not carry out activities that would be contrary to law. An internal control and inspection system of a given institution should discover such conduct immediately. However, if it involves a financial entity or even any obliged person within the meaning of the law who are not subject to supervision by a state authority, the risk increases substantially. Therefore, it would be useful to call for an amendment to the current law and rule out some of the entities from the option of identification at a distance.

2.5 Simplified identification process

Some constraints of the identification process has been already discussed in the section above, but one important fact was omitted deliberately, specifically consideration of a possible approach to apply "simplified" identification. Why this fact can be considered at all will be briefly explained in the following section.

2.6 Impact of the Fourth Directive on client identification

The Directive of the EP and of the Council (EU) No. 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (hereinafter referred to as the "Fourth Directive") does not speak about identification of entities directly, but it does speak about identification of risks related to the possibility of money laundering taking into account "risk factors" such as the factors related to clients, countries, etc. The Directive does not mention client identification and identification attributes directly, as mentioned above, nor describes how the client's identity should be verified; however, it mentions verification based on the documents or even information received from reliable and independent sources. This provision is too wide for practical use, since it is a matter of interpretation what independent sources mean. The area of documents is, according to the authors, quite known. They will continue to include ID cards, passports, various extracts from official registers (business register, trade register, etc.). Nevertheless, the Fourth Directive, Article 25, mentions a possibility to rely on third parties at client due diligence, but it emphasises that the final responsibility for meeting the requirements of performing it correctly remains on the obliged person who should perform this due diligence itself. This indirectly allows further use of the above-mentioned taken-over identification, however, with emphasis on responsibility of the entity that has decided to use this option.

When applying the Fourth Directive it would be good to consider, with knowledge of the client's risk category whether it were not really clearer and more understandable at transposition of the Directive to apply the simplified identification, or more precisely identity verification. It can justifiably expected that in the simplified due diligence of the client the current practices will continue, that means the client will be identified at distance or by means of the taken-over identification. According to the authors, it is not good to continue with these practices in the long run. However, it depends on the member states how they resolve the above situation.

3. Computers

The experience of financial institutions – banks in particular – is that there might be clients whom the bank does know, verifies their identity and no suspicion of illegal intentions is raised at the identification process. However, when working with the bank account, they start requesting transactions that do not match the life style of the household (account holder) or the existing method of undertaking by the company. It can be one of the payment services that are discussed in detail by Schlossberger (2012).

There is little probability that bank employees would be able to monitor their clients' transactions in detail. We must take into account the data mentioned by the Czech National Bank in its most recently published report (2015):

- One bank employee is allotted 268.8 citizens, on average;
- One point of sale (bank office) attends to 5,000 citizens, on average;
- One bank provides services to 233,900 citizens, on average.

If high-performance computer systems are implemented in banks, they may alert banks to suspicious activities on which particular accounts. According to Karttunen, Ammanda and O´Keefe, Rae, Lynn (2015), the algorithms are based on the knowledge that suspicious are such accounts for which a financial institution records many small deposits transferred to other accounts shortly after their depositing. These accounts often have a high overall depositing activity and minimum balances. Analyses also point out that money laundering suspicion should be also raised when the account receives deposits from many different natural and legal persons and often from many territories and from non-banking entities. Suspicious should be also accounts with many deposits from many sources (i.e. cash, cheques, electronic payments, etc.).

Money laundering suspicion is also indicated by situations when:

- Immigrants open accounts in a given country and then transfer money to another country (often electronically);
- When deposits are withdrawn or transferred elsewhere immediately (in 1 or 2 days);
- Accounts receive anonymous deposits from domestic depositors followed by rapid withdrawals abroad.

In such cases, it is mostly an activity of natural persons. Suspicious methods of account usage can be also employed by companies, i.e. legal persons. It is manifested, for example, as follows:

- Accounts show such financial activities that do not correspond to the business activity or employment of their holder,
- Accounts show a rapid change in activity.

Both natural and legal persons may try to use individual branches of financial institutions for purchasing securities and other products of financial markets with the purpose of masking connection of the deposited money with cross-border transfers.

The above-mentioned processes are routinely being evaluated already now. However, it is impossible to check all the clients' operations systematically and every day. Based on signals from the computer model, an experienced employee or a forensic analyst can rapidly specify a potentially suspicious account, its holder and identify potential evidence.

Conclusion

The aim of this paper was to characterise different ways of client identifying clients of financial institutions. The authors came to the conclusion that based on practical experience it would be useful to limit or entirely cancel the possibility of taken-over identification or identification carried out at a distance, especially for such financial entities that are not banks. Based on the analysis of the current legal regulation of the

identification process, amendment to the law with respect to the possibility to use the "simplified identification" for selected deals can be recommended. The new Fourth Directive reckons with such alternative as part of the simplified due diligence of clients. Consequently, it would more than desirable to use this opportunity and include the above proposals to the amendment to the national legislation at transposition of the Fourth Directive.

Implementation of high-performance computer systems may facilitate and give precision to detection of suspicious activities on client accounts, as well as in situations when employees do not have a possibility of everyday personal monitoring of deposits, withdrawals and transfers – often carried out electronically – on client accounts.

Acknowledgement

The paper has been prepared within the project "Current trends in development of financial markets", supported by the Institutional support for long-term strategic development of research organization, University of Finance and Administration in 2016.

References

Clunan, Anne L. 2007. "The Fight Against Terrorist Financing." *Political Science Quarterly* 121(4):569-596 (http://search.proquest.com/docview/208276644?accountid=37662).

Czech National Bank Report on Financial Market Supervision in 2014 Prague 2015. 148 pages. ISBN 978-80-87225-60-8. Made available online on 11 May 2016 at http://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/dohled_financni_trh/souhrnne_informace_fin_trhy/zpravy_o_vykonu_dohledu/download/dnft_2014_cz.pdf

Koker, Louis. 2009. "Identifying and Managing Low Money Laundering Risk." *Journal of Financial Crime* 16(4):334-352 (http://search.proquest.com/docview/236012000?accountid=37662). doi: http://dx.doi.org/10.1108/13590790910993717.

Karttunen, Ammanda and O´Keefe, Rae, Lynn. FRAML for Dummies. Verafin Special Edition. John Wiley & Sons, Inc. 2015. 68 pages. ISBN 978-1-119-11227-3

Kyncl, L. et al.: Get to know your client – Basic principles of financial law (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

Schlossberger, O. Payment services. 1st edition Prague: Management Press, 2012, 325 pages. ISBN 978-80-7261-238-3

Schlossberger, O. at al. Do you know your client (Znáte svého klienta). 1st edition Prague: EUPress, 2013, 96 pages. ISBN 978-80-7408-090-6

Tang, J. and Lishan Ai. 2013. "The System Integration of Anti-Money Laundering Data Reporting and Customer Relationship Management in Commercial Banks." Journal of Money Laundering Control 16(3):231-237

(http://search.proquest.com/docview/1370336913?accountid=37662). doi: http://dx.doi.org/10.1108/JMLC-04-2013-0010.

Thalassinos, I. E. *et al.*, (2013). Way of Banking Development Abroad: Branches or Subsidiaries. *International Journal of Economics and Business Administration*, *1*(3), 69-78.

Thalassinos, I.E., Liapis, K. and Thalassinos, E.J. (2014). The role of the rating companies in the recent financial crisis in the Balkan and black sea area. *Chapter book in Economic Crisis in Europe and the Balkans*, *79-115, Contributions to Economics, Springer International Publishing, DOI: 10.1007/978-3-319-00494-5-6.*

Thalassinos I.E. and Liapis K. (2014). Segmental financial reporting and the internationalization of the banking sector. *Chapter book in, Risk Management: Strategies for Economic Development and Challenges in the Financial System,(eds), D. Milos Sprcic, Nova Publishers, 221-255, ISBN: 978-163321539-9; 978-163321496-5.*