Antonín Korauš,
Professor, dipl. Eng., Ph.D., LL.M., MBA,
Academy of the Police Force in Bratislava, Slovak Republic

Miroslav Gombár,
Associate professor, dipl. Eng., Ph.D.,
University of Prešov in Prešov, Faculty of Management, Slovak Republic

Filip Černák,
Mgr., PhD. Student,
University of Prešov in Prešov, Faculty of Management, Slovak Republic

DETECTION OF UNUSUAL BUSINESS OPERATIONS

Published: 20 March 2022

Abstract. *Effective measures to prevent the proceeds of crime from entering the legal financial system require the development of scientifically sound methods that can form the basis for software that can systematically reveal unusual business operations. The systematic detection of such operations depends on the development and implementation of new software based on scientifically well-founded methods.*

Keywords: *money laundering, cross-border crimes, criminal law, criminal law, detection and prosecution of crime.*

Citation: Korauš, A.; Gombár, M.; Černák, F. (2022). DETECTION OF UNUSUAL BUSINESS OPERATIONS. Conferencii, (2) 4. http://doi.org/10.51586/RAI2022-2-4

Introduction

Within academic research on the issue of money laundering, to which the question of unusual business operations relates, there are contributions of varying levels of quality. The best work is published in journals indexed in the Web of Science database. There are not a few such contributions but often researchers choose not to publish their algorithms or procedures, preferring to patent them instead because making them public could have an undesirable impact on the detection of unusual business operations. It is more common for contributions to concern themselves with developing the fundamental framework from which anti-money laundering applications can be built.

Contributions can also be classified in two types based on their content. The first group consists of research that focuses on the literature about money laundering and secondary data. There are very few cases of empirical research on money laundering or measures to control it. This type of research is based mainly on theory, with support from analysis and deduction. The papers are analytical and often

descriptive in character. The second group is based on the description of mathematical and statistical methods and algorithms that are used in the development of tools for identifying unusual trading operations linked to money laundering. These papers are analytical and precise in character.

Literature Review

The detection of unusual business operations is the continuous monitoring and evaluation of processes with regard to political, legal, economic, educational and technical measures to reduce the risks associated with the financial area (Limba et al. 2017). Detection of unusual business operations is one of the main concerns of state and delegated institutions, especially in increasing sophistication threats and attacks. Many vulnerabilities have led to the misuse of security infrastructure criminals.

The activities of criminals create problems with irrevocable transfer of funds, monetary loss, loss security breaches, disclosure and theft of customer personal data and intellectual property rights violations assets, leading to a significant financial loss of brand assets and a loss of investor / customer confidence in them financial institutions (Christiansen and Piekarz, 2019).

It is necessary to emphasize the detection of unusual business operations security issues, which are often perceived as synonymous with critical infrastructure security (Korauš et al., 2019a). Detection of unusual business operations security includes technologies, systems, processes, standards, regulatory frameworks that are financial institutions in euro area countries use it to prevent any form of intrusion into the organisation's network (Schwab, 2018). Therefore, the detection of unusual business transactions is an integral part of financial institutions. Her e-commerce is doing well platform as a modern means of business transactions using internet and mobile banking (Okoro and Ekwueme, 2018). Given the vulnerable impact on financial institutions in the euro area cyber security serves to protect these institutions (Thapliyal et al., 2017). Due to the complexity the cyber domain lacks sophisticated detection of unusual business operations to protect the network and other systems before the attack (Korauš et al., 2019b).

The issue of detecting unusual business operations is a major concern for financial institutions in euro area countries, as this threat the success of institutions

due to their complete reliance on information progress technologies (Bayuk, et al. 2012). With information technology financial institutions in euro area countries started e-commerce through the development of the Internet, networks, technological tools such as computers and computer systems, application and software development for mobile e-commerce applications, as well as development of codes, giving the institutions a competitive advantage (Ras, 2016). Due to the use of the Internet and due to the vulnerabilities that existed in the network, growth brought an increase in the detection of unusual business operations. These vulnerabilities have made it easier to hack and commit crimes such as illegal transfers of funds, identity theft, fraud and much more (Marty 2013). Litview Literre Review Literature Review

Mei and Gao (2014) provide a valuable insight into the state of the art in research on unusual operations and money laundering. In their paper they analyse academic journal articles on the fight against money laundering and terrorist financing indexed in the Web of Science database from 1993 to 2013. They identified a total of 891 published articles in Web of Science in the area in question. Our own research indicates that 193 articles were published in 2014–2015. From this it is possible to include that there is growing interest in this area in the scientific community, possibly as a result of alarming increase in money laundering and terrorist financing.

The article by Mei and Gao (2014) presents the state of development and the orientation of research on international money laundering based on an analysis of the distribution of authors, distribution organisations, cited journals and keywords.
The authors define three main fronts in research on money laundering. They are:

- research on predicting money laundering crimes;
- research on anti-money laundering legislation;
- research on the risk of money laundering in Germany.

Methods

This article deals with the results of research and subsequent analysis. Its aim is to contribute to knowledge and understanding of the behaviour of natural and legal persons in a financial environment aimed at detecting unusual business operation with a special focus on the aspect their safety. The article analyses the opinions and

attitudes of respondents to the issues security of payment systems and their behaviour when using unusual business operation.

Detection of unusual business operations (UBOs) is one issue in an increasingly important area of research and development in information and communication technologies currently being pursued by all the top scientific research institutions with an interest in the critical sector of services in the European Economic Area. These institutions have created a complex ecosystem for continuous research and innovation. Maintaining this continuity is critical for achieving the innovations needed to enable legal and security frameworks to keep up with expanding financial markets and economic growth in line with the commitments of EU countries in important documents such as Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005, Commission Directive 2006/70/EC of 1 August 2006, national legislation against money laundering and terrorist financing and laws on the implementation of international sanctions.

These legal frameworks represent high costs for the whole sector (e.g., obliged persons) especially as regards implementing automated procedures for evaluating unusual business operations, which amount to more than EUR 3 billion per year just in Slovakia. Under the legislation referred to in the previous paragraph, any legal or natural person who executes a non-standard financial operation becomes an obliged person with a duty to report the UBO.

Results and discussion

The detection of unusual business operations is a very topical issue not only in the Slovak Republic but throughout the European Union and also at the worldwide level.

In Slovak law, the definition of unusual business operations is laid down in Act No 297/2008 on protection against money laundering and terrorist financing and amending certain acts. Unusual business operations are legal acts or other acts bearing indications of being used for money laundering or terrorist financing.

The laundering of “dirty money” is a global problem with significant economic and social consequences. Financial institutions expend a major part of their resources on automated information systems to monitor transactions and experience indicates

that institutions are increasingly dissatisfied with their current automated monitoring capabilities and therefore seek software that can reduce the load on their compliance units. Some such systems are implemented quickly “out of the box” simply to satisfy regulators and subsequently calibrated to detect serious suspicious activity.

Continuing advances in computer technology increase interest in the use of information technology to fight money laundering, especially in areas such as using data mining to detect transactions involving proceeds of crime or sophisticated methods for detecting non-standard financial flows. In the past the fight against money laundering was studied mainly by financial and state institutions. With the tightening of laws in recent years and the intensification of the fight against money laundering and terrorist financing, the field is increasingly drawing the attention of universities.

The development of a new generation of systems in this area to meet future regulatory requirements and standards for the financial sector requires an interdisciplinary approach and more sophisticated information technology. Slovakia lags significantly in research and development on money laundering. There is practically no academic research and development in this area, though there is interest in establishing a partnership to build up a modern, well-equipped academic research centre to fill the gap in this important area of research.

Corruption and money laundering are internally connected. Crimes of corruption such as embezzlement of public funds are usually intended for personal gain and enrichment. Money laundering is the process of hiding illicit gains generated through crime. Successful money laundering can reduce the risk that these illicit gains will be confiscated.

Money laundering is also an issue of concern for the UN which has an organisational unit dedicated to it – the United Nations Office on Drugs and Crime (UNODC).

OECD activities in the area of tax crime and money laundering are supported by the measures issued by the Financial Action Task Force (FATF). These activities are implemented in various ways such as typological exercises, the preparation and dissemination of practical instructions for detecting money laundering for central tax

authorities, tax advisors and auditors, investigation of the key areas of risk and coordination of the procedures of OECD countries for sharing information on money laundering. The key material include OECD recommendations to facilitate co-operation between tax and other law enforcement authorities to combat serious crimes.

The Financial Action Task Force (FATF) sets standards for the development and support of national and international policies on combatting money laundering and terrorist financing. The FATF Recommendations are designed to ensure that the fight against money laundering and terrorist financing is fought effectively and corruption is wiped out. The measures focus mainly on:

- preserving the integrity of the public sector,
- protecting significant private sector institutions against abuse,
- increasing the transparency of the financial system,
- facilitating the detection, investigation and prosecution of corruption and money laundering and recovering stolen assets.

The implementation of a coordinated procedure in accordance with anti-money laundering standards creates an environment in which it is much more difficult for corruption to take root, thrive and, above all, remain undetected.

At present, it is possible to observe a change in patterns of criminal behaviour and the structure of crimes. Alongside traditional forms of crime there is increased prominence of new forms of crime committed by organised criminal groups. Crimes are planned with a long-term focus on high profitability and measures are taken to prevent their discovery. These new forms of crime focussing on high long-term profits, often employing sophisticated anti-detection measures are increasingly committed on an international scale.

Conclusion

The organised groups that are more and more often operating on the international level bring in enormous amounts of illicit income. The vast scale of these profits creates problems when criminals wish to introduce them into the legal financial system and invest them in profitable businesses or otherwise capitalise them.

It is noteworthy that the commercial and financial operations through which the proceeds of crime – dirty money – are introduced into the legal financial system are usually inconspicuous and barely distinguishable from normal operations. There is now a wide range of products and services available that facilitate the introduction of funds into the system. The use of information and communications technologies in banking, finance and payment system makes all transactions easier but also increases the risk of global money laundering and terrorist financing.

ACKNOWLEDGMENTS

This publication has been written thanks to the support of the Operational Programm Integrated Infrastructure for the project: "Electronic methods for detecting unusual business transactions in a business environment" (ITMS code: 313022W057), co-funded by the European Regional Development Fund (ERDF) and also by the "VEGA1/0194/19—Research on process-oriented management of financial management focusing on detection of tax evasion in terms of international business".

References

Arabska, E. (2016). Active social policies - insights in developing a functioning labor market. Balkan and Near Eastern Journal of Social Sciences BNEJSS 2016 (02) 03, pp. 47-63.

Bayuk, J.L., Healey, J., Rohmeyer, P., Sachs, M., Schmidt, J., Weiss, J. (2012) Cyber Security Policy Guidebook, Wiley Publishing, 2012, ISBN: 1118027809 9781118027806. http://www.fatf-gafi.org/

Christiansen, B., Piekarz, A. (2019) Global Cyber Security Labor Shortage and International Business Risk, IGI Global publishing, USA, ISSN 2327-3429.

Mei, D., Ye, Y. and Gao, Z. (2014) Literature Review of International Anti-Money Laundering Research: A Scientometrical Perspective. Open Journal of Social Sciences, 2, 111-120. doi: 10.4236/jss.2014.212016.

Korauš, A., Gombár, M., Kelemen, P. & Backa, S. (2019a). Awareness of security risks associated with payment systems analyzed by the methods of multidimensional statistics. Journal of Security and Sustainability Issues, 8(4), 687-703. https://doi.org/10.9770/jssi.2019.8.4(12)

Korauš, A.; Dobrovič, J.; Polák, J.; Backa, S. (2019b). Aspects of the security use of payment card pin code analysed by the methods of multidimensional statistics, Entrepreneurship and Sustainability Issues 6(4): 2017-2036. https://doi.org/10.9770/jesi.2019.6.4(33)

Limba T., Agafonov K., Paukštė L., Damkus, M., Plėta T. 2017. Peculiarities of cyber security management in the process of internet voting implementation,

Entrepreneurship and Sustainability Issues 5(2): 368-402. http://doi.org/10.9770/jesi.2017.5.2(15)

Marty, R., (2013) Cyber security: how visual analytics unlock insight, KDD '13 Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining, Pages 1139-1139, Chicago, Illinois, USA — August 11 - 14, 2013

ACM New York, NY, USA ©2013, ISBN: 978-1-4503-2174-7, http://doi.org/10.1145/2487575.2491132

Okoro, E. G., Ekwueme, C. M. (2018). Determinants of bank performance in Nigeria: the dynamics of internality and externality measures. Acta Oeconomica Universitatis Selye 7(1), 108 – 120. ISSN 1338-6581

Ras, J. (2016) Cyber Security, Lulu.com ©2016, ISBN:1365288234 9781365288234

Rusanov, G., Pudovochkin, Y. (2020). Money laundering in the modern crime system. Journal of money laundering control. DOI 10.1108/JMLC-08-2020-0085

Schwab, K. (2018) Global Competitiveness Report 2018, World Economic Forum91-93 route de la CapiteCH-1223 Cologny/GenevaSwitzerland. ISBN-13: 978-92-95044-76-0

Teichmann, F. (2017). Twelve methods of money laundering. Journal of money laundering control. Volume 20. Issue 2. Page 130-137. DOI 10.1108/JMLC-05-2016-0018

Teichmann, F., Falker, M. (2020). Money laundering - the gold method. Journal of money laundering control. DOI 10.1108/JMLC-07-2019-0060

Tai, CH., Kan, T.J. (2019). Identifying Money Laundering Accounts. Proceedings of 2019 international conference on system science and engineering (ICSSE). Book Series International Conference on System Science and Engineering. Page 379-382. ISSN 2325-0925

Thapliyal, K., Pathak, A., Banerjee, S. (2017) Quantum cryptography over non-Markovian channels, Journal Quantum Information Processing, Volume 16 Issue 5, May 2017, Kluwer Academic Publishers Hingham, MA, USA, https://doi.org/10.1007/s11128-017-1567-1

Unger, B., Linde, D. (2013). Research Handbook on Money Laundering. Edward Elgar Publishing. ISBN: 9780857933997. https://www.elgaronline.com/view/9780857933997.xml

Whisker, J., Lokanan, M.E. (2019). Anti-money laundering and counter-terrorist financing threats posed by mobile money. Journal of money laundering control. Volume 22. Issue 1. Page 158-172. DOI 10.1108/JMLC-10-2017-0061.