THE NEW TECHNOLOGIES AND THE FIGHT AGAINST MONEY LAUNDERING AND THE TERRORISM FINANCING

Eva Jančíková[114]
Stanislava Veselovská[115]
DOI: https://doi.org/10.31410/EMAN.2018.334

Abstract: *Money laundering and terrorism financing can have potentially devastating social, economic, and security consequences. Combating Money laundering is an important part of the overall fight to drug dealing, organised crime and since a number of years, also against terrorist financing. The past twenty years we can see an enormous amount of technological changes and the banking industry has to be prepared to adapt their procedures to the new innovative products and technologies. The aim of this paper is to define the impact of new products and technologies on banks' practices in the fight against money laundering and terrorist financing. In order to meet our aim we analyse how the banking sector in Slovak Republic is prepared to handle these new challenges. We are evaluating primary and secondary data, using qualitative methods such as analysis, synthesis, comparison and basic statistical methods.*

Key words: *Money Laundering, Terrorism financing, New Technologies, Banking industry in SR*

1. INTRODUCTION

Money laundering and terrorism financing can have potentially devastating social, economic, and security consequences. The negative impacts of money laundering tend to be magnified in these markets because they tend to have less stable financial systems, a lack of banking regulations and effective law enforcement, and, therefore, are more susceptible to disruption from criminal or terrorism influences.

But before asking the question of how to combat money laundering, perhaps the first question should be: What is causing it? One viable answer is embedded in the globalization and technological advancement that has shaped the world these past few decades. Controlling the hundreds of billions of transnational transactions that take place yearly all over the world has proved to be difficult to say the least. This challenge has been made potentially more difficult with the gaining momentum of a technology named Bitcoin. [1]

As a reaction to the new situation, in October 2006, the Financial Action Task Force (FATF) published a typologies report on new payment methods (NPMs) used for legitimate economic transactions which could be exploited by money launderers. Featured were the increasing role of non-banks in offering prepaid value cards, electronic purses, mobile payments, internet payment services and digital precious metals. The FAFT continued to follow up these issues and published regular reports related to various NPMs including reports “Money Laundering

[114] University of Economics in Bratislava, Faculty of International Relations, Dolnozemská cesta 1, 852 35 Bratislava 5, Slovakia
[115] Paneuropean University in Bratislava, Faculty of Economics and Entrepreneurship, Tematinská 10, 851 05 Bratislava, Slovak Republic

using New Payment Methods" [6], and "Virtual Currencies, Key Definitions and Potential AML/CFT Risks" [5].

In 2009 the European Commission (EC) addressed the possible misuse of NPM by terrorists and in the Stockholm programme stated that the instruments for combating the financing of terrorism must be adapted to the new potential vulnerabilities of the financial system, as well as cash smuggling and abuse of money services, and to new payments methods used by terrorists. [3]

The aim of this paper is to define the impact of new products and technologies on banks' practices in the fight against money laundering and terrorist financing. In order to meet our aim we analyse the international AML/CFT regulation, institutional cooperation and how the Slovak Republic is prepared to handle these new challenges. We are evaluating primary and secondary data, using qualitative methods such as analysis, synthesis, comparison and basic statistical methods.

2. LEGISLATION ON MONEY LAUNDERING AND TERRORIST FINANCING IN SR

In June 2017 the Fourth Anti-Money Laundering Directive (AMLD 4) entered into force to strengthen the existing rules with ambition to make the fight against money laundering and terrorism financing more effective. On 1 February 2018, the Slovak Parliament has adopted an amendment to the Act No. 297/2008 Coll. on the Prevention of Legalization of Proceeds of Criminal Activity and Terrorist Financing, which implemented AMLD4 to Slovak legal system. The new legislation reinforces the existing rules by introducing the following changes:

- reinforcing the risk assessment obligation for banks, lawyers, and accountants;
- setting clear transparency requirements about beneficial ownership for companies. This information will be stored in a central register, such as commercial registers, and will be available to national authorities and obliged entities;
- facilitating cooperation and exchange of information between Financial Intelligence Units from different Member States to identify and follow suspicious transfers of money to prevent and detect crime or terrorist activities;
- establishing a coherent policy towards non-EU countries that have deficient anti-money laundering and counter-terrorist financing rules;
- reinforcing the sanctioning powers of competent authorities. [2]

One of the most important tools used in AML/TF is the knowledge of methods used for money laundering which are increasingly sophisticated and complicated, which also makes them more difficult to detect. It is anticipated that in the coming period the attention of the perpetrators of this activity will focus mainly on:

- the misuse of electronic money by using more sophisticated ways of committing crime using false identification documents and people in need who are usually resident outside the European Union,
- establishment of specialized companies and profiling of professionals carrying out hiding and placing of proceeds from crime and their legalization to order,
- investments of foreign entities committing criminal activity in the Slovak Republic and vice versa; investments in real estate, securities, goods of high value and in the shares of companies,
- private banking, which offers, in particular, wealthy clients comprehensive banking services, securities transactions issued by the client's bank,

- increased organizer and flexibility of offenders to place illegally acquired funds, mainly from Internet fraud and phishing; in the case of organized groups, it is often a national community, and there is a prerequisite for the mutual cooperation of several such groups of different nationalities,
- use of domestic and foreign accounts for on-line betting,
- expansion of high gambling on the territory of the Slovak Republic,
- gradual transfer of trafficking in human beings, drugs, weapons and stolen motor vehicles from natural persons to commercial companies,
- gradual engagement of the non-financial sector (notably notaries, lawyers, auditors, tax advisers, accountants and estate agents) into the legalization process,
- actively engaging tax advisers and accountants in placing, blending and integrating illegally acquired money into the legal economy,
- increasing the number of non-profit organizations, non-investment funds and foundations, while increasing the number of foreign financial transactions through these organizations,
- placement of proceeds from crime on life insurance accounts and other alternative savings products outside banks,
- increasing the number of transactions realized in favour of companies with headquarters in the so- tax havens or in favour of companies that are registered in a European Union country but which are property linked to companies registered in offshore areas,
- enforcement of claims for the refund of value added tax and subsequent placement of revenues in a legal business environment.

Regarding the control of the fulfilment of the obligations of the obliged persons, the law was also included among the supervisory authorities by the National Bank of Slovakia and the Ministry of Finance of the Slovak Republic, thus ensuring greater control efficiency. Both institutions have the power to control only the entities in their competence. If the supervising or state supervisor of a liable entity detects a violation of the law, the information shall be immediately notified to the Financial Intelligence Unit (FIU). For banks, it is necessary to define the basic standards of bank behaviour towards itself, within the bank and especially towards clients. In addition to ethical principles, it is important for the bank to identify also regulated rules of conduct in relation to clients and investors regarding integrity, transparency and avoidance of conflicts of interest in the conduct of banking activities. The Act on the Protection of Legalization of Income from Crime and Terrorist Financing also defines the Financial Intelligence Unit as a special unit within the framework of the Financial Police Service and defines its tasks and powers. We can see the positive results of this Act in increasing dynamic development of received unusual transaction reports (UTR) after 2008 (Figure 1).

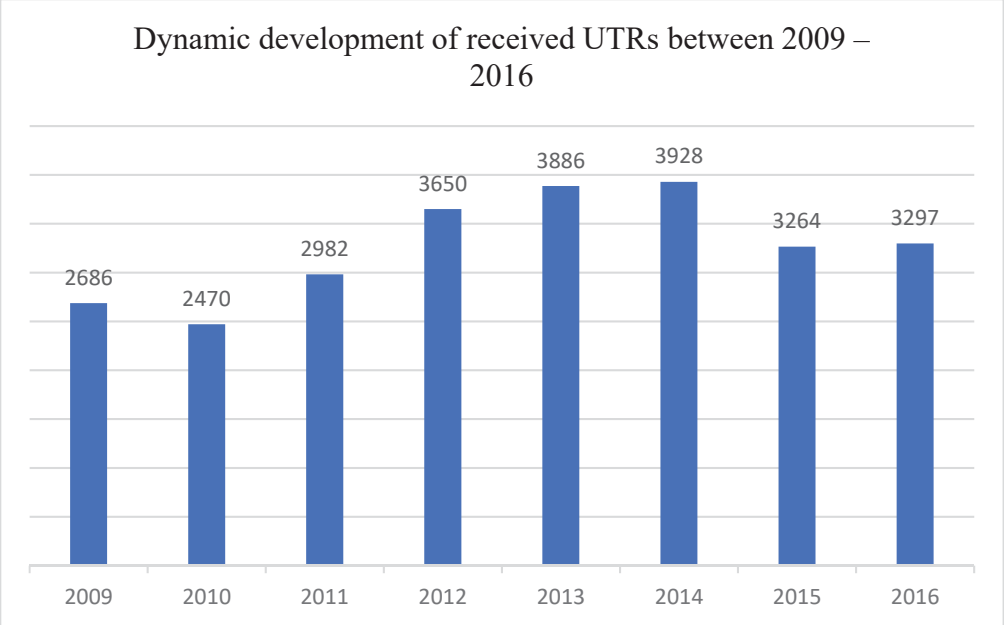

Figure 1: Dynamic development of received UTRs between 2009-2016
Source: Author´s calculations based on Annual Reports of Financial Intelligence Unit of the SR 2009-2016 available on https://www.minv.sk/?informacie-o-cinnosti-1

In 2016 FIU received 3297 UTRs in total amount of 1.803.820.832,- EUR from all Obliged Entities. On the basis of the legal characteristic of the Obliged Entities stipulated by the AML/CFT Law the particular UTRs could be split into 3 fundamental groups:

- the UTRs in total number of 3073 received from all the banks acting in the territory of the Slovak Republic, including the National Bank of Slovakia (NBS),
- the UTRs in total number of 179 received from financial institutions other than banks,
- the UTRs in total number of 45 received from non-financial institutions. [8]

TYPE OF OBLIGED ENTITY	2014	2015	2016
National Bank of Slovakia	126	77	79
Commercial banks	3252	2876	2994
Central Depository and Asset MNG Co.	20	34	11
Insurance Company	174	112	65
Pension Insurance Company	64	1	41
FX office	8	9	5
Leasing and Factoring Companies	25	21	19
Payment Institutions	129	53	38
Gambling Game Operators	6	22	15
Postal Undertake	108	54	22
Court Distrainer, Lawyers, auditors	1	4	8
Other Non-Financial Subjects	15	1	-
TOTAL	**3928**	**3264**	**3297**

Table 1: Number of UTRs sent by banks in 2014-2016
Source: Author´s calculations based on Annual Reports of Financial Intelligence Unit of the SR 2014-2016 available on https://www.minv.sk/?informacie-o-cinnosti-1

We can see that in Slovak Republic the most important obliged entities are commercial banks, NBS, insurance companies, payment institutions and postal undertake. Regarding the control of the fulfilment of the obligations of the obliged persons, the law was also included among the

supervisory authorities by the National Bank of Slovakia and the Ministry of Finance of the Slovak Republic, thus ensuring greater control efficiency. Both institutions have the power to control only the entities in their competence. If the supervising or state supervisor of a liable entity detects a violation of the law, the information shall be immediately notified to the FIU. [8]

From the Table 2 we can read that wire transactions domestic and foreign are beside the cash transaction the most frequent. These transactions are realized mostly through electronic banking channels.

Patterns of UTRs	Number of UTRs	Value of UTRs in EUR
Wire transactions	2193	1 036 403 045
Cash transactions	1907	631 208 890
Foreign transfers	1272	617 924 215
Offshore transactions	71	75 323 221
Phishing, Pharming	30	1 041 188
Insurance	41	12 518 802
Real estates	60	20 273 312
Internet frauds	106	5 232 541
Counterfeited securities	3	50 070
Hazard	15	1 442 971

Table 2: Summary of the patterns of UTRs in 2016
Source: Author´s calculations based on Annual Reports of Financial Intelligence Unit of the SR 2016 available on https://www.minv.sk/?informacie-o-cinnosti-1

In 2016 the most frequent transactions registered, analysed and assessed by FIU were: wire transactions, cash transactions, foreign transfers, transactions realized by subjects in countries so called "tax heavens" (offshore transactions"), phishing, pharming, internet frauds and hazard.

3. NEW PAYMENT METHODS AND THEIR POTENTIAL FOR MISUSE IN EU AND SLOVAK REPUBLIC

New payment methods (prepaid cards, mobile payments and Internet payment services) have become more widely used and accepted as alternative methods to initiate payment transactions. Some have even begun to emerge as a viable alternative to the traditional financial system in a number of countries. The rise in the number of transactions and the volume of funds moved through NPMs has been accompanied by an increase in the number of detected cases where such payment systems were misused for ML/TF purposes. Based on the analysis of case studies FATF identified red flags which are relevant to all NPM products and services. These red flags can be used as indicators of suspicious activity where a product´s actual use deviates from its intended use or does not make economic sense. For example, cash withdrawals in foreign jurisdictions will be expected where the product is a prepaid traveller card, but unusual where the product is marketed to minors. Red flags should therefore not be applied unthinkingly, but tailored to the product´s characteristics. [6]

According to EU legislation, the issuing of electronic money is a regulated financial activity, regardless of any value limits or thresholds that may apply to a certain product. Accordingly, issuers of electronic money are subject to the member states´ national AML/CFT laws.

The new EU regime for the issuance of e-money as revised by the second E-Money Directive 6(EMD) aims at facilitating market access to newcomers, namely telecommunication companies or large-scale retailers who want to engage in the market of e-money. Following the Payment Services Directive, the exclusivity principle will no longer apply to electronic money institutions, who are now entitled to engage in any business activity besides issuing electronic money.

In this part we would like to analyse the most important instruments of NPMs and their use in EU and in Slovak republic.

Prepaid payment cards provide access to monetary funds that are paid in advance by the cardholder. While there are many different types of prepaid cards that are used in a variety of ways, they typically operate in the same way as a debit card and ultimately rely on access to an account. There may be an account for each card that is issued or, alternatively, there may be a pooled account that holds the funds prepaid for all cards issued. The cards may be issued by, and accounts may be held at, a depository institution or a non-bank organization; pooled accounts would be normally held by the issuer at a bank.[5]

In European Union 13 prepaid card issuers are operating with e-money license. Of the 3 biggest prepaid products offered, 2 non-reloadable have a maximum limit of 150 EUR and one is a Mastercard reloadable prepaid; estimated 164 million cards at end of 2008. When maximum limit of 150 EUR for non-reloadable and 2 500 EUR for reloadable cards – no CDD necessary. In Slovak Republic 12 providers (banks) have issued almost 4 million cards; agents can serve as intermediaries and are covered under the Payment Services Directive (2007/64/EC). [6]

Internet payment services are payment services that rely on a bank account and use

Eva Jančíková, PhD.
Educations
201 - habilitation in Economy and Management, University of Sopron, Faculty of Economics
2002 - PhD. in International Economic Relations, University of Economics, Faculty of Commerce, Bratislava.
1995 –1996 Diploma from the Jack t. Conn Graduate School of Community Banking, Oklahoma City University, Oklahoma City (USA).
1993 McINTIRE International Baking School, University of Virginia, Charlottesville (USA)

Work Experiences
1979 – 2009 ČSOB, a.s. Bratislava (KBC Bank) – Retail Banking Manager, Trade Finance Division Director, Finance Director in ČSOB Factoring.
2009 Assistant Professor and 2017 Associate Professor at University of Economics in Bratislava, Faculty of International Relations
Specialisation: Trade Finance, Banking, International Finance

Most important publications:
JANČÍKOVÁ, Eva - PÁSZTOROVÁ, Janka. Internationalization of Renminbi. – Registered in: Scopus. In Actual problems of economics : scientific economic journal. - Kyiv : National academy of management, 2015. ISSN 1993-6788, 2015, no. 7, pp. 377-387.
JANČÍKOVÁ, Eva - STRÁŽOVSKÁ, Ľubomíra. New trends in financing small and medium enterprises in the EU. - Registrovaný: SCOPUS. In Actual Problems of Economics : peer-reviewed journal. - Kiev : National Academy of Management, 2015. ISSN 1993-6788, 2015, no. 11, pp. 87-95.
JANČÍKOVÁ, Eva - RANETA, Leonid - BRAGA, Denys. Internationalization of renminbi and the real effective exchange rate. In Ekonomický časopis : časopis pre ekonomickú teóriu, hospodársku politiku, spoločensko-ekonomické prognózovanie = journal for economic theory, economic policy, social and economic forecasting. - Bratislava : Ekonomický ústav SAV : Prognostický ústav SAV, 2016. ISSN 0013-3035, 2016, roč. 64, č. 7, s. 666-685.

the Internet as a means of moving funds to or from a bank account; payment services provided by non-bank institutions operating exclusively on the Internet and that are only indirectly associated with a bank account. [5]

In European Union 18 online payment service providers (over 90 million accounts but not all active) – two main ones have 65 million and 10 million accounts respectively. In Slovak Republic provided info on both online banking services (not covered in this report and online payment services) for a total of 21 providers – number of online payment services not clearly identified. [6]

Mobile payments refer generally to the use of mobile phones and other wireless communications devices to pay for goods and services. Payments are initiated from a mobile communications device using voice access, text messaging protocols (such as short/single messaging service or SMS), or wireless application protocols (WAPs) that allow the device to access the Internet. Authorization often occurs by keying in a unique personal identification number (PIN) associated with the customer or mobile device. Adoption of mobile payments varies from country to country. [5]

The estimate number of providers in EU is 8; accounts can be funded by credit card or bank transfers, and between account holders with the same mobile payment provider; payments done using SMS. In SR they are 3 mobile service providers. [6]

The trend in Slovak Republic over the last four years shows that the amount of cash is slightly decreasing. People are starting to use other payment methods (cashless payments and card transactions). In 2016 the volume of cash withdrawals declined by 1,19% and the number of withdrawal declined by 4,88% compared to 2015. [4]

5. CONCLUSION

Combating Money laundering is an important part of the overall fight to drug traffic, organised crime and since a number of years, also against terrorist financing. Thirty years after adoption of the first international convention, the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances we can see that this fight is not over yet. Just the opposite. Every day we can realize new challenges to combat money laundering and terrorist financing. The globalisation and new technologies has shaped the world these past few decades. For all the good the open borders and online-bank transfers have given us, it has also given criminals a whole new playing field in which to transfer and conceal illicitly gained money, allowing them to lower the transaction costs of crime. It is more and more difficult to control the hundreds of billions of transnational transactions that take place yearly all over the world.

The anti-money laundering legislation in Slovak Republic is in accordance with international and European Union standards but still we can still see reserves in their application in practice.

REFERENCES

[1] Bååth D., Zellhorn Handledare F. (2016). *How to combat money laundering in Bitcoin? An institutional and game theoretic approach to antimoney laundering prevention measures aimed at Bitcoin.* [online]. [cit.2018-02-22]. Available at: www.liu.se

[2] European Commission (2016). *Commission strengthens transparency rules to tackle terrorism financing, tax avoidance and money laundering, Strasbourg, 5. July 2016.*

[online]. [cit.2018-02-22]. Available at: http://europa.eu/rapid/press-release_IP-16-2380_en.htm

[3] European Council 2009, *Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC*, [Online]. [cit.2018-02-22]. Available at: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:EN:PDF

[4] European Payment Council. (2018). *The Slovak payment landscape.* [Online]. [cit.2018-02-22]. Available at: *https://www.europeanpaymentscouncil.eu/news-insights/insight/slovak-payment-landscape*

[5] FATF, (2006) *Report on new payment methods*. [online]. [cit.2018-02-22]. Available at:http://www.fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf

[6] FATF, (2010). *Money Laundering Using New Payment Methods- October 2010.* [online]. [cit.2018-02-22]. Available at: http://www.ctif-cfi.be/website/images/NL/typo_fatf/46705859.pdf

[7] FATF (2014). FATF Report. *Virtual Currencies Key Definitions and Potential AML/CFT Risks.* [online]. [cit.2018-02-22]. Available at: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

[8] The Ministry of Interior of the SR (2018). *Annual Reports of Financial Intelligence Unit of the SR 2009-2016.* [online]. [cit.2018-02-22]. Available at: https://www.minv.sk/?informacie-o-cinnosti-1

[9] The National Council of the Slovak Republic (297). *Act No. 297/2008 Coll. on Protection against the Legalization of Income from Crime and on the Protection against the Financing of Terrorism.* [online]. [cit.2018-02-22]. Available at: *https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2008/297/20160701*

[10] VYHNÁLIK, J., FENDEKOVÁ, I. (2005). *Tretia smernica EÚ proti praniu špinavých peňazí a financovaniu terorizmu.* In *Biatec.* ISSN 1335-0900, 2005, vol. 13, iss. 9, pp. 10-14.