Received: 7 August 2018 | Revised: 15 April 2019 | Accepted: 23 April 2019
DOI: 10.1002/isaf.1446

RESEARCH ARTICLE

WILEY

How to detect illegal corporate insider trading? A data mining approach for detecting suspicious insider transactions

M. Fevzi Esen[1] | Emrah Bilgic[2] | Ulkem Basdas[3]

[1] Istanbul Medeniyet University, Istanbul, Turkey
[2] Kayseri University, Kayseri, Turkey
[3] Philip Morris International, Izmir, Turkey

Correspondence
Esen, M. Fevzi, Istanbul Medeniyet University, Istanbul, Turkey
Email: fevzi.esen@medeniyet.edu.tr

Summary

Only in the U.S. Stock Exchanges, the daily average trading volume is about 7 billion shares. This vast amount of trading shows the necessity of understanding the hidden insights in the data sets. In this study, a data mining technique, clustering based outlier analysis is applied to detect suspicious insider transactions. 1,244,815 transactions of 61,780 insiders are analysed, which are acquired from Thomson Financial, covering a period of January 2010–April 2017. In order to detect outliers, similar transactions are grouped into the same clusters by using a two-step clustering based outlier detection technique, which is an integration of k-means and hierarchical clustering. Then, it is shown that outlying transactions earn higher abnormal returns than non-outlying transactions by using event study methodology.

KEYWORDS

Corporate Insider Trading, Event Study, Fraud Detection, Outlier Analysis

1 | INTRODUCTION

CEOs, directors, managers and other executive members, those who are required to disclose their transactions to the public, are a class of corporate insiders accessing inside information of a company. Corporate insiders are required to report their transactions in their own firms following the transaction. Therefore, the stock returns of their transactions are widely studied in the literature. Early researches focused more on the empirical background of corporate insider transactions and descriptive findings. In general, these studies suggest that corporate insiders were willing to exploit their preferential and superior access to non-public information in order to get unfair informational advantage over the market. Besides, the profits generated by insiders (i.e., the returns of these trades) were found statistically significant (Lakonishok & Lee, 2001; Lin & Howe, 1990; Marin & Olivier, 2008; Seyhun, 1986). These researches confirmed that corporate insider trading is informative and corporate insiders gain higher returns than the market.

Despite the proved informativeness of insider trading, insiders make their trades for a variety of reasons. Traders, who do not have any preferential access to inside information and trade for liquidity or some other reasons, are associated with informational disadvantage against informed corporate insiders. The uninformed traders (i.e., outsiders) must ascertain whether insider transactions are privileged of possession of inside information that would affect the firm value. Therefore, the classification of information content of an insider trading is also critical to drive conclusions.

There are specific kinds of corporate insider transactions that have been prohibited by the law. Insider - Trading Sanctions Act of 1984 and Insider - Trading and Securities Fraud Enforcement Act of 1988 define illegal insider trading as *"buying or selling securities by insiders, while in possession of material, non-public information which is not available to the public"* (SEC, 2018). Martha Stewart's stock trading on preferential information and Levine & Boesky's misappropriation of material, non-public information about firms for the purpose of profiting are high-profile cases of people, who were convicted of engaging in illegal insider trading.

The presence of abnormal returns from corporate insider transactions shows that insiders use preferential information to conduct profitable trades and they perform significantly better than market. If insiders' transactions contain predictive content for future returns, we would expect to see significant abnormal returns (Seyhun, 2000; Tavakoli, McMillan, & McKnight, 2012).

A number of studies find some specific trading patterns in corporate insiders' transactions (Cohen, Malloy, & Pomorski, 2012; DellaVigna & Pollet, 2009; Lebedeva, Maug, & Schneider, 2017; Seyhun, 1986). These hidden patterns deviate from the standard patterns and the variables constituting these patterns are considered as a measure of insider trading profitability (Dai, Fu, Kang, & Lee, 2016; Fidrmuc, Goergen, & Renneboog, 2006; Kaniel, Saar, & Titman, 2008).

Companies listed on stock exchanges are obliged to announce their filings through an electronic information disclosure system. U.S. Securities and Exchange Commission's (SEC) EDGAR, U.K. Financial Conduct Authority's STOR and Canada Securities Commission's System for Electronic Disclosure by Insiders (SEDI) are the examples of the electronic platforms that manage information disclosures of listed companies to all investors in real-time. These platforms provide up-to-date information on corporate insiders' transactions and holdings that are required to be reported in accordance with the regulations and securities law.

Market survelliance systems are mainly focused on monitoring and reviewing trading activities around the key corporate events such as mergers and acquisitions, tender offers, earning reports, regulations and so on. These systems are developed for the purpose of a benchmark for market supervision and compliance. If abnormal price movements or trading volumes occur in the securities market, survelliance system assists officials to understand trading activity in market context and it provides preliminary evidence on illegal trading practices for in-depth investigation (Li, Sun, Chen, Fung, & Wang, 2015).

Illegal insider trading is a very difficult economic crime to detect in real-time manner. Most of the cases involve the use of circumstantial evidence to prove that a corporate insider misappropriated material non-public inside information at the time of the trade (Ferrara, Thomas, & Nagy, 2018). The authorities develop an investigation process by obtaining evidence from many data sources including insider transactions, investor tips, witnesses, media reports, informants and informal inquiries. Identification of suspicious trades according to various trade characteristics including size, price and date of transaction is one of the steps in illegal insider trading investigations (SEC, 2018a).

Data Mining (DM) is an effective methodology widely used for financial fraud detection. Despite the implementation of DM on financial statement fraud, banking, money laundering, there is a lack of research on the use of data mining for detection of insider trading. For this reason, in this study, our purpose is to handle insider trading as a fraud detection problem and employ a DM technique to detect suspicious transactions of insiders.

To our knowledge, no prior research has examined the insider transactions in accordance with its origin profiles and DM based outlier detection. In securities market, outlier detection can monitor the specific features of transactions to detect novel changes in the trading patterns of investors, which may indicate market opportunities as well as securities fraud. Detection of outliers is vital for further inspection of insider cases. In this study, we aim to provide an evidence of possible illegal insider trading by detecting suspicious insider transactions, as a part of a formal order of insider trading investigations. Based on previous research on insider trading, we identified key properties of insider transactions such as number of shares traded (Iqbal & Shetty, 2002; Lakonishok & Lee, 2001; Seyhun, 1986), value of shares traded (John & Lang, 1991; Tavakoli et al., 2012) and transaction types of insiders' (Chowdhury, Howe, & Lin, 1993; Fidrmuc et al., 2006) that are related to illegal insider trading. The input data of our analysis consists of insiders' transaction volume, value and transaction type which derived from database of Thomson Reuters Insider Transactions. Then, we discover outlying patterns of insider transactions by partitioning the trades on these properties.

This study contributes to the literature by profiling corporate insider transactions within its peer group. In order to test whether outlier insider transactions have a predictive power for returns, we also measure the abnormal returns by event study methodology. It is found out that outlying transactions portfolio has significantly higher abnormal returns than other transactions.

The paper is organized as follows: Section 2 reviews prior research done in the field of DM for financial fraud detection. Section 3 provides the outlier detection technique while Section 4 presents the dataset and the model applied. Then, Section 5 gives the results of outlier detection analysis. Section 6 explains the event study methodology to examine the stock return performance of outlying transactions versus the transactions, which are not flagged as outliers. Finally, Section 7 concludes the paper and gives some ideas for further research.

2 | DATA MINING APPROACHES TO FINANCIAL FRAUD DETECTION

In DM literature, the fraud detection systems are used to identify the patterns of suspicious or fraudulent transactions. Indeed, DM techniques can provide an effective way to handle high-volume insider transactions by flagging illegal trades (Tamersoy et al., 2014). These techniques are generally conducted to calculate the probabilities of transactions that can be suspicious or fraudulent by examining the claims. This enables analysts to make further investigation for the marked or flagged transactions (Kirlidog & Asuk, 2012).

In accounting, DM techniques are implemented to detect firms issuing fraudulent financial statements whereas in finance, the researches focus more on detecting different kind of frauds with a greater focus on credit card related ones. West and Bhattacharya (2016) reviewed more than fifty articles about intelligent systems for financial fraud detection covering 2004–2014. After classifying the content of articles (algorithm based, fraud type based and performance based), major types of the financial frauds are determined as: credit card fraud, securities and commodities fraud, financial statements fraud, and money laundering. Furthermore, major techniques applied to detect frauds are also stated such as Bayesian Belief Networks, Logistic Regression and Support Vector Machines. In another study by Jha, Guillen, and Westland (2012), a transaction aggregation strategy was proposed, which captures buying behaviours of customers, in order to detect fraudulent credit card transactions. In this method, the behaviours are input for the estimation of model used.

Rather than using quantitative approaches to detect companies filing fraudulent statements, Goel and Gangolly (2012) examined qualitative textual content in annual reports to predict fraud. They used a text mining approach by which the authors suggested six categories of linguistic cues such as complex sentential structures, positive tone and passive voice. Bahnsen, Stojanovic, Aouada, and Ottersten (2013) used a Bayesian approach by integrating the financial costs as an outcome of credit card fraud. In the study a real life data set is obtained from a European card processing company. Sahin, Bulkan, and Duman (2013) performed a credit card fraud detection study on a real data set with over 22 million transactions for a period of 12 months and they developed a decision tree algorithm that minimizes the misclassification costs. Their model works better than the classical tree models such as C5.0, CART, CHAID and CHAID. Wei, Li, Cao, Ou, and Chen (2013) created an alert system called “i-Alertor” for banking frauds. The system integrates the database, pre-processing, modelling and alerting tiers. The results obtained from a real life data set consisting of eight million transactions were compared with a rule based fraud detection system.

Junqué et al. (2014) conducted several DM techniques for detecting corporate frauds. They used a dataset consisting of three million transactions from various sources such as invoice records and data of foreign companies. Halvaiee and Akbari (2014) used Artificial Immune Systems (AIS) and introduced a new model called AIS-based Fraud Detection Model (AFDM) for credit card fraud detection. AIS are a recent branch of artificial intelligence based on the biological metaphor of the human immune system. Seeja and Zareapoor (2014) proposed credit card fraud detection model from imbalanced transaction datasets, which are based on frequent items. Zareapoor and Shamsolmoali (2015) used an ensemble classifier which handles both classification and regression methods. The dataset consisted e-commerce transactions with thousands of credit card transactions labelled by a bank as “legitimate” and “fraudulent”. They applied bagging classifier based on decision tree and indicated that the model detects the fraudulent transactions with a high detection rate. Mahmoudi and Duman (2015) used a linear discriminant, Fisher Discriminant Function, to detect credit card frauds. Lahmiri (2016) used several DM techniques for financial risk prediction. The developed predictive models accurately classified bankrupted and non-bankrupted companies which can be a useful information for corporate frauds. Bahnsen, Aouada, Stojanovic, and Ottersten (2016) proposed a new set of features to be used in detecting credit card frauds more effectively and they evaluated how different set of features impacts the results. Ahmed, Mahmood, and Islam (2016) surveyed various clustering techniques for financial fraud detection. They found out that clustering algorithms Pam, Clara, Clarans and hierarchical algorithms such as Birch, Cure, Rock are the popular ones for financial fraud detection. Carneiro, Figueira, and Costa (2017) examined the fraud problem by using real life data, an online retailer's transactions for four months, with different DM techniques.

Despite the increasing number of the studies on financial fraud detection there is a very limited number of studies applying DM data mining techniques to securities fraud. Senator et al. (1995) proposed a data-driven expert system to detect illicit financial activities with rule based reasoning. The system has ability to construct the patterns of financial transactions that are potentially related with each one by NetMap linking for scaling money laundering schemes. Kirkland et al. (1999) performed association rules analysis to detect temporal relationships in quotation and trade records. This method finds the relationships among the triggering events within a time sequence to detect suspicious transactions. Safer (2002) performed neural network analysis, which is one of the most important DM tools, in order to measure abnormal stock returns precisely. Goldberg, Kirkland, Lee, Shyr, and Thakker (2003) developed an early detection system for insider trading and other fraudulent activities including misrepresentations of filings and events in stock markets. The system combines market data, issue information and news associated with the issuer company by a rule based on reasoning and fuzzy matching. Donoho (2004) used decision tree, neural networks and k-means clustering techniques to find insider trading activities in option markets. Tamersoy et al. (2014) examined insider trading behaviors by partitioning large amount of data on factors such as transaction date and type, role of insiders and number of shares traded. They analysed the timing of transactions and trade similarities that are likely to be correlated with each other.

The literature survey of DM techniques in financial fraud indicates that the authors used a wide range of DM tools for the analysis performed. There is no consensus on which tool to use or which tool is the best, it differs according to the data and the problem to be solved. As mentioned before, there are not many studies on securities fraud detection with DM approach. Furthermore, papers about DM based outlier detection for financial frauds are also limited. In this paper, the problem of detecting suspicious insider transactions is treated as an outlier detection problem. An important and popular DM tool, cluster analysis, is used to group similar insider behaviours into the same clusters.

3 | PROPOSED TECHNIQUE: DATA MINING BASED OUTLIER DETECTION

3.1 | Overview of outlier detection techniques

The task of finding patterns that are non-conforming to the data is outlier detection or in other words, anomaly, novelty, discordant, noise, contaminant detection. According to Barnett and Lewis (1994), the definition of an outlier is “*an outlying observation, or outlier, is one that appears to deviate markedly from other members of the sample in which it occurs*”.

Outlier detection is applied to many application fields covering data cleansing, fraud detection, network intrusion, clinical trials, statistical quality control and many other tasks. Studies on outlier detection have been pursuing from nineteenth century to nowadays since there are several factors that make outlier detection challenging, and solutions with numerous techniques for these problems are still being developed. The problems such as impreciseness of the boundary between normal and anomalous behaviour and non-availability or scarceness of the labelled data make outlier detection problems hard to solve. On the other hand, the advancement of outlier detection field has been sped up depending on the advances in technology for data collection, software technology for data organization (Aggarwal, 2017).

Yamanishi, Takeuchi, Williams, and Milne (2004) states that outlier detection techniques are the most vital issue in DM. The techniques can be inspected in three general aspects: supervised, unsupervised and semi-supervised scenarios. Generally, supervised methods are being used for application-specific anomaly detection whereas unsupervised methods are for anomaly detection (Aggarwal, 2017). To be able to obtain better results, researchers apply different kind of approaches for various types of data with different numbers of attributes. The literature on outlier detection techniques indicate different aspects. For example, Hodge and Austin (2004) inspected numerous different statistical outlier detection techniques from supervised, unsupervised and semi-supervised aspects separately. Ben-Gal (2005) examined statistical methods for univariate and multivariate observations. Chandola, Banerjee, and Kumar (2009) partitioned statistical outlier detection techniques into parametric and non-parametric ones.

Patcha and Park (2007) inspected DM based outlier detection techniques in three categories: classification-based, clustering-based and association rule-based techniques. Ngai, Hu, Wong, Chen, and Sun (2011) provided a detailed literature review on detecting financial fraud via DM methods based on 49 articles, in which DM tools such as regression, classification, prediction and outlier detection were used. The most recent outlier detection survey study by Aggarwal (2017) inspected outlier detection problem in a broad range of areas such as proximity based models, information-theoretic models and supervised-unsupervised-semi-supervised models. The techniques used to detect outliers are still being improved by researchers. As far as our knowledge, Aggarwal's approach for outlier investigation seems the best so far since the investigation contains all kinds of techniques for outlier detection, from k-nearest neighbour to neural networks and k-NN distance to Principal Component Analysis.

3.2 | Outlier detection with two-step clustering

The detection of outliers in this study is performed by so-called Two-step Cluster Analysis. The approach can be viewed as integration of k-means and hierarchical clustering. As its name suggests two-step clustering first pre-clusters the cases into many small sub-clusters and then performs the hierarchical clustering to group the cases into desired number of clusters using Bayesian Information Criterion (BIC).

After forming the clusters, the outliers are searched based on deviations from the norms of their peer groups. This means that outliers to the peer group are not necessarily outliers to the population. This procedure will be detailed later.

A technical introduction can be given as follows. The processed input variables $\{X_k, k = 1,2\ldots,K+1\}$ are used to create a clustering model. The two-step clustering algorithm consists of: (a) a pre-cluster step that pre-clusters cases into many sub-clusters and (b) a cluster step that groups the sub-clusters resulting from pre-cluster step into the desired number of clusters. Given a case the closest cluster h is found. The variable deviation index VDI_k of variable X_k is defined as the contribution $d_k(h, s)$ of the variable to its log-likelihood distance $d(h, s)$. The corresponding norm value is M_{hk}, which is the cluster sample mean of X_k. The group deviation index GDI of a case is the log-likelihood distance $d(h, s)$, which is the sum of all the variable deviation indices $\{VDI_k, k = 1,\ldots,K+1\}$.[1]

Tkaczynski (2017) implies that two-step clustering has been performed in many researches since its first version. It has been used in many applications from tourism to health, marketing to transportation (Ahlqvist et al., 2017; Kent, Jensen, & Kongsted, 2014; Cerin, Leslie, Du Toit, Owen, & Frank, 2007; Grifin et al., 2014; Hsu, Kang, & LAM, 2006). Beside its user friendly usage it has also many scientific advantages too. First, two-step clustering can easily analyse mixed types of data (both categorical and numerical data) and data of just numerical or categorical. The second advantage of the approach is it solves the problem of how to decide the best number of clusters by automatically selecting the optimal number of clusters. The other advantage of pre-clustering is that it reduces the size of the distance matrix. It can also efficiently handle extremely large datasets. A further advantage of the Two-Step Cluster analysis approach is that it enables the user to identify the importance of each item in the cluster solution rather than imposing an a priori scheme. This can be very important when seeking to determine how relevant a specific variable is to the total solution (Conry et al., 2011; Pitombo, Kawamoto, & Sousa, 2011; Tkaczynski, Rundle-Thiele, & Prebensen, 2015; Vidden, Vriens, & Chen, 2016).

There are a limited number of studies that compare a two-step approach with other clustering techniques. There is also no any prior research conducted two-step clustering based outlier detection on financial fraud detection problem. Despite the limited studies, two-step approach is performed with higher levels of accuracy. Bacher, Wenzig, and Vogler (2004) found that SPSS two-step is able to assign the data points into the segments with very high accuracy when all variables are continuous. Chiu, Fang, Chen, Wang, and Jeris (2001) used both numerical and categorical data and they obtained over 95% accuracy in identifying the number of clusters and cluster membership assignment. Tan (2018) performed two-step clustering approach for data discretization. He proposed discretization of association rules since association rule mining requires all attributes to be categorical and datasets with numerical attributes first need to be discretized before rule mining. The empirical results showed that clusters obtained by two-step clustering are high quality rules when compared to other discretization methods. Kent et al. (2014) concluded

[1] The outlier detection procedure can be found in the Appendix.

that two-step clustering, Latent Gold clustering and SNOB clustering obtained a near-perfect detection of known subgroups and correctly classified individuals into those subgroups.

Additionally, some sequential models have been used in data mining and its business applications. Lahmiri and Gagnon (2016) presented a two – stage algorithm for bankruptcy prediction in financial institutions and governments. They used a regression model to process and select important features that affect business failure prediction and then, a probabilistic neural network model was adopted to achieve high probability of success for data classification. To reduce the risk of noise in learning processes of algorithms, Lahmiri (2017) proposed a two – step prediction approach with an application on bank telemarketing problem. The study shows that two – step system is robust to nonlinear and noisy data and it is suitable to make fast and easy prediction for large datasets.

4 | DATASET

The sample comprises 1,244,815 transactions from 61,780 insiders, covering the period of January 2010–April 2017. Insider transactions data is obtained from Thomson Reuters Insider Filings database, and includes insider purchases and sales on NYSE, AMEX, and NASDAQ. Data contains all insider transactions as filed on SEC form 4, 5 and 144. Insiders' transactions are also electronically available through SEC's EDGAR for the benefit of community and corporations.

Non-common shares, convertible debentures, American Depository Receipts, options, warrants and convertible bonds are excluded from dataset, only open market purchases and sales (CRSP share codes 10 and 11) are considered. Stock prices are adjusted for splits.

Table 1 gives the distribution of insider transactions by year. Number of active insiders, who have at least one transaction during the year is the highest in 2014 with the highest total number of transactions. According to Seyhun (2000) there is a strong relationship between the volume of insiders' transactions and profitability. Therefore, the highest value of average number of shares traded per transaction in 2015 may indicate a signal for profitability. It also refers that the price movement of the insiders' stocks during 2015 is higher than other years. Furthermore, starting from 2011 the average price of insiders' shares increase gradually reaching its peak value in 2016. This price performance of the insider transactions can help outsiders to determine how the stocks perform as a whole.

TABLE 1 Total number of firms, insiders, transactions and total values of shares by years

Year	Number of active insiders	Number of transactions	Average volume of shares traded (million)	Weighted average Price of shares traded ($)	Insider trading days
2010	17,420	122,363	0.069	53.38	253
2011	21,464	132,824	0.135	41.23	252
2012	21,481	130,179	0.114	47.81	253
2013	22,295	124,683	0.119	55.20	254
2014	22,709	247,694	0.112	172.74	260
2015	21,134	227,996	0.168	191.62	260
2016	19,023	195,444	0.155	329.17	257
2017	9,061	63,632	0.093	64.83	85

Note: Number of active insiders represents total number of insiders who actively purchased or sold stocks during the year. The average volume of shares traded is calculated by dividing the total volume of shares traded by total number of transactions of insiders in the corresponding year. The average price of shares traded is also calculated by adding up the dollar value of transactions (multiplying the number of shares by transaction price for each transaction) and then dividing by the total shares traded for the corresponding year. Insider trading days present total number of days on which insiders trade. The sample contains a total of 1,244,815 insider transactions covering a period between January 2010 and the end of April 2017.

5 | RESULTS OF OUTLIER DETECTION

Outlier detection with two step clustering approach yields some indices which can be used to decide which cases are candidate to be outliers. One of the indices called Anomaly Index (AI) is the most important index for detecting outliers which is defined as the abnormality of a case with respect to its peer group and hence calculated by Group Deviation Index (GDI) as shown in Appendix A. Peer group states the cluster that a case belongs to. GDI of a case is the log-likelihood distance, which is the sum of all the variable deviation indices. Rather than using GDI, the AI is better to use because of its ease to interpret. Higher AI value shows higher abnormality of the transaction (i.e., becoming outlier) since increasing values of this index correspond to greater deviations from the average. Total number and volume of shares traded for both purchases and sales transactions are used as inputs for clustering algorithm.

Based on the definition of AI and GDI, 753 transactions out of 327,000 purchases transactions are detected as anomalies that have higher values than their peers as shown in Table 2. These transactions are outliers since the owner of the transactions purchased vast amount of shares (volume variable) or the value of the shares (value variable) are very high compared to their peers.

First, AI is calculated by taking the ratio of the GDI to its average over the cluster which the case belongs to. Since more deviation means larger AI, index value greater than 2 could be anomaly candidates because the deviation in this case is at least twice the average. Thus the minimum AI value is considered as 2 in our analysis while the maximum is calculated as 31,207.5 as seen in the Table 2.

For the purchases, the highest AI value 31,207.5 belongs to the case of (transaction) 12902 as shown in Table 3. The case number 12903 also has the highest index value, and outlying transactions are the trades of the same insider. For the purchases, analysis is formed one peer group or cluster. The difference between the first and the

TABLE 2 Anomaly index summary

	N in the anomaly list	Minimum	Maximum	Mean	Std. deviation
Anomaly index	753	2.005	31207.5	180.8	1674.5

TABLE 3 Anomaly case reason list for purchases

Case	Reason variable	Variable value	Variable norm	Anomaly index
12902	Value	1,6E+13	105,099,859.7	31,207.5
12903	Value	1,6E+13	105,099,859.7	31,207.5
3558	Shares	1,403,250,000	237,201.1	9,969.7
15106	Shares	798,403,194	237,201.1	3,352.8
15107	Shares	798,403,194	237,201.1	3,352.8
50641	Shares	60,4155,998	237,201.1	1,935.3
50642	Shares	604,155,998	237,201.1	1,935.3
50643	Shares	604,155,998	237,201.1	1,935.3
50644	Shares	604,155,998	237,201.1	1,935.3
51267	Shares	604,155,968	237,201.1	1,935.3
51268	Shares	604,155,968	237,201.1	1,935.3
13572	Shares	582,293,105	237,201.1	1,799.2
…	…	…	…	…
6319	Shares	16,666,700	237,201.1	2.0
18861	Shares	16,522,500	237,201.1	2.0
18862	Shares	16,522,500	237,201.1	2.0

Note: In reason variable, “value” denotes the value of transaction and “shares” denotes the volume of shares traded.

last AI values (31207.5 and 2.0) is very high which indicates the cases 12902, 12903, 3558, 15106 and so on, are clearly outliers. While the reason of the first two anomalies is the value of the trade (value variable), the third and fourth ones are detected as outliers due to the high volume of the shares purchased.

Table 4 indicates that four out of 753 outliers are caused by the variable of transaction “value” while 749 outliers are driven by “volume of shares” variable which means the stocks purchased by insiders.

Considering the sales, approximately 915,000 transactions are analysed and 2,334 outlying transactions are detected. The maximum anomaly index is 86,021.1, which belongs to the case of (transaction) 878235 and 878236 as shown in Table 5. These two outlying transactions are the trades of the same insider. Similar to purchases, analysis is formed just one peer (group or cluster) again. Anomaly index values are very high which indicates the cases of 878235, 878236, 912085, 887551 and so on are identified as outliers. While the reason of the first two anomalies is the “value” of the trade, the rest of the outliers originate from the high volume of the “shares” sold. The value of the variable norm (mean) for the “value” variable is 4,886,186.5 and the norm (mean) of the “shares” variable is 78,304.0.

TABLE 4 Reason list

	Occurrence as reason		Variable impact statistics			
Variable	Frequency	Percent	Minimum	Maximum	Mean	Std. dev.
Shares	749	99.5%	.590	1.000	.943	.051
Value	4	.5%	.992	1.000	.996	.005
Overall	753	100.0%	.590	1.000	.944	.051

TABLE 5 Anomaly case reason list for sales

Case	Reason variable	Variable value	Variable norm	Anomaly index
878235	Value	1E+12	4,886,186.5	86,021.1
878236	Value	1E+12	4,886,186.5	86,021.1
912085	Shares	1,403,250,000	78,304	71,435.5
887551	Shares	607,200,000	78,304	15,039.7
887552	Shares	607,200,000	78,304	15,039.7
889648	Shares	428,676,000	78,304	7,615.4
889649	Shares	428,676,000	78,304	7,615.4
902335	Shares	333,505,500	78,304.	4,633.7
902336	Shares	333,505,500	78,304	4,633.7
902297	Shares	260,619,365	78,304	2,839.8
913031	Shares	223,992,000	78,304	2,100.8
912044	Shares	200,000,000	78,304	1,676.2
900845	Shares	180,505,415	78,304	1,369.2
900846	Shares	180,505,415	78,304	1,369.2
900701	Shares	180,000,000	78,304	1,358.6
…	…	…	…	…
911320	Shares	5,882,350	78,304	2.0

Note: In reason variable, “value” denotes the value of transaction and “shares” denotes the volume of shares traded.

6 | MEASURING ABNORMAL RETURNS

After detection of the outlier transactions with the two-step cluster approach, event study methodology is adopted to test whether these transactions bring significant abnormal returns. Following the common approach noted by MacKinlay (1997) the event study methodology with a market model (with equally weighted index and log returns) is implemented to understand whether purchase and sale transactions of insider traders have predictive power for abnormal returns. Basically an event study is composed of the identification of an event or event window in case of longer lasting events, estimation window to forecast without event-driven or normal returns, calculation of abnormal returns around event, and testing the significance of event returns.

Here, event day is defined as insider trading days and transaction date refers $T = 0$ Based on the market model, for security i on day t; beta (β_i) is a measure of risk representing the slope coefficient of regression model and (α_i) is firm-specific other factors. Therefore, abnormal returns ($AR_{i,t}$) are calculated as the difference of actual return of the security ($R_{i,t}$) and expected returns as follows:

$$AR_{i,t} = R_{i,t} - \left(\alpha_i + \beta_i R_{m,t}\right) \tag{1}$$

where ($R_{m,t}$) is CRSP index with equally weighted return to proxy market portfolio. Average abnormal return, AAR_t, is the average of all abnormal returns for event day, where N_t is number of abnormal returns on event day t:

$$AAR_t = \frac{1}{N_t}\sum_{i=1}^{N_t} AR_{i,t} \tag{2}$$

The cumulative average abnormal returns (*CAAR*) that refers summation of *ARs* over event window starting at t_1 and ending at t_2,are calculated as follows:

$$CAAR\ (t_1, t_2) = \sum_{t=t_1}^{t_2} AR_{i,t} \tag{3}$$

Considering that the choice of model may affect the test results, the market model is selected based on previous studies analyzing several markets (Brown and Warner, 1980 & 1985; Campbell, Cowan, & Salotti, 2010; Corrado & Truong, 2008).

Parametric and non-parametric tests are applied to cover the discussions indicating that non-parametric tests can outperform the parametric ones due to non-normality of price series (Corrado & Truong, 2008). A vast amount of studies supports the sufficient performance of parametric test statistics (Bernard, 1987; Brown & Warner, 1980; Brown & Warner, 1985; Collins & Dent, 1984; Heinkel & Kraus, 1988; Jain, 1986). Due to the inconclusive literature, in this study, following the approach of MacKinlay (1997) a non-parametric test, generalized sign test, is also employed.

Aforementioned insider transactions dataset covering the period from January 2010 to April 2017, an estimation window of 255 days (−46, +208) and different event windows around event date (day 0) are used. In order to cover information leakage before the event date, and the persistence of the impact, (−30,-2), (−1,0), and (+1,+30) event windows are considered. For purchases, 749 out of 955 event (i.e., anomaly) dates, and for sales 3305 events were used. To interpret the results, the common results of all three tests are considered.

Based on abnormal returns dates on each date around purchasing transaction, on day +1 and + 2 abnormal returns are statistically significant at 0.001 level for all three tests, even on the event day, day +3, and day +4 under 0.05 level. For sales, even from day −11 to date +1 the abnormal returns become significant under 0.05 level. Starting from date +1 to date +5, the abnormal returns are significant at only 0.10 level. On the other hand, joint results of tests cannot confirm the significance of abnormal returns over from date +6 to +30 for both purchases and sales.

The tests over different event windows for outlying transactions (Table 6. II a, II b) indicate that the abnormal returns for purchases (−30,-2), and (+1,+30) event windows and for sales (−30,-2), (+1, +30) and (−1, 0) event windows are significant. As expected, the abnormal returns for purchases are positive indicating that insider traders gained advantage by using the private information, and then share prices increased. On the other hand, for sales the insider traders were the first ones selling their shares again by using their inside information, and then share prices declined. Therefore, the purchase versus sale abnormal results support the use of inside information. These results also confirm that the outlying insider transactions have higher abnormal returns than non-outlying transactions (i.e., higher positive performance for purchases, and avoidance from higher return declines). Specifically, aforementioned event windows before the event refers information leakage before outlying transactions, and after the event there is a persistence impact on the returns.

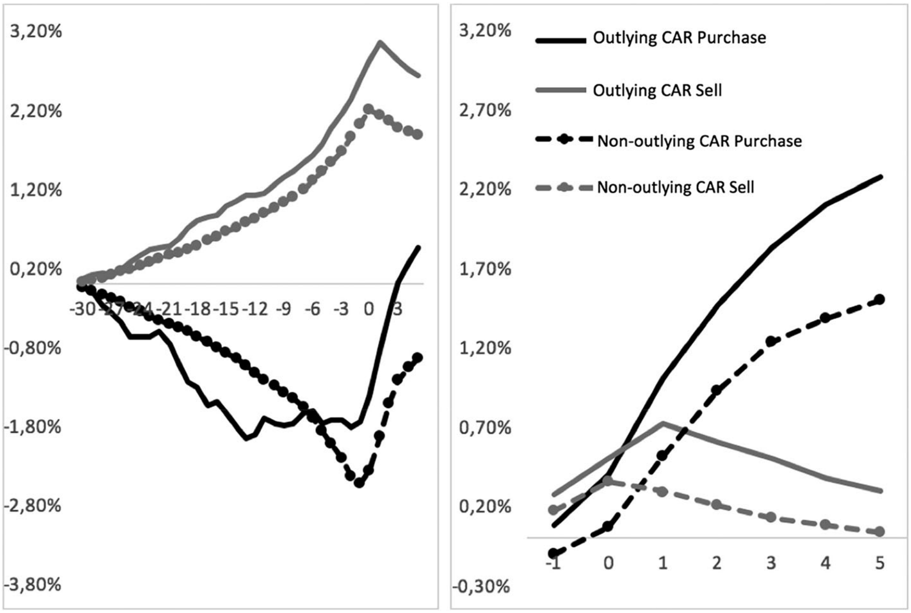
Even though the value of the abnormal returns is limited for outlying transactions, (2.43% over (+1,+30)), considering the number of cases where an insider can gain from inside information and higher invested value, this may have a significant financial value. Especially, in the current financial system with arising transaction commissions, this strategy instead of an algorithm based strategy involving several transactions would definitely bring more returns net of other costs.

Comparing the abnormal returns of outlying transactions and non-outlying transactions (Table 6. (I) vs. (II)), there is a significant difference, even non-outlying transactions have significant abnormal returns over same event windows. In other words, the results indicate that all transactions have the predictive power to explain abnormal returns. However, outlying transactions have higher abnormal returns especially at and after the event window (Graph 1). Outlying transactions seem to be handled separately since their abnormal returns are higher than non-outlying transactions. Even though previous studies found evidence on abnormal returns relating with insider trading, this study draws attention to the classification of insider transactions. It can be possible to have misleading results when all insider transactions are pooled together.

TABLE 6 Abnormal returns around anomaly dates

PANEL A. Purchases Event Window	(I) Mean CAR for non-outlyings	(II) Mean CAR for outlyings	(Ia) Patell Z	(IIa) Patell Z	(Ib) Generalized sign	(IIb) Generalized sign
(−30, −2)	−2.42%	−1.81%	−5.641***	−2.919***	−3.242***	−1.789*
(−1, 0)	0.07%	0.41%	1.665*	3.020***	0.377	0.404
(+1, +30)	1.94%	2.43%	4.159***	4.142***	3.981***	2.963**
PANEL B. Sales **Event Window**	**(I) Mean CAR for non-outlyings**	**(II) Mean CAR for outlyings**	**(Ia) Patell Z**	**(IIa) Patell Z**	**(Ib) Generalized sign**	**(IIb) Generalized sign**
(−30, −2)	−1.84%	2.56%	−14.865***	8.053***	15.790***	2.638**
(−1, 0)	0.35%	0.46%	11.169***	6.442***	8.478***	1.937**
(+1, +30)	−1.15%	−1.56%	−7.013***	−3.940***	−3.016**	−4.071***

Note: The symbols *,**, and *** denote statistical significance at the 0.05, 0.01 and 0.001 levels, respectively. Number of events for outlying purchases: 749, and for outlying sales: 3305; number of events for non-outlying purchases: 46,695, and for non-outlying sales: 147,121. (Ia) and (Ib) denote the test statistics for non-outlyings, (IIa) and (IIb) denote the test statistics for outlyings.



GRAPH 1 Cumulative average returns for outlying and non-outlying transactions over different event windows

7 | CONCLUSIONS AND FUTURE WORK

The increasing volume of transactions draws attention to the issue of fraud detection to uncover suspicious patterns and illegal activities in the stock markets. Data mining techniques have a vital role in fraud detection by both statistical and computational approaches. Even though the data mining techniques have capabilities to cope various forms of fraudulent cases, the detection of insider trading by these techniques is rarely studied.

Most of the corporate insider trading studies have provided evidence that unlike other investors, insiders have unusual returns from their purchases and sales (Seyhun, 1986; Meulbroek, 1992; Qiu, He, Xiao, 2018). In these studies, it has been shown that insiders gain an average of 3% - 30% abnormal returns in the following or preceding periods of the transaction. This shows that insider transactions can be used as a predictive tool for future returns.

Corporate insiders have some trading characteristics such as value, volume, frequency, and timing of trade, insiders' position, tenure, regulations and so on. The analysis of how to treat conflicting transactions is a part of illegal insider trading investigations. In accordance with the literature, we include volume and value of trade in the analysis to understand suspicious trading patterns in corporate insiders' transactions. This study also introduces a data mining approach for illegal insider trading in stock markets. One of the well-known outlier analysis based on two-step clustering to detect outlying transactions of insiders is employed. Cluster analysis is used to detect outliers as creating groups of insiders indicating the same behaviour into the same clusters. The transactions are identified as outliers based on the anomaly index value greater than 2 since the deviation to cluster or peers in this case is at least twice the average.

Our study contributes to insider trading literature in several ways: first, as far as our knowledge, the detection of suspicious insider transactions are studied for the first time within the field of outlier detection. We employ an outlier detection technique based on two step clustering to spot suspicious transactions and then, we measure the abnormal returns of spotted transactions to confirm suspicion for illegal insider trading. We find evidence that outlying insider transactions have higher abnormal returns than normal transactions. This evidence is consistent with the interpretation that outlying transactions of insiders convey special information signals indicating selling and purchasing opportunities over a period of time. Outside investors can execute their trades by following outlying transactions and they can add an extra 2.43% to their returns from purchases and 1.56% from sales in accordance with existing literature. Considering with the insiders' transactions as given in Table 1, insiders' abnormal profits are approximately ranged from an average of $31,000 to $48,000 per transaction in a year. Second, we draw attention to individual insider transactions for further examination by spotting outlying transactions.

For future research, various outlier detection methods both for supervised and unsupervised techniques can be used. After separating the transactions of insiders into different managerial groups, researchers can create transaction clusters for these groups and detect the outliers which have different behaviour from the norms of their peers (clusters). There is also opportunity to discover insiders' trading patterns using important variables such as transaction date, the role of insiders, number of shares held by insiders and outstanding shares of insiders' companies on insider transaction day as discriminative classifiers.

This initial step shows that data mining approaches to insider trading can also be useful for early warning system for detection of illegal insider trading by combining different algorithms. Furthermore researchers may have better results with supervised techniques if there are samples of fraudulent transactions available. Datasets of market surveillance activities, tips and complaints may also provide a better understanding of illegal insider trading.

ORCID

M. Fevzi Esen https://orcid.org/0000-0001-7823-0883

REFERENCES

Aggarwal, C. C. (2017). *Outlier analysis*. Springer, New York, USA.

Ahlqvist, E., Storm, P., Karajamaki, A., Martinell, M., Dorkhan, M., Carlsson, A., & Wessman, Y. (2017). Clustering of Adult-Onset Diabetes into Novel Subgroups Guides Therapy and Improves Prediction of Outcome. bioRxiv, 186387.

Ahmed, M., Mahmood, A. N., & Islam, R. (2016). A survey of anomaly detection techniques in financial domain. *Future Generation Computer Systems*, *55*, 278–288.

Bacher, J., Wenzig, K., & Vogler, M. (2004). SPSS Two-Step Cluster-A First Evaluation. Retrieved from: https://opus4.kobv.de/opus4-fau/frontdoor/index/index/docId/74, Accessed on 1.21.2019

Bahnsen, A. C., Aouada, D., Stojanovic, A., & Ottersten, B. (2016). Feature engineering strategies for credit card fraud detection. *Expert Systems with Applications*, *51*, 134–142.

Bahnsen, A.C., Stojanovic, A., Aouada, D., Ottersten, B. (2013): Cost sensitive credit card fraud detection using Bayes minimum risk. 12th International Conference on Machine Learning and Applications (ICMLA).

Barnett, V., & Lewis, T. (1994). *Outliers in statistical data* (Vol. 3). New York: Wiley.

Ben-Gal, I. (2005). *Outlier detection, Data mining and knowledge discovery handbook*. Springer, Boston, MA.

Bernard, V. L. (1987). Cross-sectional dependence and problems in inference in market-based accounting research. *Journal of Accounting Research*, *25*(1), 1–48.

Brown, S. J., & Warner, J. B. (1980). Measuring security price performance. *Journal of Financial Economics*, *8*(3), 205–258.

Brown, S. J., & Warner, J. B. (1985). Using daily stock returns: The case of event studies. *Journal of Financial Economics*, *14*(1), 3–31.

Campbell, C. J., Cowan, A. R., & Salotti, V. (2010). Multi-country event-study methods. *Journal of Banking & Finance*, *34*(12), 3078–3090.

Carneiro, N., Figueira, G., & Costa, M. (2017). A data mining based system for credit-card fraud detection in e-tail. *Decision Support Systems*, *95*, 91–101.

Cerin, E., Leslie, E., Du Toit, L., Owen, N., & Frank, L. D. (2007). Destinations that matter: Associations with walking for transport. *Health & Place*, *13*, 713–724.

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys (CSUR)*, *41*(3), 1–72.

Chiu, T., Fang, D., Chen, J., Wang, Y., & Jeris, C. (2001, August). A robust and scalable clustering algorithm for mixed type attributes in large database environment. In *Proceedings of the seventh ACM SIGKDD international conference on knowledge discovery and data mining* (pp. 263–268). ACM.

Chowdhury, M., Howe, J. S., & Lin, J. C. (1993). The relation between aggregate insider transactions and stock market returns. *Journal of Financial and Quantitative Analysis*, *28*(3), 431–437.

Cohen, L., Malloy, C., & Pomorski, L. (2012). Decoding inside information. *The Journal of Finance*, *67*(3), 1009–1043.

Collins, D. W., & Dent, W. T. (1984). A comparison of alternative testing methodologies used in capital market research. *Journal of Accounting Research*, *22*(1), 48–84.

Conry, M. C., Morgan, K., Curry, P., McGee, H., Harrington, J., Ward, M., & Shelley, E. (2011). The clustering of health behaviours in Ireland and their relationship with mental health, self-rated health and quality of life. *BMC Public Health*, *11*(1), 692.

Corrado, C. J., & Truong, C. (2008). Conducting event studies with Asia-Pacific security market data. *Pacific-Basin Finance Journal*, *16*(5), 493–521.

Dai, L., Fu, R., Kang, J. K., & Lee, I. (2016). Corporate governance and the profitability of insider trading. *Journal of Corporate Finance*, *40*, 235–253.

DellaVigna, S., & Pollet, J. M. (2009). Investor inattention and friday earnings announcements. *The Journal of Finance*, *64*(2), 709–749.

Donoho, S. (2004): Early detection of insider trading in option markets. Paper presented at the Proceedings of the tenth ACM SIGKDD international conference on Knowledge discovery and data mining, 420–429.

Ferrara, L. C., Thomas, H., & Nagy, D. M. (2018). *Ferrara on Insider Trading and the Wall*. USA: Law Journal Press.

Fidrmuc, J. P., Goergen, M., & Renneboog, L. (2006). Insider trading, news releases, and ownership concentration. *The Journal of Finance*, *61*(6), 2931–2973.

Goel, S., & Gangolly, J. (2012). Beyond the numbers: Mining the annual reports for hidden cues indicative of financial statement fraud. *Intelligent Systems in Accounting, Finance and Management*, *19*(2), 75–89.

Goldberg, H.G., Kirkland, J. D., Lee, D., Shyr, P., Thakker, D. (2003): The NASD Securities Observation, New Analysis and Regulation System (SONAR), Paper presented at the IAAI, 11-18

Halvaiee, N. S., & Akbari, M. K. (2014). A novel model for credit card fraud detection using artificial immune systems. *Applied Soft Computing*, *24*, 40–49.

Heinkel, R., & Kraus, A. (1988). Measuring event impacts in thinly traded stocks. *Journal of Financial and Quantitative Analysis*, *23*(1), 71–88.

Hodge, V., & Austin, J. (2004). A survey of outlier detection methodologies. *Artificial Intelligence Review*, *22*(2), 85–126.

Hsu, C. H. C., Kang, S. K., & Lam, T. (2006). Reference group influences among Chinese travelers. *Journal of Travel Research*, *44*, 474–484.

Iqbal, Z., & Shetty, S. (2002). An investigation of causality between insider transactions and stock returns. *The Quarterly Review of Economics and Finance*, *42*(1), 41–57.

Jain, P. C. (1986). Analyses of the distribution of security market model prediction errors for daily returns data. *Journal of Accounting Research*, *24*(1), 76–96.

Jha, S., Guillen, M., & Westland, J. C. (2012). Employing transaction aggregation strategy to detect credit card fraud. *Expert Systems with Applications*, *39*(16), 12650–12657.

John, K., & Lang, L. H. P. (1991). Insider trading around dividend announcements: Theory and evidence. *The Journal of Finance*, *46*(4), 1361–1389.

Junqué, F., Enric, S., Marija, M., Julie, M., Bart, P., Martens, D. (2014): Corporate residence fraud detection. Paper presented at the Proceedings of the 20th ACM SIGKDD International conference on KDD.

Kaniel, R., Saar, G., & Titman, S. (2008). Individual investor trading and stock returns. *The Journal of Finance*, *63*(1), 273–310.

Kent, P., Jensen, R. K., & Kongsted, A. (2014). A comparison of three clustering methods for finding subgroups in MRI, SMS or clinical data: SPSS two-step cluster analysis, latent gold and SNOB. *BMC Medical Research Methodology*, *14*(1), 113.

Kirkland, J. D., Senator, T. E., Hayden, J. J., Dybala, T., Goldberg, H. G., & Shyr, P. (1999). The nasd regulation advanced-detection system (ads). *AI Magazine*, *20*(1), 55–68.

Kirlidog, M., & Asuk, C. (2012). A fraud detection approach with data mining in helath insurance. *Procedia - Social and Behavioral Sciences*, *62*, 989–994.

Lahmiri, S. (2016). Features selection, data mining and finacial risk classification: A comparative study. *Intelligent Systems in Accounting, Finance and Management*, *23*(4), 265–275.

Lahmiri, S. (2017). Two-step system for direct bank telemarketing outcome classification. *Intelligent Systems in Accounting, Finance and Management*, *24*(1), 49–55.

Lahmiri, S., & Gagnon, S. (2016). A sequential probabilistic system for bankruptcy data classification. *In Analyzing Risk through Probabilistic Modeling in Operations Research* (pp. 138–147). IGI Global, Hershey PA, USA.

Lakonishok, J., & Lee, I. (2001). Are insider trades informative? *The Review of Financial Studies*, *14*(1), 79–111.

Lebedeva, O., Maug, E., & Schneider, C. (2017). Trading strategies of corporate insiders. *Journal of Financial Markets*, *34*, 48–68.

Li, X., Sun, S., Chen, K., Fung, T., & Wang, H. (2015). Design theory for market surveillance systems. *Journal of Management Information Systems*, *32*, 278–313.

Lin, J. C., & Howe, J. S. (1990). Insider trading in the OTC market. *The Journal of Finance*, *45*(4), 1273–1284.

MacKinlay, A. C. (1997). Event studies in economics and finance. *Journal of Economic Literature*, *35*(1), 13–39.

Mahmoudi, N., & Duman, E. (2015). Detecting credit card fraud by modified fisher discriminant analysis. *Expert Systems with Applications*, *42*(5), 2510–2516.

Marin, J. M., & Olivier, J. P. (2008). The dog that did not bark: Insider trading and crashes. *The Journal of Finance*, *63*(5), 2429–2476.

Meulbroek, L. K. (1992). An empirical analysis of illegal insider trading. *The Journal of Finance*, *47*(5), 1661–1699.

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.

Patcha, A., & Park, J. M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks*, *51*(12), 3448–3470.

Pitombo, C. S., Kawamoto, E., & Sousa, A. J. (2011). An exploratory analysis of relationships between socioeconomic, land use, activity participation variables and travel patterns. *Transport Policy*, *18*(2), 347–357.

Qui, Y., He, H., & Xiao, G. (2018). The information content of insider trading: Evidence from China. *Finance Research Letters*, *26*, 126–131.

Safer, A. M. (2002). The application of neural networks to predict abnormal stock returns using insider trading data. *Applied Stochastic Models in Business and Industry*, *18*(4), 381–389.

Sahin, Y., Bulkan, S., & Duman, E. (2013). A cost-sensitive decision tree approach for fraud detection. *Expert Systems with Applications*, *40*(15), 5916–5923.

SEC (2018): Securities Laws, [Online] at https://www.sec.gov/answers/about-lawsshtml.html, accessed January15th, 2019.

SEC (2018a): Insider Trading Investigations, [Online] at https://www.sec.gov/about/offices/oia/oia_enforce/foster.pdf, accessed January 14th, 2019.

Seeja, K. R., & Zareapoor, M. (2014). FraudMiner: A novel credit card fraud detection model based on frequent itemset mining. *The Scientific World Journal*, 1–10.

Senator, T. E., Goldberg, H. G., Wooton, J., Cottini, M. A., Khan, A. F., Umar, K., … Wong, R. W. H. (1995). Financial crimes enforcement network AI system (FAIS) identifying potential money laundering from reports of large cash transactions. *AI Magazine*, *16*(4), 21–39.

Seyhun, H. N. (1986). Insiders' profits, costs of trading, and market efficiency. *Journal of Financial Economics*, *16*(2), 189–212.

Seyhun, H. N. (2000). *Investment intelligence from insider trading*. MIT Press, London, England.

Tamersoy, A., Khalil, E., Xie, B., Lenkey, S. L., Routledge, B. R., Chau, D. H., & Navathe, S. B. (2014). Large-scale insider trading analysis: Patterns and discoveries. *Social Network Analysis and Mining*, *4*(1), 201–210.

Tan, S. C. (2018). Improving Association Rule Mining Using Clustering-based Discretization of Numerical Data. In *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)* (pp. 1–5). IEEE, Plaine Magnien, Mauritius.

Tavakoli, M., McMillan, D., & McKnight, P. J. (2012). Insider trading and stock prices. *International Review of Economics & Finance*, *22*(1), 254–266.

Tkaczynski, A. (2017). Segmentation using two-step cluster analysis. In *Segmentation in social marketing* (pp. 109–125). Singapore: Springer.

Tkaczynski, A., Rundle-Thiele, S. R., & Prebensen, N. K. (2015). Segmenting potential nature-based tourists based on temporal factors: The case of Norway. *Journal of Travel Research*, *54*, 251–265.

Vidden, C., Vriens, M., & Chen, S. (2016). Comparing clustering methods for market segmentation: A simulation study. *Applied Marketing Analytics*, *2*(3), 225–238.

Wei, W., Li, J., Cao, L., Ou, Y., & Chen, J. (2013). Effective detection of sophisticated online banking fraud on extremely imbalanced data. *World Wide Web*, *16*(4), 449–475.

West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers & Security*, *57*, 47–66.

Yamanishi, K., Takeuchi, J. I., Williams, G., & Milne, P. (2004). On-line unsupervised outlier detection using finite mixtures with discounting learning algorithms. *Data Mining and Knowledge Discovery*, *8*(3), 275–300.

Zareapoor, M., & Shamsolmoali, P. (2015). Application of credit card fraud detection: Based on bagging ensemble classifier. *Procedia Computer Science*, *48*, 679–685.

How to cite this article: Esen MF, Bilgic E, Basdas U. How to detect illegal corporate insider trading? A data mining approach for detecting suspicious insider transactions. *Intell Sys Acc Fin Mgmt*. 2019;26:60–70. https://doi.org/10.1002/isaf.1446

APPENDIX A

THE OUTLIER DETECTION PROCEDURE[2]

n	:The number of cases in the data
X_{ok},k = 1,2…,K	:The set of input variables in the data
M_k,k ∈ {1,2…,K}	:The grand mean or average of the variable across the entire data.
SD_k,k ∈ {1,2…,K}	:The grand standard deviation or standard deviation of the variable across the entire data.
H	:H is the pre-specified number of cluster groups to create. Alternatively, the bounds (H_{min},H_{max}) can be used to specify the minimum and maximum numbers of cluster groups.
n_h,h = 1,…H	:The number of cases in cluster h, h = 1, …,H
M_{hk},k = 1,…,K+1, h=1…,H	:The cluster mean or average of the variable in cluster h
SD_{hk},k ∈ {1,…,K+1}, h = 1…,H	:The cluster standard deviation or standard deviation of the variable in cluster h
VDI_k,k = 1,…,K+1	:The variable deviation index of a case is a measure of the deviation of variable value X_k from its cluster norm
GDI	:The group deviation index *GDI* of a case is the log likelihood distance *d(h,s)*, which is the sum of all of the variable deviation indices {VDI_k,k = 1,…,K+1}.
anomaly index	:The anomaly index of a case is the ratio of the GDI to that of the average GDI for the cluster group to which the case belongs.
variable contribution	:The variable contribution measure of variable X_k for a case is the ratio of the VDI_k to the case's corresponding *GDI*
cut point anomaly	:A pre-specified cut point; cases with anomaly index values greater than cut point anomaly are considered anomalous.
k anomaly	:A pre-specified integer threshold $1 \leq k\ anomaly \leq K + 1$ determines the number of variables considered as the reasons that the case is identified as an anomaly

[2] IBM SPSS Modeler Algorithms Guide Book, [Online] at https://www.ibm.com/support/knowledgecenter, accessed December 3rd, 2017.