Available online at www.sciencedirect.com

ScienceDirect

Procedia Economics and Finance 32 (2015) 1827 – 1836

Procedia Economics and Finance

www.elsevier.com/locate/procedia

Emerging Markets Queries in Finance and Business

Detecting and Preventing Fraud with Data Analytics

Adrian Bănărescu[a,b,*]

[a]*Institutul de Economie Nationala, Calea 13 Septembrie nr.13, Bucharest 050711, Romania*
[b]*Agenţia Naţională de Administrare Fiscală, Splaiul Independenţei, 202A, sector 6, Bucharest 060022, Romania*

Abstract

Although fraud is not a new issue, the current financial crisis has enlightened that fraud occurs mainly during a recession, as compared with normal periods of economic growth. In counterbalance to the slow economic recovery, managers need to start a series of antifraud measures, as a leverage of cost control, while reducing available resources. Fraud involves inclusively significant financial risks which may threaten profitability, and the image of an economic entity. In these circumstances, in which development of the IT systems plays a central role in the creation of competitive companies, the amount of processed data has grown exponentially. Internal control team members should need to look at every transaction that takes place, but, unfortunately this issue can no longer be manually performed, requiring the use of data analysis tools and programs. Since the companies usually operate with large volumes of data, it is absolutely necessary to implement such processes of continuous monitoring, in order to identify anomalies in the data stream or behavioral patterns, potentially fraudulent. Such new and significant information will be later used in directing investigations, as well as to make recommendations to improve the control activities. We strive to provide an overview of the way in which technology can be implemented to improve fraud prevention and detection, inside of a public or private economic entity.

Selection and peer-review under responsibility of Asociatia Grupul Roman de Cercetari in Finante Corporatiste

Keywords: data analytics; preventing fraud; IT systems.

* Corresponding author. Tel.: +40-721-335-620.
E-mail address: rescuadrian@yahoo.com.

Selection and peer-review under responsibility of Asociatia Grupul Roman de Cercetari in Finante Corporatiste
doi:10.1016/S2212-5671(15)01485-9

1. Introduction

Economic and financial crisis, which began in 2008 with the bankruptcy of Lehman Brothers in the USA, unlike previous crises, has had a very rapid nationally and internationally spread, so that, in 2009 it established its systemic nature, most countries being affected directly or indirectly by a strong recessionary phenomena, imbalances and turbulence in real and nominal economy.

This has affected the industrialized world by lack of credit and falling property prices. Slowing economic growth of developed countries produced effects on emerging economies, major EU trading partners, with negative effects on exports. No doubt, the economic downturn will be felt by modern societies for years to come. As you could easily find, these manifested differently from state to state, depending on the features related to their debt exposure to the so-called "real estate boom", the ability to innovate and compete, resistance to fraud.

In this context, economic crime and fraud remains an intractable problem for global companies. According to 2014 ACFE report, organizations lose 5% of revenues each year to fraud. If applied to the 2013 estimated Gross World Product, this translates to a potential projected global fraud loss of nearly $3.7 trillion. Also, the median duration (the amount of time from when the fraud commenced until it was detected) for the fraud cases reported to us was 18 months. We believe that fraud mechanisms are more important than ever, being a key tool for maintaining productivity growth conditions and sustained economic growth.

2. The current state of implementing data analysis software for preventing and detecting fraud

In the last few years, we have been witnessing a massive increase in the quantity of data (text, pictures, audio, video etc.), both at global and economic level entities. This process is amplified by the entry of any entity mentioned above into the virtual environment. Data comes from everywhere, from numerous and diverse sources like contracts, customer interactions, call centers, social media, phones, emails, faxes, and others. The trend is to use these data for the interest of the entity (conceiving strategies, opportunities identification, goodwill development, preventing and detecting fraud etc.).

The use of data analysis processes and the software dedicated to these operations provide extensive and in-depth analysis of the phenomena and processes of the informal economy, fraud and corruption, as the information and communication technology becomes a sine qua non instrument of registered (formal) economy. Although on the analytical market, there is a wide spectrum of specialized tools capable to support and enhance the antifraud activity, unfortunately, the survey results indicate that managers are not taking advantage of them.

Forensic data analytics (FDA) tools are currently in use in the organizations, but there is much lower adoption of more sophisticated FDA tools as depicted in Table 1. 65% of survey participants report the use of spreadsheet tools such as Microsoft Excel and 43% report the use of database tools such as MS Access or MS SQL Server. While these tools are important to every FDA program, they often focus on the matching, grouping, ordering, joining or filtering of data that is primarily descriptive in nature.

Table. 1. Forensic data analytics tools use in the organizations

Forensic data	Percent
Spreadsheet tools such as Microsoft Excel	65%
Database tools such as Microsoft Access or Microsoft SQL Server	43%
Continuous monitoring tools, which may include governance risk and compliance (GRC) tools (SAP, SAI Global, Oracle)	29%
Text analytics tools or keyword searching	26%
Forensic analytics software (ACL, iDEA)	26%
Social media/web monitoring tools	21%
Visualization and reporting tools (Tableau, Spotfire, QlikView)	12%
Statistical analysis and data-mining packages (SPSS, SAS, R, Stata)	11%
Big data technologies (Hadoop, Map Reduce)	2%
Voice searching and analysis (Nexidia, NICE)	2%

Source:http://www.ey.com/Publication/vwLUAssets/EY-Global-Forensic-Data-Analytics-Survey-2014/$FILE/EY-Global-Forensic-Data-Analytics-Survey-2014.pdf

According to the conclusion of the 2014 ACFE report, it should be noted that the authors identify the proactive data monitoring/analysis as one of the most effective tool for antifraud control, in helping reduce fraud losses and fraud scheme duration. Therefore, 34,8% of organizations affected by fraud used proactive data monitoring/analysis as a control tool; organizations using proactive data monitoring/analysis faced with a near 59,7% reduction in median loss compared to those that did not; organizations using proactive data monitoring/analysis experienced a 50% reduction in median duration of fraud scheme compared to those that did not. The main barriers of implementing an analytical system are presented below in Table. 2.

Table 2. The greatest barrier in leveraging data analytics/CAATs when performing audit activities

Forensic data	Percent				
The requisite skills and knowledge do not currently reside within the internal audit department.	34%	21%	18%	14%	12%
Lack of access to data analytics/CAATs tools	20%	23%	21%	23%	13%
Lack of audit methodology and approach supporting the use of data analytics/CAATs	12%	28%	35%	19%	6%
Use of data analytics/CAATs is not perceived as a means to increase the efficiency of conducting audit activities.	13%	18%	19%	34%	15%
Other	44%	10%	9%	5%	32%

Source: PricewaterhouseCoopers (2010) State of the internal audit profession study

By authors of 2012 AuditNet survey, among the relative important factors, regarding decisions on integrating data analysis in the audit process, data quality was the most important factor, and the fraud detection situated at the fifth level from thirteen.

Table 3. The relative importance of factors, regarding decisions on integrating data analysis in the audit process

Answer Options	Extremely Important	Important	Not Very Important	Not at all Important	Rating Average	Response Count
Software cost	54	102	26	5	3,10	190
Technology capabilities of our staff	47	124	16	3	3,13	192
Training availability	42	125	20	2	3,10	191

Training costs	50	114	20	5	3,11	191
Staff retention	46	94	37	9	2,95	191
Making the audit process more efficient	95	82	10	1	3,44	190
Finding fraud	72	91	23	2	3,24	189
Audit Committee (Board support	36	71	56	10	2,77	190
Senior Management support	64	73	41	9	3,03	191
CAE support	79	71	16	4	3,32	188
Requires adjusting our audit work programs	19	83	71	13	2,58	192
Getting access to the data	91	88	11	0	3,42	191
Data quality and reliability	11	66	11	0	3,53	190

1

Source: AuditNet 2012 Survey Report on Data Analysis Audit Software

In our opinion, there are all prerequisites for the data analysis to have a great potential for changing the way that fraud detection is done. The use of analytical instruments may be deducted from specific indicators, like:

- the raise of fields based solely on data/information/intangible assets (a direct consequence of the ageing process of knowledge society);
- new categories of analyst profession (intelligence analyst according to 2012 Classification of Occupations in Romania);
- crystallization of diverse markets which offer software tools for data analysis (a direct consequence of the objective laws of supply and demand);
- strategic acquisitions made by market giants in the field (I2 acquisition by IBM Corporation).

3. Possible solutions to improve data analysis processes for preventing and detecting fraud

Data analysis can be described as in-depth examination of the meaning and essential features of available data, in order to identify significant information, using specific methods and techniques. It's an interdisciplinary domain which includes branches such as science computers (computer science), mathematical sciences, statistical, economic, psychology, law and other cognitive sciences.

This careful examination of data identifies data gaps, strengths, weaknesses, dysfunction, vulnerabilities and risk factors that may constitute threats and finally suggests guiding lines. Although on the field there are several concepts of data analysis such as intelligence analysis, business analysis etc., they all have common components. The differences depend on the scope, nature of the data, analytical products, practical utility and applicability.

According to specialized literature, related to data analysis as system for prevention and detection of fraud, can be identified over 24 types of analysis, some of them extremely complex, but among all of them, we can identify two classical types of analysis: operational analysis and strategic analysis. The basic concepts of data analysis are emphasized in the table below:

Table 4. Basic concepts of data analysis

Methods	Strategic analysis	Operational analysis
Techniques	Risk analysis, Results analysis, Phenomenon analysis, Situational picture analysis, statistical analysis, SWOT Analysis PESTEL Analysis, Scenarios technique	Case analysis, Comparative case analysis Links analysis, Flow analysis, Event analysis Analysis of activities, Financial Analysis, Analysis phones, Risk analysis, SWOT Analysis, Profile Suspect Analysis, Geospatial Analysis, Technology scenarios etc.
Procedures	Graphical representation (histograms, relation maps, flow maps, maps of activities, of events, geospatial maps), Space viewing, Three dimensional Viewing etc.	
Instruments	Mathematics, Statistics, Office Excel, Access, SAS, iDEA, GeoMedia Professional, GPS, Map, ANB, iBase, Palantir, paper, pencil, etc.	

Source: Cofan S. M. et al., 2014

Operational analysis can be successfully used on short term, by exploiting data and current information for the purposes to comply with the current activities for detection of fraud with maximum efficiency. Data analysis, in operational form, becomes a tool for improving workplace conditions, most manual activities are avoided, reduced mental effort, especially for operations involving the processing of a significant amount of data. In daily activities, the main role of operational analysis is to help antifraud manager to detect and combat illegal activities, by examining (i) links between suspects, (ii) their characteristics (direct or/and indirect subordination relations, positions in the hierarchy of the group, key positions that impact decision-making etc.), (iii) the movement of goods, money or other valuables, (iv) way of communication (email, social networking), (v) sequence of certain events, (vi) modus operandi etc. The success of such approach lies in the quality and variety of data sources.

One of the purposes of using processes analysis of the data, in the context of the operational analysis, is to complete the information gaps or to remove uncertainties and contradictions. Finally, the analytically product must be submitted in a clear and concise form, containing at least one mode of illegal operation or a worthy presumption of fraud Unlike operational analysis, the strategic analysis involves a macro-level approach of preventing and detecting fraud issues. Considering that analytical tools are much more diverse, in case of strategic analysis the amplitude of the activities is exacerbated. In this context will be studied threats, vulnerabilities, risks, trends of evolution of fraud phenomena, the evolution of the market, demographic aspects of fiscal policy, economic development or decline of the entities. It will scan both internal environment, with vulnerabilities and institutional capacities and the external context with opportunities and potential threats.

The analyst will work with large volumes of data, it will use statistics, will describe phenomena and will formulate explanations and predictions, in order to substantiate decisions for the highest level management. Metaphorically speaking, research analyst shall look at the relevant object like “a hawk from the sky”, able to distinguish rather color spots than the details (Cofan et al, 2014), (Comes, 2013). The strategic analysis offers a macro overview related to fraud. Analytic tools represents piece of software which improve methods or multiply their effects. If utilizing digital statistical tools, whether or not you have training in statistics, you can identify, for example, unusual variation by looking to the shape of a curve.

The actual statistical tools have a highly intuitive interface and a powerful statistical processing engine. For a long time, analysis techniques, such as statistics and exploration of data, were developed independently of the visual techniques. With the new generation of visualization software, we can dive into massive data sets and visually find new trends, patterns and threats that would take hours or days using conventional data mining (Bresfelean et all, 2008).

Data mining, as an analytic process, is designed to explore data, to extract information from data sets, in order to discover patterns and relations. It can be defined as “the nontrivial extraction of implicit, previously unknown, and potentially useful information from data” (Frawley et al., 1992, Bresfelean et al, 2007), or “the science of extracting useful information from large data sets or databases” (Hand and Mannila, 2001). Analysis of the data-text, known under the name of exploitation of data such as text or "text mining", refers to the process of knowledge extraction from documents, because information can be mostly found in text format. Occurrence of this form of analysis is associated with the moment when classical research methods became inefficient. The indexing methods surpassed the issue mentioned above, the search algorithms contained rules in order to accomplish a variety of analytic tasks, as categorizing documents, creating summaries, detecting relevance between documents etc. Text data mining is considered to be one of the most important area in the database system, which provides one of the most interesting and promising development in informatics industry (Crețulescu, 2011). Some authors (Ah-Hwee Tan, 2012) identifies and summarizes the capabilities of 11 (eleven) text data mining products, organized in two clusters. First cluster of products optimizes activities of organization, viewing and navigation within documents, and the second one provides functions for text analysis, in particular, the extraction, classification and summarization of information.

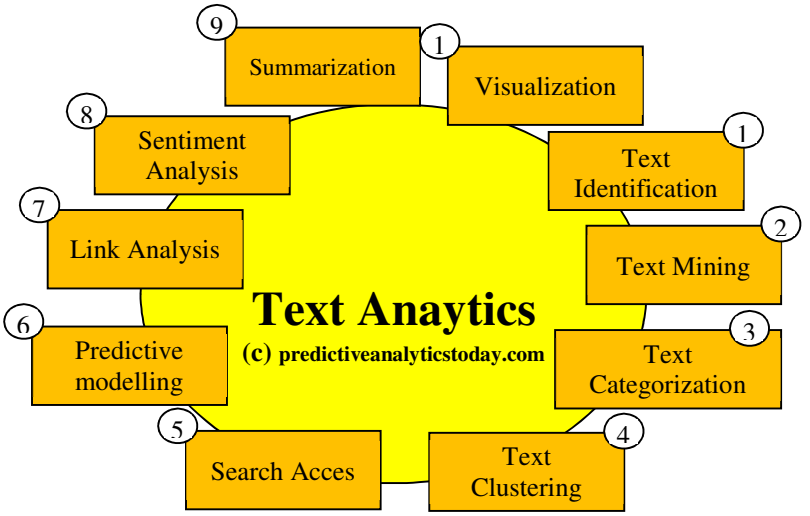

Fig. 1. Text analytics process flow

Geospatial analysis - visual analysis is also important for understanding the relevance of the location where events happened, to determine and discover patterns in fraud behavior. Analytical instruments allow identification, exploration, indexing and processing data. The biggest challenge remains implementation of automatic methods and tools. It is absolutely necessary to analyze possibilities for expansion and integration of the new models and computerized systems to prevent and detect fraudulent actions and to support wittingly managerial decisions. Successful implementation of an antifraud analytical system highly depends on the manner of retrieving data from a variety of sources, considering that most of them have different formats. It is recommended that the data collected should be interpreted in the same way, using the same techniques and the same methodology, so that creation of data bases to be homogeneous. Although a system of fraud prevention and detection could be expensive, the low degree of response to fraud and the inability to recover losses resulting from internal fraud or abuse could have multiple consequences, difficult to quantify. The actual fraud prevention and detection mechanism combines both human and technical factors. No matter how sophisticated technical

solutions may be, human factor still dictates the action mode as well as the exploitation of results. Introduction of a computerized system of control would eliminate the problem of inefficiency of control levels, referred to at points 1, 2 and 3 in Figure no. 2 below. These levels are associated with the unforeseen or repetitive inspection of work, specific to the control activity and are characterized by a low percentage of early detection of fraud. Through the leverage of automated controls and monitoring tools (level 5), it can be mitigated potential risks to misconduct and fraud.

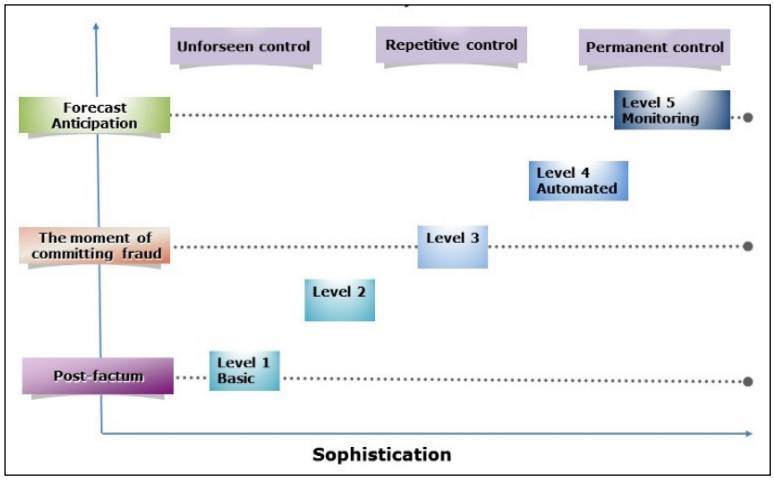

Fig.2. The efficiency of control levels
Source: adaptation of model http://www.acl.com/pdfs/White_Paper_AACM.pdf

Last but not least, integration of data analysis processes within the fraud detection system is an imperative arising from scientific and technological development of allover companies, accompanied by a series of benefits and limitations as follows.

(a) Benefits:

- get answers, in real time, to a series of questions regarding fraud issues;
- automatic data collection (predetermined flow);
- total and fast access to all data, through data indexing software (way of sorting a number of records on multiple fields.);
- eliminates double records, errors, improving quality of data;
- high productivity vs. manual work;
- operating with incomplete and inaccurate data;
- generating a positive yield and fast return on investment;
- an increased rate for fraud detection;
- fast detection and recovery of consequences of fraud activity;
- creation of statistical analysis with high degree of accuracy;
- reducing fraudulent claims;
- increase the quality of analytical products.

(b) Limitations:

- like the other labor saving tools, fraud prevention and detection software do not come cheap;
- large part of data are not introduced in databases, not all text files being included in the final reports;
- the utilization of analytical tools don’t save time, just optimize it. The time gain like this, is used for further research/analysis;

- regardless of the software complexity, a human resource is always needed;
- efficient antifraud system involves high costs, so, many of economic entities prefer to create only classical control structures;
- anti-fraud activities, based on software and hardware solutions, are recommended to be carried out and coordinated by a group of specialists, with different experience, in order to cover various fields of activity;
- the absence of audit programs is a vulnerability and for safety reasons, the access to information must be controlled in both ways, in-and-out;
- Due to the complexity of analytical research, the final product can be hard to assimilate, so, it's recommended to use descriptive part (interpretation of tables, graphs, values, metadata etc.).

4. Conclusion

Our intention is to encourage antifraud managers to use proactive data detection techniques in order to improve fraud prevention and detection. There is not a toolkit which you can start a business fraud detection, is not recommended to spend too much time selecting the perfect option. Just get started fighting fraud, use free and payable software, a combination of statistical, data visualization, data mining, and filtering tools. The processes of data analysis as a tool for preventing and detecting fraud can be used successfully in any field, mainly in those of the database and the data are or may be easily converted into electronic format. For the fiscal, banking, insurance and medical fraud existence of a structure is a sine qua non for the survival of business in the current exacerbation of fraud, financial constraints and fierce competition. Although the software are not cheap, as we have previously mentioned above, there is the possibility to maximize the benefits offered by the Office package (Excel, Access) or ActiveData for Excel/Office. Creating a system to detect and prevent fraud involves certain steps, which can be done gradually, depending on the priorities and the complexity of the system, as further presented related to hardware components:

- define the intention of preventing and detecting fraud;
- create a special entity for this purpose;
- create an it infrastructure able to transpose the internal and external data into the virtual domain;
- ensuring a flow of creating and storage of data in electronic format;
- implementation of a monitoring system data to allow, where possible, real-time detection of irregularities so as to avoid damage. The system should contain a number of templates (predefined models) built for detecting fraud schemes. As architecture, it is recommended to be partially predefined, so as some modules can be customize for the customer's needs;
- creating a recovery system;
- develop an integrated data analysis (a nucleus together with the most detection methods: statistical, relational etc.);
- creating a system able to generate intermediary and final reports, depending on the requirements of the recipient.

Acknowledgements

This paper has been financially supported within the project entitled „SOCERT. Knowledge society, dynamism through research", contract number POSDRU/159/1.5/S/132406. This project is co-financed by European Social Fund through Sectoral Operational Programme for Human Resources Development 2007-2013. Investing in people!

References

ACL 2014, Fraud Detection Using Data Analytics in the Banking Industry. Discussion whitepaper.

Alexandru, D., I, 2010. Manual de Inteligența Afacerilor, ISBN-13: 978-1446694251.

Argyriou, E.N.,Symvonis, A. 2012, Detecting periodicity in serial data through visualization. Advances in Visual Computing, vol. 7432, pp. 295-304.

Association of Certified Fraud Examiners. 2014. Report to the Nation on Occupational Fraud and Abuse,

AuditNet 2012 Survey Report on Data Analysis Audit Software.

Bresfelean, Vasile Paul, Mihaela Bresfelean, Nicolae Ghisoiu, and Calin-Adrian Comes. 2007. "Data Mining Clustering Techniques in Academia." In ICEIS (2), pp. 407-410.

Bresfelean, V. P., Bresfelean, M., Ghisoiu, N., & Comes, C. A. 2008. Determining students' academic failure profile founded on data mining methods. In Information Technology Interfaces, IEEE, pp. 317-322.

Burge, P., Shawe-Taylor, J. 2001, An Unsupervised Neural, Network Approach to Profiling the Behaviour of Mobile Phone, Users for Use in Fraud Detection. Journal of Parallel and Distributed Computing 61: 915–925.

Chersan, I.C., Carp, M., Mironiuc, M., 2013, Data mining – o provocare pentru auditorii financiari, revista Audit Financiar, anul XI, nr. 106, 10/2013, pag. 57- 64.

Cofan S.M., Ivan, L., Dogaru V., Cios A., Savin M. 2014. Analiza Informațiilor. Manual, ed. Ministerului Afacerilor Interne, ISBN 978-973-745-129-3.

Comes, C.A. 2013. Stored Procedure Migration In ERP Systems, LAP Lambert Academic Publishing, Saarbrucken, Germany.

Comes C.A, Bresfelean V. P., 2013, Social Networking Analysis of ReCADD with Petri Nets, Cambridge Scholars Publishing, Newcastle upon Tyne, UK, pp. 25-33.

Cox, K., Eick, S., Wills, G. 1997. Visual Data Mining: Recognizing Telephone Calling Fraud. Data Mining and Knowledge Discovery 1: 225–231.

Cretulescu, R. G., 2011, Contributions to the design of classification systems of the documents. Legislation, Sibiu.

D.Hand, H. Mannila, P. Smyth: Principles of Data Mining. MIT Press, 2001

Frawley W., Piatetsky-Shapiro, G., Matheus, C., 1992, Knowledge Discovery in Databases: An Overview. AI Magazine, p. 213-228

Global fraud study, 2012, Report to the nations on occupational fraud and abuse

Green, B., Choi, J. 1997, Assessing the Risk of Management Fraud through Neural Network Technology. Auditing 161: 14–28.

http://aitfis.com/image/AIT_1811ArticleWeb.pdf

http://linkanalysisnow.com/2010/11/using-visual-analysis-to-detect-fraud.html

http://www.acfe.com/rttn/docs/2014-report-to-nations.pdf.

http://www.acl.com/pdfs/DP_Fraud_detection_BANKING.pdf.

http://www.auditnet.org/publications--2/auditnet-surveys

http://www.ey.com/Publication/vwLUAssets/EY-Global-Forensic-Data-Analytics-Survey-2014/$FILE/EY-Global-Forensic-Data-Analytics-Survey-2014.pdf.

http://www.tide.org.tr/uploads/DetectingFraudBook.pdf.

http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=SA&subtype=WH&htmlfid=YTW03084USEN

IBM, Step-by-step data mining guide,

Kent, K., Chevalier, S., Grance, T., Dang H. 2006, Guide to Integrating Forensic Techniques into Incident Response, http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.

Lanza, R.B. 2003, Proactively Detecting Occupational Fraud Using Computer Audit Reports,

Mantone, P. S 2013, Using Analytics to Detect Possible Fraud: Tools and Techniques, ISBN-13: 978-1118585627

McMahon, R.J. 2001, Practical Handbook for Private Investigators, CRC Press LLC, ISBN 0-8493-0290-0.

Michalski, R. S., Bratko, I., Kubat, M. 1998. Machine Learning and Data Mining – Methods and Applications. John Wiley & Sons Ltd.

Millar, P. 2009, Detecting and Preventing Fraud with Data Analytics. http://www.acl.com/pdfs/eBook_fraud.pdf

Murad, U., Pinkas, G. 1999, Unsupervised Profiling for Identifying Superimposed Fraud. Proceedings of PKDD'99.

Nelson, J. Chen. 2011, Beyond the Next Generation Technology for Financial Crimes and Asset Forfeiture Investigations. The Eighteen Eleven: Professional Journal of the Federal Law Enforcement Officer Association, no. 1, pp. 6-7,

Nigrini, M. 2011, Forensic Analytics: Methods and Techniques for Forensic Accounting Investigations. Hoboken, NJ: John Wiley & Sons Inc. ISBN 978-0-470-89046-2.

Nițu, I., 2012, Analiza de intelligence. O abordare din perspectiva teoriilor schimbării, Editura Rao, ISBN: 978-606-609-373-6.

Oppel, A. 2011, Modelarea datelor. Ghidul începătorului, Editura: Rosetti Educațional,

Palshikar, G.K., 2002, The Hidden Truth – Frauds and Their Control: A Critical Application for Business Intelligence, Intelligent Enterprise, vol. 5, no. 9, pp. 46–51.

Phua, C., Lee, V., Smith-Miles, K. and Gayler, R. 2005, A Comprehensive Survey of Data Mining-based Fraud Detection Research. Clayton School of Information Technology, Monash University.

PricewaterhouseCoopers LLP 2009. "2009 Global Economic Crime Survey". Retrieved June 29, 2011.

Robu, I.B., Robu, M.A., 2013, Proceduri de audit pentru estimarea riscului de fraudă bazate pe indici de detectare a manipulărilor contabile, revista Audit Financiar, anul XI, nr. 106, 10/2013, pag. 3-16.

Smith, S., Mueller, J. 2012, Data Analysis Challenges: Try Proven Strategies for More Success. Association of Healthcare Internal Auditors. https://www.audimation.com/pdfs/ahia-data-analysis-challenges.pdf.

Spann , D. D. 2013, Fraud Analytics: Strategies and Methods for Detection and Prevention, ISBN-13: 978-1118230688.

Westphal, C., 2009, Data Mining For Intelligence, Fraud, & Criminal Detection Advanced. Analytics & Information Sharing Technologies. CRC Press Taylor & Francis Group. 978-1-4200-6723-1.

Young, M.R., 2014, Financial Fraud Prevention and Detection. Governance and Effective Practices, John Wiley & Sons, Inc., Hoboken, New Jersey, ISBN 9781118617632.