ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2019 Volume 6 Number 3 (March)
http://doi.org/10.9770/jesi.2019.6.3(3)

Publisher
http://jssidoi.org/esc/home

USING QUANTITATIVE METHODS TO IDENTIFY SECURITY AND UNUSUAL BUSINESS OPERATIONS

Antonín Korauš[1], Miroslav Gombár[2], Pavel Kelemen[3], Stanislav Backa[4]

[1] Academy of the Police Force in Bratislava, Sklabinská 1, 835 17 Bratislava 35, Slovak republic
[2,3,4] University of Prešov in Prešov, Faculty of Management, Konštantínova 16, 080 01 Prešov, Slovak Republic

E-mails:[1] antonín.koraus@minv.sk, [2]miroslav.gombar@unipo.sk, [3]kelemen.pavel@gmail.com,[4] stanislav.backa@gmail.com

Received 16 October 2018; accepted 29 January 2019; published 30 March 2019

Abstract. Financial institutions are the first vertical level in the fight against money laundering and to improve security. Therefore, it is essential that tools are available to enable effective detection and analysis of suspicious transactions, or unusual business operations. These, in line with the legislative requirements, report to responsible entities - FIUs representing the second vertical plane in the fight against money laundering. However, special software tools are available for obligated persons, especially for financial institutions that carry out tens of millions of financial transactions a day. These can trigger the alert to most unusual operations. The software automatically creates customer profiles, including expected behavior and executed transactions. Using advanced statistical analyses, it identifies unusual business operations, i.e. financial transactions significantly different from those carried out in the past. It is very useful to apply software support in form of electronic detection of indicators of legalization of crime proceeds. However, the output of such support software requires a more detailed and demanding investigation of the nature of operation and is based on the use of special algorithms based on mathematical and statistical methods. The software builds on the results of scientific research.

Keywords: security; unusual business operations; crime; money laundering; corruption; legal acts

Reference to this paper should be made as follows: Korauš, A.; Gombár, M.; Kelemen, P.; Backa, S. 2019. Using quantitative methods to identify security and unusual business operations, *Entrepreneurship and Sustainability Issues* 6(3): 1101-1112. . http://doi.org/10.9770/jesi.2019.6.3(3)

JEL Classifications: E26, E42, G21

1. Introduction

In mid-eighties, computational models based on biological neural networks begin to emerge in scientific contributions aimed at detecting unusual business operations associated with money laundering or terrorism. Mid-nineties are marked by the onset of the theory of fuzzy sets, fuzzy logic, and fuzzy decision making, as well as spatial statistics and, in particular, data mining. At the end of the last century, genetic algorithms were becoming popular.

Software support specifically designed for financial institutions to identify cases of legalization of proceeds of crime is based on the use of mathematical and statistical methods, especially those dealing with identification of remote values, probability distribution of data - Benford law, correlation and regression, time series, spatial statistics, core component, cluster analysis, decision trees, naive Bayes classifier, graph theory, game theory, fuzzy logic, fuzzy sets, and neural networks.

Data mining can be characterized as data stripping, discovery of knowledge in a database. It is a specific process of gathering new useful information. The process of modeling results in a description of patterns and relationships appearing in the data. It covers existing techniques of data analysis as well as knowledge and information acquisition (Mura et al, 2018; Zulova et al. 2018). The discovery of knowledge in the database is of interdisciplinary character. Data mining uses logistic regression and decision trees. Unlike the classical use of mining data, where the criterion of model quality lies in its accuracy, in case of fraud detection and money laundering, the criterion of quality lies in profitability, or in other words, in the probability of detecting fraud or money laundering (Jančíková, Veselovská 2018; Jančíková, Pásztorová 2018; Grančay et al., 2015; Mura et al. 2017).

2. Theoretical background

Gao, Ye (2007) dealt with using the process of data mining to identify money laundering. The FAIS (Financial Crimes Enforcement Network AI Systems), described by Senator (1995), allows mining data facilities to identify activities potentially related to the legalization of criminal proceeds.

Predictive data mining models suitable for the detection of insurance fraud were published by Hong and Weiss (2001). Bolton, Hand (2002) gave an overview of statistical methods for detecting fraud. Yamanishi et al. (2000) presented SmartSifter, a system identifying outliers, thus suitable for fraud detection, network monitoring, and so on. The system uses data mining. Taniguchi et al (1998) utilized data mining applications for telecommunication subchannels. Gao, Ye (2007) applied data mining techniques to identify transactions potentially related to the legalization of criminal proceeds. The authors compared the results obtained by using data mining with those achieved by traditional investigation methods. Weatherford (2002) and Phua et al. (2005) review the use of data mining in the detection of fraud. Shapiro (2002) gave an overview of the use of neural networks, fuzzy logic and genetic algorithms for fraud detection in insurance. Fu et al. (2012) combined data mining with the chart entropy matrix. They also presented an AML simulation system.

Article of Ngai et al. (2011) reviews and presents a detailed classification system for the use of data mining techniques to detect financial fraud. This document presents the first systematic, identifiable, and comprehensive review of professional literature on data mining techniques used to detect financial frauds. Forty-nine journal articles published from 1997 to 2008 were analyzed. The authors identified four categories of financial fraud (bank fraud, insurance fraud, securities and commodity frauds as well as other financial frauds). They identified six mining data classes (classification, regression, clustering, prediction, outlying values and visualization). The findings of the survey clearly show that data mining techniques have been used extensively to detect insurance fraud. Nevertheless, corporate frauds and credit card frauds have also attracted great attention of the authors in recent years. On the other hand, there is a clear lack of research on mortgage fraud and fraud in money laundering and securities and commodities. The main data mining techniques for detecting financial fraud are logistic models, neural networks, Bayesian networks and decision trees, all of which provide primary solutions to fraudulent data detection and classification problems.

Financial frauds affect millions of people every year and financial institutions must use methods for protecting themselves and their clients. Using statistical methods to address these issues faces many challenges. Financial frauds are rare occurrences leading to extreme imbalances in the data. The volume and complexity of financial data require algorithms that need to be effective. The article of Sudjianto et al. (2010) focuses on two important types of financial crime, namely fraud and money laundering. It describes some of the traditional statistical methods that have been used, as well as the newer neural networks and data mining. The aim of this article is to provide an overview of a wide range of methods accompanied by selected illustrative examples.

In recent years, the number of money laundering offenses has grown through foreign exchange and payment transactions. Cybernetic security issues, which are often perceived as synonymous with the safety of critical infrastructure (eg Dobrovič et al., 2017, Veselovska et al., 2017, Korauš, Kelemen 2018, Šišulák 2017, Limba, Šidlauskas 2018), need to be emphasized.

The Sohn study (2005) proposes four scoring models providing early warnings of money laundering in foreign exchange transactions for incoming and outgoing transfers of funds. Models of logistic regression, decision trees, and neural network are used as well as that combining all three previous models. It appears that the accumulated number of transactions is the most important indicator.

Hawkins (1994) defines an outlier as an observation that deviates so much from other observations as to arouse a suspicion that it was generated by a different mechanism. Frauds of a different nature, including the legalization of proceeds of crime, can be revealed as anomalies in the data. For this reason, outliers may become subject of interest in uncovering unusual operations.

Multiple statistical methods were used to identify outliers (Barnet & Lewis, 1994). We can divide outlier detection methods into two large groups. Methods based on probability distribution and distance-based methods. In the case of money laundering issues, distance-based methods (for example, Euclidean, Manhattan distance) are appropriate. These methods are also used for the detection of outlier in multidimensional cases (Knor, Ng 1997; Kosinski 1999; Knorr, Ng, Tucakov 2000). An unusual distance is that from the nearest neighbor. The literature lists three types of outlier identified by distance. Outliers are objects, whose average distances to the kth closest neighbors are the largest. This definition was used by Angiulli and Pizzuti (2002). Ramaswamy at al. (2000) have labeled n outlying objects whose distances to the kth closest neighbors are greatest. Knorr, Ng (1999) and Knorr at al. (2000) have labeled outlying objects for which there are fewer than p objects at a distance greater than d. Many outlier detection algorithms that work on small files cannot be used for databases containing tens or hundreds of millions of data. Hung, Cheung (1999), Hand and Blunt (2001) reported an algorithm for the detection of outliers in large databases. The Sherlock system for auditors uses a combination of detection of outliers with classification techniques (Bay et al. 2006). According to Zhu (2006), the detection of outliers is a key element for intelligent financial supervision systems to identify frauds and money laundering by discovering unusual behavior of customers. Detection procedures generally fall into two categories, namely by comparing each transaction against its account history, and then, in order to find out whether its behavior is unusual, by comparing it against the reference set. The paper presents an approach to reduce false positivity.

The Benford's law describes the probability distribution of the first and other significant numbers. It demonstrates that real data sets remarkably contradict the even probability distribution. To come to this conclusion, Benford analyzed 20,229 files from a wide variety of areas. From the statistical point of view, it is the conformity testing (for example, using the Chi-square goodness of fit test) of the empirical distribution of the first and other significant numbers of the studied accounting data with the theoretical division according to Benford's law. The Benford's Law is a simple and effective tool for detecting fraud in accounting (Durtschi at al. 2004). Nigrini (1999) used Benford's law for fraud detection in accounting. He also pointed out the difficulty in generating data that comply with Benford's law. To verify the validity of the Benford's Law, Nigrini and Mittermaier (1997) and

York (2000) have pointed it out as a technique suitable for audits. Not only is the Bernford's law applicable in detection of fraud in accounting, it can also be used for identifying money laundering from financial statements.

3. Research objective

Individual phenomena are always found in certain mutually dependent and determining relationships. The examination of their dependence requires an important step of choosing the appropriate statistical features that characterize given phenomena. The correlation number solves two basic tasks, namely the correlation task, which assesses the tightness of dependence and determines the characteristics describing to what extent the independent variables explain the variability of the dependent variable, and the regression task, which determines the shape of a regression function and estimates its parameters. Regression analysis provides a set of estimates that can predict the effect of certain variables on the variables examined. An important role is played by testing the statistical significance of variables. Nevertheless, caution should be exercised since mechanical testing of statistical significance may conceal actual significance by the size of the studied variable. Statistically significant relationships can be considered negligible if the effect size is too small. Statistical insignificance can occur with many effects that show a high degree of uncertainty. This could cause ignorance of potentially significant money laundering effects. Statistical significance itself is neither a necessary nor sufficient condition for real significance of the observed variable. Logistic regression models are among the generalized linear models. They are used to predict a discrete predictive variable from predictors. Logistic regression allows for identification of variables that significantly affect the affiliation of the object to a group and prediction of this adherence.

Several financial scandals in US corporations caused by accounting fraud have prompted an increase in researchers' interest in their early detection. Charalambos T. Spathis (2002) built a model using logistic regression to identify factors associated with false published financial statements of Greek companies. The accuracy of the correct classification exceeds 84 percent. Bell and Carcello (2000) on a sample of 77 fraudulent statements and 305 statements without fraud designed a logistic regression model to estimate the probability of fraud in the financial statement. On the basis of a set of 130 companies with detected fraud in 1989-2004 and 83 companies without fraud, Jay et al. (2006) have constructed logistic models. Annual averages, shares, percentage changes, and dummy variables entered the models. The likelihood of correct classification by model for the year in which the fraud was committed is 60.0 percent, while for the year before fraud, it is 55.8 percent, and for a year after fraud, it is 61.2 percent. Jay and others (2006) used a regression analysis to elucidate the causes of crime. Regression analysis plays an important role in the macroeconomic approach to measuring the extent of money laundering, especially in quantification based on currency demand, material input-based approach, usually electricity consumption and econometric approach when considering an unobservable variable between certain observable causes and consequences (Walker 1999; Schneider 2007; Straková et al. 2017). Reliable risk assessment method RM/RA CRAMM applicable for a crime risk assessment was described by Mullerova (2016), Mamojka and Mullerova (2017) for multi-purpose use and by Palkova et al.(2018a) for National Risk management system and for disasters (Palkova 2018b) and its legal questions by Mullerova and Mamojka (2017). At the micro level, it is mainly an estimate of the amount of proceeds from the sale of drugs, stolen goods, etc. The range of these activities is usually estimated in a few years and the values between them are approximated.

Cluster analysis is a method that enables to find internal structure in large-scale data sets in the form of so-called clusters. In case of large files, it is a key question to choose a suitable distance and right algorithm. Cluster analysis can also serve as a means for detecting outliers. Data remote from existing clusters can be considered as outliers. For clustering of huge and massive databases, special clustering algorithms need to be used (Williams, Huang 1997, Yamanishi et al. 2000, Zhang et al. 1996). Jiang et al. (2001) presented a two-stage clustering algorithm for outlier detection. The clustering approach suggested by Yang et al. (2014) is tested on bulk data provided by the bank. The result shows that this method can automatically detect suspicious cases of financial transactions. Rohit and Patel (2015) claim that clustering techniques are the best techniques for detecting non-cyclical operations.

Graph theory represents the discipline of applied mathematics. It is part of network theory. Organizational networks are important from the point of view of the analyzed issue. Special types of networks are often included in artificial intelligence and expert systems applications. Presenting the data in form of charts is useful in several areas. Relationship analysis uses a variety of theoretical techniques of graph theory.

Xu and Chen (2005) dealt with the analysis of visualized various types of criminal organizations. For fraud detection, but also for money laundering, it is important to find anomalies in Ditas which are in graph forms. Based on the entropy method, Shetty and Adibi (2005) identified the most important people in the Enron scandal based on email addresses. The most important are the vertices (in case of Enron, the people), whose omission from the chart results in the greatest entropy change. Noble and Cook (2003) transformed the structural anomalies in the graph to detect anomalous subgraphs. Lin and Chalupsky (2003) defined different metrics to quantify matching edges between the vertices. It is necessary to note that the most important peaks do not necessarily have to be anomalies. Social Network Analysis (Scott, Carrington 2011) is also useful for relationship analysis. It draws attention to the consistency of notaries who enter the notarial records of companies in which the same persons appear. Similarly, the fact that the same doctor confirms multiple injuries in the same person may signal a potential fraud. Network analysis is also useful for identifying a network of people involved in money laundering.

Decision making is the process of selecting one of several variants. The situations in which one of the more variants is to be chosen are the decision situations. A rational participant in this process is one who selects the best option in some ways. An indifferent participant is indifferent to the outcome of the decision. It is a random mechanism that selects variants according to the probability distribution. The situations when the outcome of the decision depends on the participants' decisions are referred to as being conflicting. It is assumed that the outcome of decision-making from the point of view of a rational participant can be evaluated by one (scalar evaluation) or multiple criteria (vector ratings). Game theory deals with decision-making situations with more rational participants with scalar rating. Conflict decision situations with one rational participant and vector valuation are dealt with by the theory of multicriteria optimization. Conflict decision situations with one or more rational participants and one indiscriminate participant with scalar rankings deal with the theory of decision being indefinite. Jones (2004) uses a game theory machine to model the behaviour of managers of companies with fraud. They studied the impact of four factors on the interaction between auditors and managers. The results indicate the relationship between testing, fraud detection and fraud prevention in the company. An audit model involving internal control is analyzed as a non-cooperative game. Matsumara and Tucker (1992) also used the theory of games to detect fraud.

Fuzzy sets and fuzzy logic are a generalization of classical double-valued logic and set theory. Instead of binary assignments, the interval is used for true values $\langle 0, 1 \rangle$. Knowledge and information are linguistically shaped. However, computers need accurate information. Fuzzy sets are useful for translating inaccurate verbal information into numerical information. The linguistic variable is a variable whose values are words or phrases of a natural or artificial language. Fuzzy sets are successfully used to express the content of a linguistic variable. The design of the function of affiliation of the fuzzy set is a fundamental problem. This is possible based on expert knowledge and also by using neural networks. Mastroleo et al. (2001) used a fuzzy expert system for detecting insurance frauds. Estévez et al. (2006) used a combination of fuzzy decisions and a neural network to prevent fraud in telecommunications. The fuzzy set and fuzzy logic apparatus are applied mainly in conjunction with neural networks.

The neural network is a massively parallel processor that has the ability to memorize knowledge gained experimentally and to further exploit this knowledge. The characteristic feature of the neural network lies in its structure formed by individual neurons linked by synaptic connections. Neural networks can be used successfully in addressing prediction and process management problems, as well as in classifying the objects. Neural networks are able to solve problems that are difficult to solve using classical algorithmic techniques. The neural network does not follow a predetermined algorithm. It is able to learn from examples and use the learned information.

The most common type of neural network is represented by multilayer perceptron (MLP). Another type of neural network used to detect fraud are the self-organizing maps (SOM). Their specificity is given by the fact that under certain conditions it allows a display that retains the typology and displays the characteristic features of the trained set of data. Neural networks are used in all situations where it is necessary to understand complex relationships between variables. Neural networks are non-linear in their design and do not need to explicitly specify the shape of the dependency function. They can also find interactive effects. The acquired knowledge is implicitly stored in the network setup vector. Neural networks based on fuzzy rules allow for improved performance of solutions. Neural networks are usually linked with an expert system into hybrid systems. Another option lies in extracting knowledge from a neural network into an expert system. Genetic algorithms are suitable for setting neural network parameters, difficult optimization problems, and machine learning with classification systems.

Neural networks based on decision trees are used in BAYES, FOIL, RIPPER and other fraud detection systems. The ASPeCT project of the European Commission, Vodaphone and other European telecommunication companies for detecting cell phone fraud also uses neural networks. Neural network technology is also used in the FALCON software suited to detect credit card fraud. Bolton and Hand (2002) gave an overview of neural network applications for detecting legalization of proceeds of crime, credit card fraud, and telecom fraud. The BRUTUS system allows for detecting fraud with mobile phones using neural networks. Ezawa and Norton (1996) also used neural networks to detect fraud based on telecommunication accounts. Stefano and Gisella (2001) developed a fuzzy expert system for the detection of insurance frauds. In order to identify a suspicious transaction and gain information it is possible to use intelligent multi-agent technology (MAT).

Literature brings many debates about the risk and several definitions. There are two interpretations - subjective probability and operationalism (both based on the same source of David Hume's empiricism). In a document on risk definition, Ngai et al. (2011) claims that two ingredients are needed for the risk - the first is the uncertainty of possible experimental results, and the second is that the results are material in nature. Financial institutions and other statutory bodies face two categories of risk: the first is the regulatory risk associated with the violation of rules on combating the legalization of criminal proceeds, and the second business risk (Parkitna et al., 2016) is that a liable entity must face the fact that unknowingly or otherwise, it can be providing services that can be associated with facilitating money laundering or terrorist financing. In addition, it is important to note that regulatory and business risks may overlap.

The risk-based approach is a systematic, continuous process of identifying and measuring the potential risk of money laundering and terrorist financing. At the same time, a strategy to mitigate these risks is emerging and being adapted, especially in the areas mostly at risk. An overview of methods used to detect money laundering based on a risk-based approach is listed by Hong et al. (2015).

4. Patent protection of procedures

Many excellent scientific results from the field of identifying unusual operations and money laundering are rather patented than published in scientific journals. Their publication would make it impossible to have them patented since their disclosure would be classified as a defect in novelty.

In some countries, computer algorithms that serve as bases for enhancing the functionality of computer software may be protected by a patent. In other countries, however, they are explicitly excluded from patentability and considered non-patentable. Software inventions may be patentable provided that the software provides a technical contribution to the state of technology. In most countries, the machine or source code of computer programs may be copyrighted. Although in some countries it is possible, or even necessary, this protection is not dependent on registration. Compared to patent protection, copyright protection is more limited because it only relates to the expression of ideas, not to thoughts themselves. Many companies protect the unit code of computer programs by copyright, while the source code is subject to business secrets.

USA, Canadian and other patent law allows the patenting of algorithms. The following examples are an example of patenting algorithms used to detect unusual business operations and in AML. An example of several patents follows:

Networked system for generating suggestions for exchanging foreign currency for credit in restricted account, has suggestion module for generating suggestion information for transaction locations and transmitting information to user device
Patent Number: US2016140555-A1
Patent Assignee: EBAY INC
Inventor(s): SCIPIONI G.

Computerized method for identifying accounts stored in database of computerized account management system, involves analyzing and assigning all accounts to per-jurisdiction buckets or default bucket, and no account is left unassigned
Patent Number: US2016104166-A1
Patent Assignee: MORGAN STANLEY
Inventor(s): COLE M; CHAN P; ENG K; et al.

RMB crown word number management system, has financial organization center for transmitting data to total center through bank intranet, and self-service equipment arranged on line type teller machine to process paper currency
Patent Number: CN104657818-A
Patent Assignee: SICHUAN JUNYI DIGITAL TECHNOLOGY DEV CO
Inventor(s): GOU J; ZENG L.

System for detecting unusual activity such as money laundering in cash vault transactions, determines dynamic threshold indicating whether change in proportion of large denomination currency transacted by customer is unusual
Patent Number: US2015142629-A1
Patent Assignee: BANK OF AMERICA CORP
Inventor(s): SUPLEE C; HUGHES C B; ZHOU J; et al.

Apparatus for generating graphical user interface for investigating e.g. illegal financial transaction of individual in financial institution, has module for generating interface that displays link to provide correlation between parties
Patent Number: US2015142627-A1
Patent Assignee: BANK OF AMERICA CORP
Inventor(s): LEE A.

Computer-implemented method for removing personally identifiable data, using fraud detection system, involves generating reverse hashing map and which explains how to restore identifiable information of set of hashed data

Patent Number: CA2860179-A1
Patent Assignee: VERAFIN INC
Inventor(s): BURKE A; CHALKER T; KING J; et al.

Laundry treating apparatus for washing laundry at home, has first communication module to receive identity (ID) information and second communication module which communicates with management server through communication network
Patent Number: US2014085046-A1 EP2711453-A1 KR2014038738-A CN103668859-A
Patent Assignee: LG ELECTRONICS INC
Inventor(s): SHIN H; KIM H; PARK M; et al.

Method for anti-money laundering surveillance to detect anomalies related to financial transactions, involves using outlier-shooting algorithm to identify outliers in peer comparison statistical data by generating peer comparison alert
Patent Number: US8544727-B1
Patent Assignee: BANK OF AMERICA CORP
Inventor(s): QUINN M R; SUDJIANTO A; RICHARDS P C; et al.

Method for detecting fraudulent data, involves identifying several reported data types for suspicion of fraud, when series of all digital distributions fails to show supposed theoretical development of digital distributions
Patent Number: US2014006468-A1 US9058285-B2
Patent Assignee: KOSSOVSKY A E
Inventor(s): KOSSOVSKY A E.

Conclusions

On the basis of literature assessment, it can be claimed that the current anti-money laundering research and work policies are primarily focused on the financial sector. Studies also highlight the need to have an international cooperation network, capacity building, enhancement of supervisory processes, and so on. However, in-depth studies of the main weaknesses are also required from a legislative and implementation point of view. It is also necessary to develop typologies and potential security measures using sophisticated mathematical and statistical methods.

References

Angiulli, F.; & Pizzuti, C. 2002. Fast outlier detection in high dimensional spaces. In: *Proceedings of the Sixth European Conference on the Principles of Data Mining and Knowledge Discovery*, 15-26, August 19-23 Springer-Verlag London, UK, ISBN 3-540-44037-2

Bay, S.; Kumaraswamy, K.; Anderle, M. G.; Kumar, R.; & Steier, D. M. 2006. Large Scale Detection of Irregularities in Accounting Data. *ICDM '06. Sixth International Conference on Data Mining*, Hong Kong, pp.75-86. Dec. 18 to Dec. 22, ISSN 1550-4786/ISBN: 0-7695-2701-9

Bell, T.B.; & Carcello, J.V. 2000. A Decision Aid for Assessing the Likelihood of Fraudulent Financial Reporting. *Auditing: A Journal of Practice and Theory*, 1: 169-184 https://doi.org/10.2308/aud.2000.19.1.169

Bolton, R.J.; & Hand, D.J. 2002. Statistical fraud detection: A review. Statistical Science, 17(3): 235-249, Published by: Institute of Mathematical Statistics https://www.jstor.org/stable/3182784

Dobrovič, J.; Gombár, M.; & Benková, E. (2017). Sustainable development activities aimed at combating tax evasion in Slovakia. *Journal of Security and Sustainability Issues*, 6(4): 761-772. https://doi.org/10.9770/jssi.2017.6.4(19)

Durtschi, C.; Hillison, W.; & Pacini, C. (2004). The Effective use of Benford´s law to assist in detecting fraud in accounting data. *Journal of Forensic Accounting*, 1524-5586(5): 17-34, © 2004 R.T. Edwards, Inc. Printed in U.S.A. https://pdfs.semanticscholar.org/1020/696451732ce203b219c19fdc31ef1ab8d8c8.pdf

Estévez, P.; Held, C.; & Perez, C. (2006). Subscription fraud prevention in telecommunications using fuzzy rules and neural networks. *Expert Systems with Applications*, 31: 337-344 https://doi.org/10.1016/eswa.2005:09.028

Ezawa, K.J.; & Norton, S.W. (1996). Constructing Bayesian networks to predict uncollectible telecommunications accounts. *IEEE Expert*, 11 (5): 45-51 https://doi.org/10.1109/64.539016

Fu, X.; Xiong, Z.; & Peng, B. (2012). A research on internet anti-money laundering technologies based on distributed smart agents. In *2012 7th International Conference on System of Systems Engineering* (SoSE). Genova, Italy, July 16-19, 2012. IEEE 2012, ISBN 978-1-4673-2974-3

Gao, Z; & Ye, M. (2007). A framework for data mining-based anti-money laundering research. *Journal of Money Laundering Control*. 10(2): 170 – 179 http://www.emeraldinsight.com/10.1108/13685200710746875

Gao, Z.; & Ye, M. (2007). *Journal of Money Laundering Control*. 10(2): 170–179. http://www.emeraldinsight.com/10.1108/13685200710746875

Grancay, M.; Grancay, N.; Drutarovska, J.; & Mura, L. (2015). Gravity model of trade of the Czech and Slovak Republics 1995-2012: How have determinants of trade changed. *Politicka Ekonomie*, 63(6): 759-777, ISSN 0032 - 3233. https://doi.org/10.18267/j.polek.1025

Hand, D.J.; & Blunt, G. (2001). Prospecting for gems in credit card data. IMA *Journal of Management Mathematics*, 12: 173-200. https://doi.org/10.1093/imaman/12.2.173

Hawkins, D.M. (1994). The feasible solution algorithm for the minimum covariance determinant estimator in multivariate data, *Journal Computational Statistics & Data Analysis*, 17(2): 197 – 210 https://doi.org/10.1016/0167-9473(92)00071-X

Hong, S. J.; & Weiss, S. M. (2001). Advances in predictive models for data mining. *Pattern Recognition Letters*, 22: 55-61 https://doi.org/10.1016/S0167-8655(00)00099-4

Hung, E.; & Cheung, D.W. (1999). Parallel Algorithm for Mining Outliers in Large Database. http://citeseer.nj.nec.com/hung99parallel.html

Jay, N. R.; & Saxena, A.K.; & Vijaya Subrahmanyam, Best, R.W. (2006). Accounting Fraud – Is it Predictable? International Review of Business Research Papers, the University of Wollongong Australia, ISSN 1832-9543

Jančíková, E.; & Veselovská, S. (2018). The new Technologies and the Fight against Money Laundering and the Terrorism Financing. In *2nd International Scientific Conference - EMAN 2018 - Economics and Management: How to Cope with Disrupted Times*, Ljubljana - Slovenia, March 22 ISBN 978-86-80194-11-0 https://doi.org/10.31410/EMAN.2018.334

Jančíková, E.; & Pásztorová, J. (2018). Strengthened EU Rules to Tackle Money Laundering and Terrorism Financing and their Implementation in Slovak Republic In Staníčková, M., L. Melecký, E. Kovářová and K. Dvoroková (eds.). *Proceedings of the 4 th International Conference on European Integration 2018*. Ostrava: VŠB - Technical University of Ostrava, 528-536. ISBN 978-80-248-4169-4/ISSN 2571-029X.

Jiang, M.F.; Tseng, S.S.; & Su C.M. (2001). Two-phase clustering algorithm for outliers detection, *Pattern Recognition Lett*. 22: 691–700 https://doi.org/10.1016/S0167-8655(00)00131-8

Jones, K. (2004). Improving Fraud Risk Assessments through Analytical Procedures. Working Paper, *Journal of Accounting Research*, 47(5) https://doi.org/10.1111/j.1475-679X.2009.00349.x

Knorr, E.; & Ng, R. (1997). A unified approach for mining outliers. In CASCON '97: Proceedings of the 1997 conference of the Centre for Advanced Studies on Collaborative research, Toronto, Ontario, Canada, KDD, 219–222

Knorr, E.; Ng R.; & Tucakov V. (2000). Distance-based outliers: Algorithms and applications. *VLDB Journal: Very Large Data Bases*, 8(3–4): 237–253 https://doi.org/110.1007/s007780050006

Knorr, E.M.; & Ng R.T. (1999). Finding intentional knowledge of distance-based outliers. In: *Proceedings of the 25th VLDB International Conference on Very Large Data Bases*, pp. 211-222, Morgan Kaufmann Publishers Inc. San Francisco, CA, USA ISBN: 1-55860-615-7

Korauš, A.; & Kelemen P. (2018). Protection of persons and property in terms of cybersecurity in Economic, *Political and Legal Issues of International Relations 2018. Faculty of International Relations of Univerzity of Economics in Bratislava*, 1-2. Juni 2018, Virt, Editor: EKONÓM, 2018, ISBN 978-80-225-4506-8/ISSN 2585-9404

Limba, T.; & Šidlauskas, A. (2018). Secure personal data administration in the social networks: the case of voluntary sharing of personal data on the Facebook. *Entrepreneurship and Sustainability Issues* 5(3): 528-541. https://doi.org/10.9770/jesi.2018.5.3(9)

Kosinski, A. S. (1999). A procedure for the detection of multivariate outliers. *Computational Statistics and Data Analysis*, 29(2): 145-161, https://doi.org/10.1016/S0167-9473(98)00073-5

Lin, S.; & Chalupsky, H. (2003). Unsupervised Link Discovery in Multi-relational Data via Rarity Analysis. *Proceedings of the Third IEEE ICDM International Conference on Data Mining*, pp. 171-178, November 19 – 22, IEEE Computer Society Washington, DC, USA, ISBN:0-7695-1978-4

Mamojka, M.; & Müllerová, J. (2016). New methodology for crisis management RM/RA CRAMM and its legal frame. In: Production management and engineering sciences. - Leiden: CRC Press/Balkema, 2016. pp 185-190. ISBN 978-1-138-02856-2.

Mastroleo, G. Facchinetti, G. & Magni, C. A. (2001). A proposal for modeling real options through fuzzy expert system. Proceeding SAC '01 Proceedings of the 2001 ACM symposium on Applied computing, pp. 479-481, Las Vegas, Nevada, USA, ISBN 1-58113-287-5. https://doi.org/10.1145/372202.372422

Matsumara, E.M.; &Tucker, R.R. (1992). Fraud Detection: A Theoretical Foundation. *The Accounting Review*, 67(4): 753-782.

Müllerová, J. 2016. *RM/RA CRAMM as a new risk management method for prevention of ecology disasters*, 16th International Multidisciplinary Scientific GeoConference SGEM 2016, SGEM2016 Conference Proceedings, June 28 - July 6, Book 5(1): 607-612. ISBN 978-619-7105-65-0/ISSN 1314-2704

Müllerová, J.; & Mamojka, M. 2017. Legal possibilities of the rescue forces during the emergency event. In: SGEM2017 Conference Proceedings, 29 June-5 July, 17(51): 605-612. ISBN 978-619-7408-08-9/ISSN 1314-2704. https://doi.org/10.5593/sgem2017/51/S20.079

Mura, L.; Daňová, M.; Vavrek, R.; & Dúbravská, M. (2017). Economic freedom – classification of its level and impact on the economic security. *AD ALTA, Journal of Interdisciplinary Research*, 7 (2): 154 – 157 ISSN/ISBN

Mura, L.; Marchevska, M.; & Dubravska, M. (2018). Slovak Retail Business across Panel Regression Model. *Marketing and Management of Innovations*, 4: 203-211. http://doi.org/10.21272/mmi.2018.4-18

Nigrini, J.M.; & Mittermaier, L. I. (1997). The Use of Benford's Law as an Aid in Analytical Procedures, Auditing. *A Journal of Practice and Theory* 16 (Fall)

Nigrini, M. J. (1999). I've got your number. *Journal of Accountancy*, 79–83, https://www.journalofaccountancy.com/issues/1999/may/nigrini.html

Ngai, E. W. T.; Hu, Y.; Wong Y. H.; Chen Y.; & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, 50(3): 559-569 http://doi.org/10.1016/j.dss.2010.08.006

Noble, C.; & Cook, D. (2003). Graph-based Anomaly Detection. *Proceedings of the ACM Conference on Knowledge Discovery and Data Mining*, pp. 631-636, Washington, D.C. ISBN 1-58113-737-0. http://doi.org/10.1145/956750.956831

Pálková, M.; Müllerová, J.; Endrizalová E. (2018). Risk management system in Czech Republic. In: SGEM 2018 conference proceedings. 30 June - 9 July 2018 Albena, Bulgaria [print]. Sofia: STEF92 Technology 18(5.2), pp. 1049-1056. ISSN 1314-2704/ISBN 978-619-7408-47-8.

Pálková M.; Müllerová J.; Novák M.; & Němec V. (2018). Risk and uncertainty assessment of natural disasters. In: SGEM 2018 conference proceedings, 30 June - 9 July 2018 Albena, Bulgaria, Sofia: STEF92 Technology 18 (5.2): pp. 1057-1064. ISSN1314-2704/ISBN 978-619-7408-47-8.

Parkitna, A.; Kamińska, A.; & Pędziwiatr, A. (2016). The impact of external economic factors on the level of the enterprises' efficiency in Poland in the context of business risk. *Acta Oeconomica Universitatis Selye* 5 (2): 144 – 158, ISSN 1338-6581

Phua C.; Lee V.; Smith K.; & Gayler R. (2005). *A comprehensive survey of data mining - based fraud detection research*. http://www.bsys.monash.edu.au/people/cphua/

Ramaswamy, S.; Rastogi, R.; & Shim, K. (2000). Efficient algorithms for mining outliers from large data sets. In: *Proceedings of the ACMSIGMOD Conference*, pp. 427-438, Dallas, Texas, USA — May 15 – 18. ISBN 1-58113-217-4 http://doi.org/10.1145/342009.335437

Rohit, K. D.; & Patel, D. B. (2015). Review on Detection of Suspicious Transaction in Anti-Money Laundering Using Data Mining Framework. *International Journal for Innovative Research in Science and Technology*, 1(8): 129-133, ISSN (online): 2349 – 6010 https://pdfs.semanticscholar.org/23a2/3da2dc5956297cc86c8f0f4c58a5e05f0070.pdf

Scott, J.; Carrington, P.J. (2011). The SAGE Handbook of Social Network Analysis, Sage Publications Ltd. ISBN 1847873952 9781847873958

Senator, T. E.; Goldberg, H. G.; Wooton, J.; Cottini, M. A.; Khan, A. U.; Klinger, C. D.; & Wong, R. W. (1995). Financial Crimes Enforcement Network AI System (FAIS) Identifying Potential Money Laundering from Reports of Large Cash Transactions. *AI magazine*, 16(4): 21. From: IAAI-95 Proceedings. Copyright © 1995, AAAI (www.aaai.org) https://www.aaai.org/Papers/IAAI/1995/IAAI95-015.pdf

Shapiro, A. F. (2002). The merging of neural networks, fuzzy logic, and genetic algorithms. *Insurance: Mathematics and Economics*, 31: 115–131 https://doi.org/10.1016/S0167-6687(02)00124-5

Shetty, J.; & Adibi, J. (2005). Discovering Important Nodes through Graph Entropy: The Case of Enron Email Database. KDD, *Proceedings of the 3rd international workshop on Link discovery*, pp. 74-81, Chicago, ISBN 1-59593-215-1 https://doi.org/10.1145/1134271.1134282

Schneider, F. (2007). Money Laundering: Some Preliminary Empirical Findings. *Conference Tackling Money Laundering* http://www.awi.uni-Heidelberg.de/with2/seminar/WS%200708/Schneider_Money%20 Laundering_102007.doc

Sohn, S. Y.; Moon T. H.; & Kim, S. (2005). Improved technology scoring model for credit guarantee fund. In Journal Expert Systems with Applications. *An International Journal*, 28(2): 327-331. https://doi.org/10.1016/j.eswa.2004.10.012

Spathis, C.T. (2002). Detecting false financial statements using published data: some evidence from Greece, *Managerial Auditing Journal*, 17(4): 179-191, https://doi.org/10.1108/02686900210424321

Straková, J.; Pártlová, P.; & Váchal, J. (2017). Business management in new global economy. *Acta Oeconomica Universitatis Selye* 6 (1): 155 – 166. ISSN 1338-6581

Sudjianto A.; Nair S.; Yuan M.; Zhang A.; Kern D.; & Cela-Díaz F. (2010). Statistical methods for fighting financial crimes. *Technometrics* 52(1): 5-19. https://doi.org/10.1198/TECH.2010.07032

Šišulák, S. (2017). Userfocus - tool for criminality control of social networks at both the local and international level. *Entrepreneurship and Sustainability Issues* 5(2): 297-314. https://doi.org/10.9770/jesi.2017.5.2(10)

Taniguchi, M.; Haft M.; Hollmen J.; & Tresp V. (1998). Fraud detection in communication networks using neural and probabilistic methods. In Proceedings of the 1998 IEEE International Conference in Acoustics, Speech and Signal Processing, 2: 1241–1244. https://doi.org/10.1109/ICASSP.1998.675496

Walker, J. (1998). *Modelling Global Money Laundering Flows – some findings*. http://members.ozemail.com.au/~john.walker/crimetrendsanalysis/mlmethod.htm

Weatherford, M. (2002). Mining for fraud. *IEEE Intelligent Systems*, 17: 4-6. https://doi.org/10.1109/ MIS.2002.1024744

Veselovská, S.; Korauš, A.; & Polák, J. (2018). Money Laundering and Legalization of Proceeds of Criminal Activity, *Second International Scientific Conference on Economics and Management - EMAN 2018*, March 22, Ljubljana, Slovenia, Printed by: All in One Print Center, Belgrade, 2018, ISBN 978-86-80194-11-0 https://doi.org/10.31410/EMAN.2018

Williams G.; & Huang Z. (1997). Mining the knowledge mine: The hot spots methodology for mining large real world databases. In *Abdul Sattar, editor, Advanced Topics in Artificial Intelligence*, pp. 340–348, November 30 - December 04, Springer-Verlag London, UK, ISBN 3-540-63797-4

Xu, J; & Chen, H. (2005). Criminal network analysis and visualization. *Communications of the ACM*, 48(6): 101-108 https://doi.org/10.1145/1064830.1064834

Yamanishi, K.; Takeuchi, J.; Williams, G. & Milne, P. (2000). On-line unsupervised outlier detection using -nite mixtures with discounting learning algorithms. *Proceedings of the 6th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 320–324, Boston, Massachusetts, USA, ISBN 1-58113-233-6 https://doi.org/10.1145/347090.347160

Yang Y., Lian B., Li L., Chen C., & Li P. (2014). DBSCAN clustering algorithm applied to identify suspicious financial transactions. In *Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), International Conference*, 60-65, ISBN 978-1-4799-6236-5. https://doi.org/10.1109/CyberC.2014.89

York, D. (2000). Auditing technique – Benford´s law. *Accountancy*, 1283: 126

Zhang, T.; Ramakrishnan, R.; & Livny, M. (1996). An efficient data clustering method for very large databases. In *Proc. ACM SIGMOD*, pp. 103–114, Montreal, Quebec, Canada, ISBN 0-89791-794-4 https://doi.org/10.1145/233269.233324

Zhu, T. (2006). An outlier detection model based on cross datasets comparison for financial surveillance. In *2006 IEEE Asia-Pacific Conference on Services Computing (APSCC'06)*, pp. 601-604, ISBN 0-7695-2751-5 https://doi.org/10.1109/APSCC.2006.33

Short biographical note about the contributors at the end of the article (name, surname, academic title and scientific degree, duties, research interests):

Ass.prof.Ing. Antonín KORAUŠ, PhD., LL.M., MBA is an associate professor at Academy of the Police Force in Bratislava, Slovak republic. Research interests: economy security, finance security, cyber security, energy security, finance, banking, management, AML, economy frauds, financial frauds, marketing, sustainability.
ORCID ID: https://orcid.org/0000-0003-2384-9106

Ass. Prof. Ing. Miroslav GOMBÁR, PhD. is an associate professor in the Department of Management, Faculty of Management at the University of Prešov in Prešov since 2016. Since 2016, he works as head of the Department of Management, and he teaches school subjects: statistics, management, operations management, and logistics.
ORCID ID: https://orcid.org/0000-0002-8383-7820

Mgr. Pavel KELEMEN, Ph. D. Candidate at the Faculty of Management at the University of Prešov in Prešov, Slovak Republic
ORCID ID: https://orcid.org/0000-0001-7563-3142

JUDr.Stanislav BACKA, Ph. D. Candidate at the Faculty of Management at the University of Prešov in Prešov, Slovak Republic
ORCID ID: https://orcid.org/0000-0002-0411-4158