Macrothink Institute™

International Journal of Accounting and Financial Reporting
ISSN 2162-3082
2021, Vol. 11, No. 4

Financial Statement Fraud: Challenges and Technology Deployment in Fraud Detection

Intan Waheedah Othman

Faculty of Accountancy, Universiti Teknologi MARA

Selangor Branch, Malaysia

E-mail: waheedah87@uitm.edu.my

Received: October 4, 2021 Accepted: October 30, 2021 Published: November 17, 2021

doi: 10.5296/ijafr.v11i4.19067 URL: https://doi.org/10.5296/ijafr.v11i4.19067

Abstract

Fraudulent financial reporting and other forms of earnings misstatement are catastrophic and pose a considerable threat to capital market stability. This study reviews the literature on existing technology-based methods of detecting financial statement fraud. The aim is to describe the challenges of predicting a rare fraud event and provide an understanding of the various data-mining based techniques for financial statement fraud detection. Given that fraudsters are becoming more adaptable and are constantly devising new ways to outwit the fraud detection system, the study provides directions for future research in detecting the evolutionary fraudulent financial reporting.

Keywords: Anti-fraud technology, Data mining, Fraud detection, Fraudulent financial statement

1. Introduction

Fraud cases have significantly increased and continued to gain prominence. Following the well-renown fraud cases such as Enron and WorldCom that had their earnings decreased by billions (Graham et al., 2008), recent cases such as Tesco, JP Morgan and Green Mountain Coffee have caused severe erosion of shareholder confidence in capital markets and drawn public attention to the criticality of fraud (Peterson & Buckhoff, 2004; Rezaee et al., 2004).

Financial statement fraud is one of the main classes of fraud and is defined as “the material omissions or misrepresentations resulting from an intentional failure to report financial information in accordance with generally accepted accounting principles” (Nguyen, 1995). It includes malpractices such as fabricating or altering records, documenting bogus transactions, omission of transactions or events from records, and masquerading substantial information (Stolowy & Breton, 2004). Financial statement fraud or financial misstatements which are the

focus of this study are distinguished from unintentional financial misrepresentations such as accounting errors.

The global fraud survey by The Association of Certified Fraud Examiners (ACFE, 2020) documented that fraudulent financial reporting is the least common (10% of schemes) but the costliest form of fraud. It is reported that each occupational fraud case would incur a median cost of $125,000 over a median period of 14 months. Whilst asset misappropriation and corruption happen more frequently than financial statement fraud, the impact of the latter crime is considerably greater in magnitude. Financial statement fraud cases alone reported a median loss of $954,000 with a median period of 24 months.

Generally, financial statement fraud results in the impairment of a firm's productivity, operational efficiency, and innovation. It shifts resources to unproductive business projects, restricts a firm's prospect to grow, reduces a firm's equity value and places a company in a risky position of being delisted from the stock exchange (Rezaee, 2005). Over the last two decades, a projected amount of $5.127 trillion has been incurred being the financial repercussions from fraud activities that have occurred worldwide. This phenomenon is associated with the rise in related losses by 56% in the last ten years [Gee & Button, 2019]. The true underlying costs of fraud might be greater when considering the indirect costs suffered, such as the credibility damage faced by creditors, employees and investors, including the destruction of business reputation caused by the accounting scandals. The eventual bankruptcy and delisting of companies exacerbated the situation (Craja et al., 2020).

The deployment of an effective fraud detection strategy is crucial due to the costly and catastrophic nature of fraud. Fraud detection further facilitates fraud prevention. As firms continually improve fraud detection methods, employees become more certain that fraud will be detected, thus discouraging them from committing fraud in the future. Ngai et al. (2011) highlight that the detection of financial statement fraud allows decision makers to design suitable measures to minimize the effect of fraud and generate an average yearly gain in profit ranging from 10 to 40 percent. It is also contended that the long-term benefits of implementing fraud prevention and detection control measures outweigh the associated costs (Hopwood et al., 2012).

The Statement of Auditing Standards (SAS) No. 82 issued by the American Institute of Certified Public Accountants (AICPA) highlights the responsibility for detecting fraudulent activities lies heavily with the auditors. Nonetheless, no specific guidelines on detecting fraud were provided, regardless of the task being complicated for the auditors. Based on the ACFE 2020 report, external and internal auditors detected only a limited number of fraud incidences, at rates of 4% and 15% and 4%, respectively (ACFE, 2020). Superseding SAS No. 82, SAS No. 99 established a framework for addressing weaknesses in fraud detection processes, with the aim of boosting auditor quality and effectiveness in detecting fraud via an assessment of fraud risk factors in companies. Nevertheless, despite reforms of accounting and auditing standards, and new anti-fraud laws being enacted to combat the prevalent cases of fraudulent financial reporting, numerous firms' anti-fraud measures are rather superficial and outdated (Andersen, 2004). The commonly applied red flag approach, which entails a checklist of

fraud warning signals, is deemed ineffective. Krambia-Kardis (2002) argued that red flags do not indicate the occurrence of fraud incidences, but they serve as cues to warn auditors of the likelihood of fraud incidences. It is further contended that the red flag approach suffers from two main drawbacks, i.e. (i) there is an association between red flags and fraud, however, the association is imperfect, and (ii) red flags put emphasis on specific cues which prevent auditors from discovering other causes of fraud.

The detection of fraudulent financial reporting cases is very challenging in view of the contemporary business environment, which is very much information-oriented, with complex and dynamic business operations and systems (Chen et al., 2019). The use of automated systems for detecting fraudulent financial reporting has gained increasing attention as a result of the application of computer-assisted mechanisms to commit fraud and the evolution of technologies used to evade fraud detection (SEC, 2019). These automated systems for fraud detection are critical, especially for auditors, since they enhance the pace and accuracy of auditing (Abbasi et al., 2012; Albrecht et al. 2008). A faster and efficient fraud detection strategy can substantially reduce the magnitude and loss of fraud (ACFE, 2020). In addressing this issue, significant attempts have been undertaken to develop intelligent systems capable of detecting financial statement fraud. This paper discusses (1) the low predictability of rare events, (2) explores existing technology-based methods in financial statement fraud detection, and (3) suggests future research in detecting the evolutionary fraudulent financial reporting.

2. The Low Predictability of Rare Fraud Event

Financial statement fraud is a rare event and rare events can be very hard to predict. Forecasting business and economic activity, and particularly fraud event prediction, is almost always difficult owing to the high degree of uncertainty surrounding the activities. It is asserted that the possibility of prediction inaccuracy creates a massive problem for decision- and policy-makers alike (Makridakis et al., 2009). On the one hand, acknowledging the limitations of prediction accuracy may indicate an inability to gauge associated uncertainty and decision accuracy. Accepting the possibility of accurate prediction, on the other hand, would mean surrendering to shocks and illusions of control, both of which may have catastrophic consequences.

Goodwin & Wright (2010) discuss factors that contribute to the difficulty of predicting uncommon occurrences such as fraud. Firstly, when the data contains a huge number of comparable occurrences (large reference class), prediction improves due to the ability to extract relative frequency information. Whilst a large reference class is related to large sample sizes, it is feasible to obtain a highly precise assessment of the underlying probability distribution. It is also possible to avoid biases in judgment since a large reference class can be assessed using statistical analysis throughout the estimation process. In contrast, constructing a relative frequency-based probability for a rare event, for instance, financial crisis or fraud, is hence more challenging due to its small reference class.

Secondly, a prediction model may simplify the actual system and may fail to embed the complex interactions between the system's various distinct components. This is mostly

relevant in models of the economy, the human body and weather systems (Orrell & McSharry, 2009). Small modifications in any of the system's components may cause an amplified impact due to the intricate interplay of the system's components. This may lead to underestimation by the prediction model of the actual arrays of uncertainty, resulting in probabilities that are inaccurately estimated.

Thirdly, the fundamental assumption of most prediction models is the causal relationship between variables. Nonetheless, despite general acceptance among experts in the field, the coherent theory of causality does not prove the reality of causation. Correlations may be illusory or the result of unknown spurious factors (Hamilton & Rose, 1980) particularly when involving human judgment, or they may be applicable only under specific circumstances pertinent to the specified reference data. Nonetheless, the misconception that strong correlation implies causality may significantly influence one's reasoning.

Finally, human judgment is often used to estimate the probability of a rare event happening, particularly when the reference class has insufficient event cases for statistical analysis. Tversky & Kahneman (1974) assert that individuals employ basic mental strategies or heuristics in dealing with the complexities of probability estimation. While heuristics may result in good estimates at times, they can also result in systematic bias in judgments.

Based on the above factors, it can be concluded that catastrophic rare fraud events can be hardly predictable. However, efforts to develop a detection tool capable of alerting interested parties to fraud perpetrators or financial fraud cases remain crucial in order to bring red flags of fraudulent activities to the attention of interested parties at an early stage. The continual attempts to develop a fraud detection model may allow for incremental improvement of previous detection models' shortcomings. This may improve the accuracy of future fraud predictions.

3. Technology Deployment in Detecting Financial Fraud

Traditional methods of fraud detection depend heavily on conventional approaches such as auditing, which are less efficient due to the complexity of the fraud case. Data mining-based techniques have been found to be more effective in detecting fraud due to their capacity of identifying small anomalies in big data sets (Ngai et al., 2011). The two main types of data mining are statistical and computational. Statistical methods are those traditional mathematical techniques, such as Bayesian theory and regression, whereas computational techniques refer to modern intelligence techniques, such as support vector machines and neural networks. The way the statistical method operates is relatively inflexible compared to the computational methods that can learn from and adapt to the problem domain (West & Bhattacharya, 2016). The data mining concepts are applied to various fraud detection methods used in numerous circumstances involving fraud, although they may vary in many ways depending on the particular domain knowledge (Zhou & Kapoor, 2011).

Zhou & Kapoor (2011) highlight five common data-mining techniques used for fraud detection reviewed in past literature, which include regression, neural networks, decision trees, support vector machines and Bayesian networks. Studies have shown that regression is

the most commonly used statistical method to detect fraud. The specific type of regression analysis includes logistic regression, stepwise regression, multi-criteria decision aid method and exponential generalized beta two.

Logistic regression is one of the commonly used method to detect financial statement fraud by predicting patterns in data with numeric or unambiguous traits (Ngai et al., 2011; Bhattacharyya et al., 2011). Logistic regression is a statistical technique for categorizing binary data that entails doing regression on a collection of variables using a linear model (Ngai et al., 2011; Ravisankar et al., 2011). It employs a dependent response variable and a set of input vectors to determine the likelihood that the outcome falls into a certain category using the natural logarithm. Studies such as Yao et al. (2019); Dechow et al. (2011); Hribar et al. (2014); and Hasnan et al., (2013) applied logistic and selection of the right covariates seems to play a significant role in determining the predictive ability of the fraud detection model.

Dechow et al. (2011) analyzed the predictability of off-balance sheet activities, market-based measures, accruals quality and financial performance to detect financial misstatements. They examined 451 earnings misstatement firm-years using stepwise logistic regression and applied the backward elimination technique using the first-order approximation of the remaining slope estimates based on the Lawless and Singhal 1978 computational logarithm. The overall analysis outcome is a scaled probability (F-score) which reports that revenue overstatements, expense misstatements and cost capitalization are the common types of financial misstatements. Hasnan et al. (2013) examined 53 fraud firms and a matched 53 non-fraud firms in Malaysia between 1996–2007. By using logistic regression, results show that financial distress, multiple directorships, audit quality, founders on the board, prior violations are significant predictors of the likelihood of fraudulent financial reporting.

Bayes classifier is a basic statistical method which is widely applied for detecting fraud. It operates on the classification principle by computing the posterior probability using the Bayesian formula based on an object's prior probability. Specifically, the likelihood of an item belonging to a particular class is initially determined, followed by the selection of the class with the highest probability, being the class which the item belongs to. Xu & Zhu (2014) applied the Bayesian classifier model on a large dataset comprising firms that were subject to US Securities and Exchange Commission (SEC) enforcement actions for allegedly engaging in financial misstatements between 1982 and 2005. Findings have shown that the Bayesian method appears to be an alternative approach that effectively assesses financial misstatement risks and provides supplementary inferences beyond those generated by the classical models such as financial ratios and regression analysis.

A neural network also gained an increased application in the computational-based technique category due to its relative effectiveness in detecting fraud. Neural networks are capable of mining inter-correlated data and may be used to solve issues when some assumptions related to regression are not true (Zhou & Kapoor, 2011). White (1989) reports that feed-forward neural networks do not require a predefined functional form and perform a stochastic approximation similar to nonlinear regression. Back propagation neural network is adaptable

and has become one of the most common methods for addressing prediction and classification issues. The learning process of the back propagation is iterative in nature, with constant minor weight adjustments made in each neural network layer to minimize systematic error. The iterative steps of the learning process recur until the total error value falls below a predefined threshold (Koh Low, 2004). However, neural network has its limitations in detecting financial statement fraud, particularly when the data examined is volatile or when the causal functionality evolves in an unpredicted manner. Based on datasets of 550 firm-years, Omar et al. (2017) compared fraud companies with matched non-fraud companies across small market capitalization firms. The analysis of ten financial ratios using the artificial neural network produces a higher prediction result for the financial fraud model at 94.87 percent when compared to linear regression (92.4 percent) and other relevant techniques.

Decision tree is a supervised learning algorithm and is often employed to predict credit card, corporate and financial fraud (Sharma & Panigrahi, 2012). It is a computational-based prediction method which works by properly choosing traits that best segregate observations into mutually exclusive and exhaustive subgroups. The attributes and likely outcomes are presented in the form of a tree-like structure, whereby branches represent attributes and leaves represent the predictions or outcomes. No prior domain knowledge is required to develop the leaves, branches, or prediction model. The decision tree classifier mainly determines the initial node using the top-down selection approach. In developing the prediction model, a series of ‘if then’ procedures are performed in conjunction with the attribute selection method. Delen et al. (2013) examined the effect of financial ratios measuring profitability, solvency, turnover, liquidity and asset structure on firm performance using the well-known decision tree algorithms, i.e. QUEST, C5.0, CART and CHAID. The findings indicate that the C5.0 and CHAID decision trees provided the greatest firm performance prediction accuracy.

Support vector machine is another preferred data mining classification option due to its highly accurate prediction (Abbasi et al., 2012; Perols, 2011). It is an artificial intelligence learning method that converts a linear problem into a higher dimensional feature space. Support vector machine allows the solution of non-linear, complex problems such as the detection of financial fraud via linear classification without adding in computational complexities. There are also possibilities for real-time operation as support vector machine training and operation require relatively low computational power. Although support vector machines are prone to overfitting, they perform well on noisy financial fraud data (Pai et al., 2011). A study by Cecchini et al. (2010) applied the support vector machine to samples of fraud and non-fraud companies. Results reveal that the support vector machine accurately identified 90.6 percent of non-fraudulent firms, and 80 percent of fraudulent firms. The findings indicate that the support vector machine is capable of predicting fraud with relatively high accuracy.

Random forest is another advanced classification algorithm in data mining that extends the well-known decision tree method (Podgorelec, 2012). A random forest is made up of numerous decision trees, each of which includes a random factor. Random forest trains by

using a subset of random selection instance, and further chooses a selection of attributes to join the randomness. If a new instance occurs after a random forest has been created, each tree in the random forest is voted on and classified, with the majority vote's classification serving as the prediction result (Shipway et al., 2012). Random forest is superior in terms of accuracy and ability to handle huge datasets (Breiman, 2001). It offers several advantages, including rapid classification and training, reduced noise effects, and less susceptibility to overfitting (Khalilia et al., 2011). Cheng et al. (2021) demonstrate that random forest is a robust model capable of constructing the optimum financial statement fraud detection model. An & Suh (2020) discovered that the modified random forest model outperforms other benchmark models. Additionally, their results show that all profit-related variables appear on the list of the most important indications of financial statement fraud.

Research has shown that many data mining-based techniques have been successful and have developed into becoming a dominant tool in fraud detection. Prevalent applied techniques include regression, neural networks, decision trees and Bayesian belief networks, and thus far, no single technique can be identified as the best for fraud detection (Zhou & Kapoor, 2011). Despite the superiority of the computational learning-based fraud detection methods, it is argued that these techniques did not evolve in tandem with the current variants in the tactics used to perpetrate fraud. In fact, it gets harder to detect fraudulent financial reporting when adopting the current detection mechanisms. This may indicate that a fraudster with the necessary resources would be able to beat and deceive the detection system (Deloitte, 2008). Due to the nature of financial fraud being destructive and costly, more attention is called for the research on the computational performance of fraud detection techniques for real-time usage which is currently in scarcity (West & Bhattacharya, 2016).

4. Conclusion

Fraudulent financial reporting detection is an important topic in accounting research. This study reviews literature on the importance, challenges, and the various statistical and computational intelligence approaches to detecting fraudulent reporting. Despite their differences in performance effectiveness, the literature review revealed that each technique is capable of detecting financial fraud. Whilst a huge amount of time, effort and capital has been invested in new anti-fraud technologies, organizations that use new tools such as artificial intelligence discover benefit when used properly. The anti-fraud technology needs to be supported with appropriate expertise, governance and monitoring. Relying solely on the one-tool technology would render it incapable of addressing all fraud cases. The study by Deloitte Forensic Centre (2008) however, revealed that, regardless of the significant effort and time spent on detecting fraud, the rate and number of fraud detection have been greatly reduced. Consistent with Zhou & Kapoor (2011), applying straightforward data mining methods to detect financial statement fraud has a number of drawbacks and usage limitations. There is a challenge in that the more executives who are engaged in financial fraud are aware of the software and techniques available for fraud detection, the more likely they are to adapt their fraud tactics and evade detection, particularly by currently available techniques (Zhou & Kapoor, 2011). New innovative techniques are urgently required that are both efficient and effective in keeping up with these adaptive or potentially newly emerging financial scams.

Future studies may explore detection techniques that could orient the program in response to a firm's specific conditions. A model for detecting fraud may not provide the best prediction when using merely historical financial statement data to identify fraud (Sharma and Panigrahi, 2012). Hence, studies may consider including the analysis of governance factors since it has been argued that the deficiencies in corporate governance mechanisms have led to the wave of corporate financial scandals (Fich & Shivdasani, 2007). Moreover, exogenous parameters inclusive of internal firm-specific factors and external factors related to the economy, industry and institutional environment would provide more accurate financial fraud prediction and detection.

Acknowledgments

The author gratefully acknowledge the Research Management Centre, UiTM, Malaysia for the research grant (ref: 600-IRMI 5/3 LESTARI (060/2019) and Universiti Teknologi MARA for providing research facilities.

References

Abbasi, A., Albrecht, C., Vance, A., & Hansen, J. (2012). Metafraud: a meta-learning framework for detecting financial fraud. *MIS Quarterly: Management Information Systems*, 1293-1327.

ACFE, Report to the Nations 2020 Global Study on Occupational Fraud and Abuse, Tech. Rep. (2020) 1-57 Retrieved from https://acfepublic.s3-us-west-2.amazonaws.com/2020-Report-to-the-Nations.pdf

Albrecht, W. S., Albrecht, C., & Albrecht, C. C. (2008). Current trends in fraud and its detection. *Information Security Journal: A Global Perspective, 17*(1), 2-12.

American Institute of Certified Public Accountants (AICPA). (1997). *Statement on Auditing Standards No. 82, Consideration of Fraud in a Financial Statement Audit.* New York, NY: AICPA.

American Institute of Certified Public Accountants (AICPA). (1997). *Statement on Auditing Standards No. 99, Consideration of Fraud in a Financial Statement Audit.* New York, NY: AICPA.

An, B., & Suh, Y. (2020). Identifying financial statement fraud with decision rules obtained from Modified Random Forest. *Data Technologies and Applications, 54*(2), 235-255. https://doi.org/10.1108/DTA-11-2019-0208

Andersen, S. (2004). Despite more rigorous compliance programs, corporate fraud still thrives. *Corporate Legal Times*, 1-6.

Avery, R. J., Bryant, W. K., Mathios, A., Kang, H., & Bell, D. (2006). Electronic course evaluations: Does an online delivery system influence student evaluations?. *The Journal of Economic Education, 37*(1), 21-37. https://doi.org/10.3200/JECE.37.1.21-37

Breiman, L. (2001). Random forests. *Machine Learning, 45*(1), 5-32.

Cecchini, M., Aytug, H., Koehler, G. J., & Pathak, P. (2010). Detecting management fraud in public companies. *Management Science, 56*(7), 1146-1160.

Chen, Y. J., Liou, W. C., Chen, Y. M., & Wu, J. H. (2019, June). Fraud detection for financial statements of business groups. *International Journal of Accounting Information Systems, 32*(2017), 1-23. https://doi.org/10.1016/j.accinf.2018.11.004

Cheng, C. H., Kao, Y. F., & Lin, H. P. (2021). A financial statement fraud model based on synthesized attribute selection and a dataset with missing values and imbalanced classes. *Applied Soft Computing, 108,* 107487. https://doi.org/10.1016/j.asoc.2021.107487

Craja, P., Kim, A., & Lessmann, S. (2020, May). Deep learning for detecting financial statement fraud. *Decision Support Systems, 139,* 113421. https://doi.org/10.1016/j.dss.2020.113421

Dechow, P. M., Ge, W., Larson, C. R., & Sloan, R. G. (2011). Predicting material accounting misstatements. *Contemporary Accounting Research, 28*(1), 17-82.

Delen, D., Kuzey, C., & Uyar, A. (2013). Measuring firm performance using financial ratios: A decision tree approach. *Expert Systems with Applications, 40*(10), 3970-3983.

Deloitte Forensic Center. (2008). Ten things about financial statement fraud - A review of SEC enforcement. 2000–2008. Deloitte Financial Advisory Services LLP.

Dutta, I., Dutta, S., & Raahemi, B. (2017). Detecting financial restatements using data mining techniques. *Expert Systems with Applications, 90,* 374-393. https://doi.org/10.1016/j.eswa.2017.08.030

Fich, E. M., & Shivdasani, A. (2007). Financial fraud, director reputation, and shareholder wealth. *Journal of Financial Economics, 86*(2), 306-336.

Gee, J. & Button, M. (2019). The financial cost of fraud 2019, *Tech. Rep, Crowe*.

Goodwin, P., & Wright, G. (2010). The limits of forecasting methods in anticipating rare events. *Technological Forecasting and Social Change, 77*(3), 355-368.

Graham, J. R., Li, S., & Qiu, J. (2008). Corporate misreporting and bank loan contracting. *Journal of Financial Economics, 89*(1), 44-61.

Hamilton, D. L., & Rose, T. L. (1980). Illusory correlation and the maintenance of stereotypic beliefs. *Journal of Personality and Social Psychology, 39*(5), 832-845.

Hasnan, S., Rahman, R. A., & Mahenthiran, S. (2013). Management motive, weak governance, earnings management, and fraudulent financial reporting: Malaysian evidence. *Journal of International Accounting Research, 12*(1), 1-27.

Hopwood, W. S., Leiner, J. J., & Young, G. R. (2011). *Forensic accounting and fraud examination*. McGraw-Hill.

Hribar, P., Kravet, T., & Wilson, R. (2014). A new measure of accounting quality. *Review of Accounting Studies, 19*(1), 506-538.

K. Nguyen, K. (1995). Financial statement fraud: motives, methods, cases and detection. *Secured Lender, 51*(2), 36.

Khalilia, M., Chakraborty, S., & Popescu, M. (2011). Predicting disease risks from highly imbalanced data using random forest. *BMC Medical Informatics and Decision Making, 11*(1), 1-13.

Kim, Y. J., Baik, B., & Cho, S. (2016). Detecting financial misstatements with fraud intention using multi-class cost-sensitive learning. *Expert Systems with Applications, 62*, 32-43.

Koh, H. C., & Low, C. K. (2004). Going concern prediction using data mining techniques. *Managerial Auditing Journal, 19*(3), 462-476.

Krambia-Kapardis, M. (2002). A fraud detection model: A must for auditors. *Journal of Financial Regulation and Compliance, 10*(3), 266-278.

Makridakis, S., Hogarth, R. M., & Gaba, A. (2009). Forecasting and uncertainty in the economic and business world. *International Journal of Forecasting, 25*(4), 794-812.

Makridakis, S., Hogarth, R. M., & Gaba, A. (2009). Forecasting and uncertainty in the economic and business world. *International Journal of Forecasting, 25*(4), 794-812.

Ngai, E. W., 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.

Omar, N., Johari, Z. A., & Smith, M. (2017). Predicting fraudulent financial reporting using artificial neural network. *Journal of Financial Crime, 24*(2), 362-387. https://doi.org/10.1108/JFC-11-2015-0061

Orrell, D., & McSharry, P. (2009). System Economics: Overcoming the pitfalls of forecasting models via a multidisciplinary approach. *International Journal of Forecasting, 25*(4), 734-743.

Pai, P. F., Hsu, M. F., & Wang, M. C. (2011). A support vector machine-based model for detecting top management fraud. *Knowledge-Based Systems, 24*(2), 314-321.

Perols, J. (2011). Financial statement fraud detection: An analysis of statistical and machine learning algorithms. *Auditing: A Journal of Practice & Theory, 30*(2), 19-50.

Peterson, B. K., & Buckhoff, T. A. (2004). Anti-fraud education in academia. *Advances in Accounting Education: Teaching and Curriculum Innovations, 6*, 45-67.

Podgorelec, V., & Zorman, M. (2012). *Decision Trees*. Springer, New York.

Rezaee, Z. (2005). Causes, consequences, and deterence of financial statement fraud. *Critical Perspectives on Accounting, 16*(3), 277-298.

Rezaee, Z., Crumbley, D. L., & Elmore, R. C. (2004), Forensic accounting education. *Advances in Accounting Education: Teaching and Curriculum Innovations, 6*, 193-231.

Sharma, A., & Panigrahi, P. K. (2012). A review of financial accounting fraud detection based on data mining techniques. *International Journal of Computer Applications, 39*(1), 37-47.

Shipway, N. J., Barden, T. J., Huthwaite, P., & Lowe, M. J. S. (2019). Automated defect detection for fluorescent penetrant inspection using random forest. *NDT & E International, 101*, 113-123.

Stolowy, H., & Breton, G. (2004). Accounts manipulation : A literature review and proposed conceptual framework. *Review of Accounting & Finance, 3*(1), 5-92.

Tversky, A., & Kahneman, D. (1974). Judgement under uncertainty: Heuristics and biases. *Science, 185*(4157), 1124-1131.

West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers and Security, 57*, 47-66. https://doi.org/10.1016/j.cose.2015.09.005

Xu, F., & Zhu, Z. (2014). A Bayesian approach for predicting material accounting misstatements. *Asia-Pacific Journal of Accounting & Economics, 21*(4), 349-367.

Yao, J., Pan, Y., Yang, S., Chen, Y., & Li, Y. (2019). Detecting fraudulent financial statements for the sustainable development of the socio-economy in China: A multi-analytic approach. *Sustainability (Switzerland), 11*(6). https://doi.org/10.3390/su11061579

Zhou, W., & Kapoor, G. (2011). Detecting evolutionary financial statement fraud. *Decision Support Systems, 50*(3), 570-575. https://doi.org/10.1016/j.dss.2010.08.007

Copyright Disclaimer