Volume 5, Issue 7, July 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey of Business Analytics for Risk Management by Fraud Detection in Financial Services

[1]Jean Claude Turiho[*], [2]Ann Kibe, [3]Irénée Mungwarakarama
[1, 3] School of Computing and Information Technology/ JKUAT, RWANDA, Lecturer at INILAK, Rwanda
[2]School of Computing and Information Technology/ JKUAT, KENYA, Lecturer at JKUAT, Kenya

Abstract*—Timely Fraud detection is one of the weapons for business analytics to manage risks in any area among three victims of fraud: financial services, manufacturing, and public administration provision. Fraud presents many faces such as benefit/welfare fraud, financial services :plastic card/check, healthcare, insurance fraud, retail fraud, credit fraud, customs fraud, tax fraud, occupational fraud, theft, bribery, insider trading and money laundering. But words such as 'scam', 'con', 'swindle', 'bamboozle' and 'cheat' are sometimes used to describe fraud. The slang nature of these terms can often hide the seriousness of the frauds they represent. The aim of this survey paper is to build and improve awareness of fraud, in order to make substantial improvements to the risk managers' ability to prevent, deter, disrupt, detect, collect fraud faces in financial services, and reveal challenges.

Keywords*— Business Analytics, risk management, fraud detection, data, big data, challenge.

I. INTRODUCTION

The problem of fraud detection and risk management in financial services is the actuality. Business systems' electronic databases have grown tremendously with the rise of big data, and will continue to increase at significant rates. Fraudulent transactions are easily hidden in these enormous datasets, but fraud and fraud detection helps risk managers gain the data analytics skills that can bring these anomalies to light and manage well risks. According to [1] Today's fast-paced society has enabled most actions, transactions, and activities to be captured and saved on various databases in a matter of minutes. Because of this, fraud has grown in sophistication and become increasingly difficult to identify. However, this influx of technology and data capturing has also provided fraud examiners with the ability to use fraud detection methods that rival perpetrators of fraud in both complexity and innovation. The increased amount of data collected by innumerable systems in turn increases the possibilities available to fraud examiners. It is through the use of data analytics that fraud examiners can combat fraud and detect anomalies in a timely and efficient manner.

The importance of fraud detection in financial services is due to the fact that fraud in data translate to significant information in wide variety of application domains. For example, Forged cheques (a genuine cheque that has been stolen and used by a fraudster with a forged signature) still accounts for the largest area of loss.

Fraud detection has been found to be directly applicable in a large number of domains. This has resulted in a huge highly diverse literature of fraud faces and capabilities for minimizing frauds. This survey aims at providing a structured and comprehensive overview of the research done in the field of fraud prevention, detection for a good risk management in financial services. We structure our work as follows: Section II, after introduction, defines the following terms: business analytics, big data, fraud prevention and detection, fraud risk. Section III identifies different frauds up to date. Section IV describes types of risk we typically encounter in the financial services industry. Section V reveals capabilities to be considered by financial industries for minimizing frauds. Section VI concludes.

II. TERMS DEFINITION

- Business Analytics

Analytics is traditionally described as being descriptive, predictive, or prescriptive. Descriptive analytics is retrospective, describing what happened in the past and is associated with the field of business intelligence. Predictive analytics seeks to forecast trends and to determine probabilities [4]. It is associated with time-series analysis, econometrics, and the determination of statistical probabilities. Prescriptive analytics seeks to determine optimal systems states and is associated with the field of operations management and management science. You cannot talk about business analytics without data. The second term to be defined is big data.

- Big data

Big Data is a broad term implying analytics with very large data sets: data which contains many measurements over time and a breadth of variables. The confines of Big Data thus are associated with the engineering challenges of efficiently storing, retrieving, processing, and assessing very large sets of data. Otherwise, the analytics techniques applied are unique only in terms of attempting to detect patterns and trends in large data sets.

Big Data also introduces an advancement concerning the ability to rapidly identify reliable predictive models across large sets of variables. Social science traditionally progresses with the identification of a causal hypothesis which is then

tested via experimental observational data. The Big Data approach upends this framework by using computational approaches to identify rough correlative models with high predictive accuracy, many times foregoing causal explanation altogether. An example is of Google Flu Trends, a facility made available via Google which is able to reliably predict flu outbreaks in specific U.S. geographic areas based on the propensity of a collection of key search terms. Google does not propose a causal model for the terms themselves, only noting that the collection of terms themselves correlate with subsequent outbreaks of the flu as tracked by the U.S. Center for Disease Control. Similarly, Big Data predictive fraud models need not explain the causal origins of fraud behaviour, only be able to correlate sets of key tracked variables with predictive accuracy in subsequent fraud. So what is fraud, fraud prevention, and fraud detection?

- Fraud prevention and detection

Fraud encompasses a wide range of illicit practices and illegal acts involving intentional deception or misrepresentation [2].

Fraud prevention and detection are related, but are not the same concepts. Prevention encompasses policies, procedures, training, and communication that stop fraud from occurring, whereas, detection focuses on activities and techniques that promptly recognize timely whether fraud has occurred or is occurring.

While prevention techniques do not ensure fraud will not be committed, they are the first line of defense in minimizing fraud risk. One key to prevention is promoting from the board down throughout the organization an awareness of the fraud risk management program, including the types of fraud that may occur.

Meanwhile, one of the strongest fraud deterrents is the awareness that effective detective controls are in place. Combined with preventive controls, detective controls enhance the effectiveness of a fraud risk management program by demonstrating that preventive controls are working as intended and by identifying fraud if it does occur. Although detective controls may provide evidence that fraud has occurred or is occurring, they are not intended to prevent fraud.

Every organization is susceptible to fraud, but not all fraud can be prevented, nor is it cost-effective to try. An organization may determine it is more cost-effective to design its controls to detect, rather than prevent, certain fraud schemes. It is important that organizations consider both fraud prevention and fraud detection. If fraud has been detected then risk appears. So the next term to be discussed is fraud risk.

- Fraud Risk

Let us explain what we mean by the term 'fraud risk'. First, it is important to define 'fraud'. There is no universal definition and we will use the definition 'using deception to make a personal gain dishonestly for oneself and/or create a loss for another' in [3]. Plainly speaking, fraud involves a perpetrator coming a deceptive act to obtain a benefit. The term 'fraud' commonly includes activities such as theft, corruption, conspiracy, embezzlement, money laundering, bribery and extortion. Fraud can occur anywhere where there are people who are dishonest, or who become dishonest. Different types of fraud. Fraud can mean many things and result from many varied relationships between offenders and victims. Fraud includes: Crimes by individuals against consumers, clients or other business people; employee fraud against employers; crimes by businesses against investors, consumers and employees; crimes against financial institutions; crimes by individuals or businesses against government; crimes by professional criminals against major organisations; e-crime by people using computers and technology to commit crimes. Fraud is an issue that all organisations may face regardless of size, industry or country. If the organisation has valuable property (cash, goods, information or services), then fraud may be attempted.

Therefore, fraud risk is the chance of a perpetrator (or perpetrators) committing a fraud which has an impact on the organisation. A fraud risk comprises three elements: the method of fraud, the effectiveness of controls, and the degree of dishonesty and skill level of the perpetrator in [3].

III. IDENTIFICATION OF DIFFERENT TYPES OF FRAUDS UP TO DATE

Before identifying different types of fraud, we state the fraud victims. Fraud victims are banking/financial services, manufacturing, and government/public administration. So, there are three basic types of fraud: asset misappropriation, bribery and corruption, and financial statement fraud. In many fraud schemes perpetrated by employees, more than one type of fraud is present.

Asset misappropriation schemes include those frauds in which a perpetrator employs trickery or deceit to steal or misuse an organization's resources. In these cases, specific assets of the organization are taken to directly benefit the individuals committing the fraud. Individuals committing asset misappropriation-type crimes may be: employees of an organization, customers or vendors of an organization, or could be individuals unrelated to the victim organization. An asset misappropriation might include things like check forgery, theft of money, inventory theft, payroll fraud, or theft of services.

The next most frequently occurring fraud scheme is **bribery and corruption**. Bribery and corruption include schemes such as kickbacks, shell company schemes, bribes to influence decision-making, manipulation of contracts, or substitution of inferior goods.

The least common type of fraud is **financial statement fraud**. The definition of financial statement fraud can be found in several authoritative reports and textbooks. Financial statement fraud has been defined differently in the academic literature by academicians, in the professional literature by practitioners, and in official pronouncements by authoritative bodies. Financial statement fraud is defined by the [6] as: the intentional, deliberate, misstatement or omission of material facts, or accounting data which is misleading and, when considered with all the information made available, would cause the reader to change or alter his or her judgement or decision.

The following figure summarizes the three basic types of fraud identified until now, with each category further broken down into several subcategories as shown in the Occupational Fraud and Abuse Classification System, also known as the Fraud Tree in [6] . The thousands of occupational fraud cases analyzed over last two decades of research have all fallen into one or more of the categories delineated by this figure.

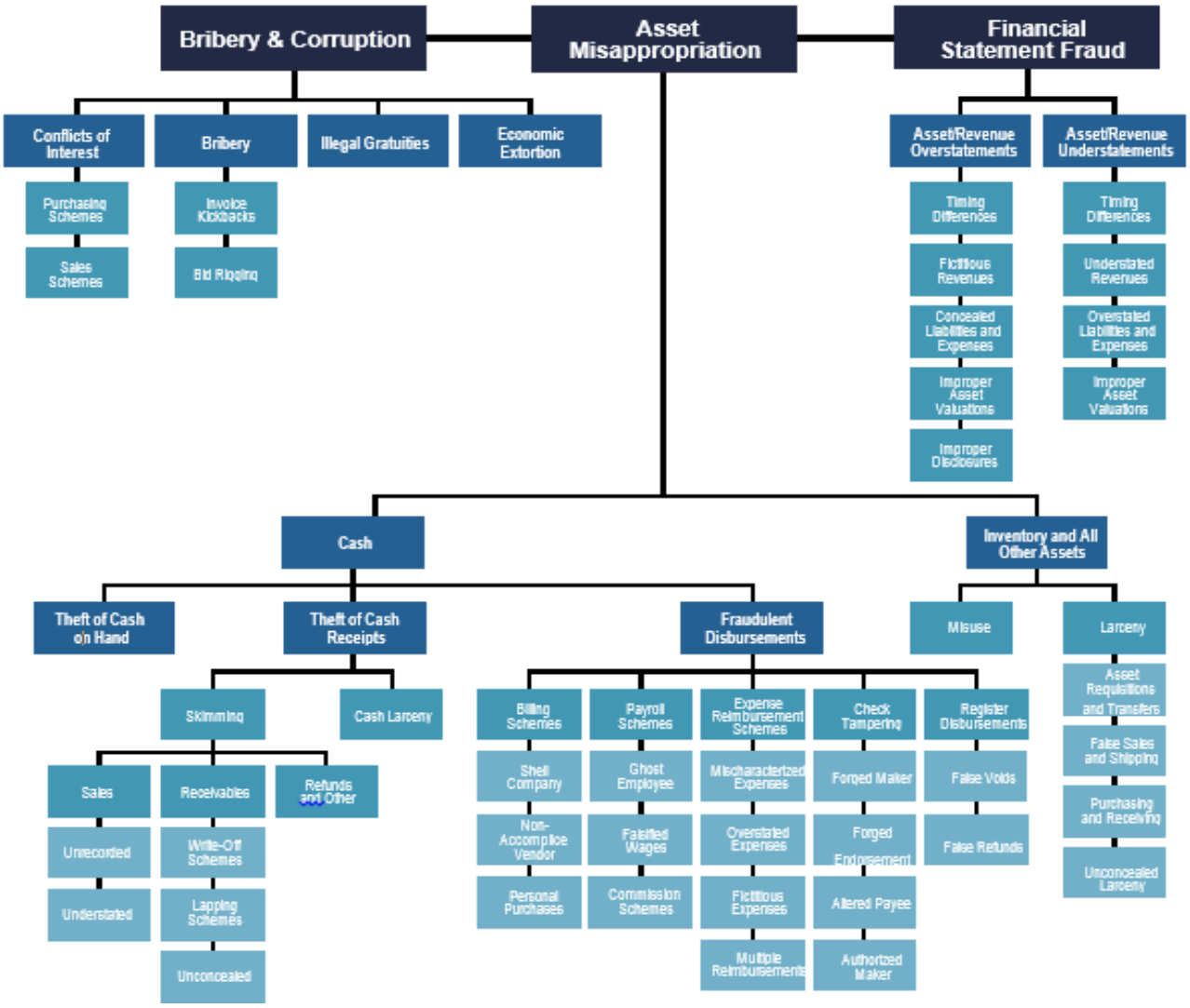

Fig 1 Fraud tree

IV. TYPES OF RISK WE TYPICALLY ENCOUNTER IN THE FINANCIAL SERVICES INDUSTRY

Reference [7] writes that the risk management has always been an explicit or implicit fundamental management process in financial services. Today, however, there is more pressure to avoid things going wrong while continuing to improve corporate performance in the new environment. Good risk management is a decisive competitive advantage. It helps to maintain stability and continuity and supports revenue and earnings growth. The main types of risk we typically encounter in the financial services according to [7] are Credit, Market, and Operational risks. Each one of them have subcategories. Normally fraud risk is one component of operational risks.

Risk management is the practice of using processes, methods and tools for quantifying and managing these risks and uncertainties. It also focuses on identifying what could go wrong, evaluating which risks should be dealt with and implementing strategies to address those risks. Firms that have identified their risks 'in advance' and have formulated a response plan will be better prepared and have a more cost-effective way of dealing with them if they do occur.

Operational risk focuses on the risks associated with errors or events in transaction processing or other business operations. A fraud risk review considers whether these errors or events could be the result of a deliberate act designed to benefit the perpetrator. Business analytics work for discovering in business operations errors or events in transaction processing, this is discussed by highlighting the capabilities to be considered by business analytics for minimizing the frauds in the next section.

V. CAPABILITIES TO BE CONSIDERED BY BUSINESS ANALYTICS FOR MINIMIZING FRAUDS

Currently, there is a lack of big data architecture for supporting identity management to combat fraud. Reference [9] notes that a key element of the architecture for an identity management system is the data set. With big data and analytics, the sourcing of several data points, or items from various sources to determine the unique identity of an individual or organisation, is achievable. Therefore, in order to detect fraud, it is necessary to develop a data set of identification

attributes that can uniquely describe individuals or potential fraudsters. This data set also needs the ability to check for inconsistencies and internally 'triangulated' for uncertainties, errors, and in particular, fraud [9], in other word outliers detection in real time.

One aspect of information processing focuses on developing dynamic network-based structures which operate as a coordination mechanism [10]. This builds the foundation for a data orientated culture, necessary to conduct business analytics, which in turn reduces the effect of uncertainty.

A number of recent studies describe the growing value of using business analytics and big data on value creation or firm performance ([11]; [12]; [13]; [14]) and citing a lot of room for further empirical research. Business analytics is an "extensive use of data, statistical and quantitative analysis, explanatory and predictive models, and fact-based management to drive decisions and actions." [15]. Business analytics has been identified to contribute to firm performance and create competitive advantage [15]. Profitability rates are 5-6% higher for firms with analytic capabilities than those without ([16]; [17]). High performing businesses have implemented data and analytics into their core business functions allowing for repeatable and accurate decision-making processes to maximise the potential of their data [19].

To prevent fraud, and –if any fraud has occurred- to identify it, reference [18] has proposed the following. By applying the information processing notion, we identify an initial set of three big data processing capabilities that financial industries must develop −based on the business analytics solution− for combatting fraud. Those capabilities are interrelated and work together, and cannot be viewed in isolation. **Developing Identity** Profiling posits the role of an authenticating reference which provides information regarding the user. **Developing Colocation Advice**: Developing information combining of both physical and digital locations is crucial to determining fraudulent behaviour. Developing Socio-Technical Expertise: **Developing and applying socio-technical information processing techniques** to big data tools are essential. To achieve successfully, we have to know that an effective big data fraud analytics program is a complex system involving the integration of **people** (organization), **processes** (methods), and **systems** (technology). The integration between these factors must be well-considered: how human process-based workflow is facilitated by technical systems to achieve measurable results. Human-computer interaction must be considered carefully, from user interface and workflow design, to the degree to which automated decision systems defer to human experts and vice versa. [4].

VI. CONCLUSION

Business analytics as weapon to fight against fraud in financial industries, faces three main categories of fraud namely asset misappropriation, bribery and corruption, and financial statement frauds. This survey has described them, the risks they are presenting, to overcome at the end with three capabilities to be considered by business analytics for minimising the frauds in financial industries. One, developing identity profiling, two, developing colocation advice, and three developing and applying socio- technical information processing techniques. Always taking into account the integration of people (organization), processes (methods), and systems (technology).

REFERENCES

[1] Sunder Gee, Fraud and fraud detection: a data analytics approach, (9781118936764), (2014, November), Published by John Wiley & Sons, Inc., Hoboken, New Jersey

[2] Litan, Avivah, Use Big Data Analytics to Solve Fraud and Security Problems, (2013, March 29), (G00247014). Retrieved from Gartner database.

[3] CIMA, Fraud risk Management: A guide to good practice, (2015, March), TEC050V0110, 26 Chapter Street, London SW1P 4NP, United Kingdom

[4] S. Mongeau, Continuous Fraud Monitoring and Detection via Advanced Analytics, (2014, March), 24th Annual ACFE Global Fraud Conference, Amsterdam, Netherlands.

[5] IBM, Fraud detection: recognize the many faces of fraud, (2010), IBM Corporation, Route 100, Sorners, NY 10589, USA

[6] ACFE, Report to the Nations on Occupational Fraud and Abuse, (2014), Global Fraud Study, Austin, USA.

[7] Hans-Ulrich Doerig, Operational Risks in Financial Services: An Old Challenge in a New Environment, (2003), Suisse

[8] Roberts, Lynne D. and Indermaur, David and Spiranovic, Caroline, 2013. Fear of cyber-identity theft and related fraudulent activity. Psychiatry, Psychology and Law 20 (3): pp. 315-328.

[9] Yang, Y., Lewis, E., and Newmarch, J. (2010). Profile-Based Digital Identity Management—a Better Way to Combat Fraud. In Proceedings of Technology and Society (ISTAS), 2010 IEEE International Symposium on, p. 260-267, IEEE

[10] Kwon, D., Oh, W., and Jeon, S. (2007). Broken Ties: The Impact of Organizational Restructuring on the Stability of Information-Processing Networks. Journal of Management Information Systems, 24 (1), 201-231.

[11] Gillon, K., Aral, S., Lin, C.-Y., Mithas, S., and Zozulia, M. (2014). Business Analytics: Radical Shift or Incremental Change? Communications of the Association for Information Systems, 34 (1), 13.

[12] Seddon, P. B., Constantinidis, D., and Dod, H. (2012). How Does Business Analytics Contribute to Business Value?

[13] Shanks, G., Sharma, R., Seddon, P., and Reynolds, P. (2010). The Impact of Strategy and Maturity on Business Analytics and Firm Performance: A Review and Research Agenda. ACIS 2010 Proceedings.

[14] Wixom, B. H., Yen, B., and Relich, M. (2013). Maximizing Value from Business Analytics. MIS Quarterly Executive, 12 (2).

[15] Davenport, T. H., and Harris, J. G. (2007). Competing on Analytics: The New Science of Winning. Harvard Business Press.

[16] Barton, D. C., David, Making Advanced Analytics Work for You, (2012), Harvard business review, 90 (10), 78-83, 128.

[17] McAfee, A., and Brynjolfsson, E., Big Data: The Management Revolution, (2012), Harvard business review, 90 (10), 60-68.

[18] Daniel Cheng, Felix Tan, Zixiu Guo, Michael Cahalane, Developing ICT-Enabled Information Processing Capabilities for Combatting E-Commerce Identity Fraud: A Case Study of Trustev's Social Fingerprinting Solution, (2015), In proceedings of Pacific Asia Conference on Information Systems (PACIS), Singapore.

[19] Mulani, N., The Million Dollar Opportunity: Reaping Returns from Analytics. Information Management, (2013).

