Asia Pacific Fraud Journal
E-ISSN: 2502-695X, ISSN: 2502-8731
Volume 8, Issue 2 (July-Desember) 2023
*Asia Pacific Fraud Journal now has been accredited "**SINTA 3**" by Ministry of Research and Technology of The Republic of Indonesia (No SK. 225/E/KPT/2022).*
Available online at: http://apfjournal.or.id/index.php/apf

Analysis of Performance Anomaly and Fraudster Profile for Fraud Prevention and Detection

✉Dona Ramadhan
PT Adira Dinamika Multi Finance & STEBI Global Mulia Cikarang, Indonesia

ARTICLE INFORMATION
Article History:
Received October 8, 2022
Revised December 9, 2022
Accepted December 5, 2023

DOI:
10.21532/apfjournal.v8i2.309

ABSTRACT
The rapid development of technology provides us with a lot of data that can be used for various purposes, such as fraud risk management. Data analytics should be the basis for anti-fraud activities related to prevention and detection processes. This study aims to elaborate on the data analytics used in developing fraud red flags based on historical reports. By applying anomaly data analytics and demographic profiles of fraudsters, this study finds that performance anomalies contribute 68% to fraud, while 3 to 10 years of service without career advancement can trigger motivation to commit fraud. Finally, the paper recommends that data analytics should be followed by human approaches such as lifestyle audits and career advancement programs. Further research is expected to be able to complement other parameters for data analysis and use statistical methods to obtain more accurate results.

Keyword: Fraudster Profile, Anomaly Data, Data Analytics.

1. INTRODUCTION

Currently, we are in the era of the industrial revolution 4.0, which is marked by the development of digital technology such as inter-machine communication and artificial intelligence (Schwab, 2016). The massive use of gadgets and the internet provides abundant data sources that can be processed into useful information for various needs, one of which is the prevention and detection of fraud (Bănărescu, 2015; Mustika et al., 2021). Fraud is an act of deception to get something, which is motivated by three factors as mentioned in the Fraud Triangle Theory: pressure, opportunity, and rationalization (ACFE).

The Covid-19 pandemic that started in Indonesia in early 2020 has caused changes in patterns of human interaction and resulted in decreased income. Restrictions on community activities during the Covid-19 Pandemic could actually increase the risk of fraud. Opportunities for committing fraud are great because of the lack of oversight as a result of activity restrictions (opportunity). In addition, the Covid-19 pandemic has also had an impact

How to Cite:
Ramadhan, D. (2023). Analysis of Performance Anomaly and Fraudster Profile for Fraud Prevention and Detection. *Asia Pacific Fraud Journal, 8*(2), 341-349. https://dx.doi.org/10.21532/apfjournal.v8i2.309.

✉Corresponding author :
Email: ramadhanza@gmail.com

on decreasing personal and company income, forcing someone to commit fraud (pressure) with the assumption that what he is doing is something common (rationalization) because he really needs it and other people are also doing the same thing (Deloitte, 2020; Ernst & Young, 2020; PricewaterhouseCoopers (PWC), 2020; Ramadhan, 2020). The most common type of fraud that causes the greatest loss is internal fraud or occupational fraud, a fraud committed by employees of a company (Association of Certified Fraud Examiners (ACFE), 2022).

Fraud committed by employees is a threat to the company. For non-bank financial service companies, this threat needs greater attention because there are still many operational processes carried out by humans. Handling fraud in non-bank financial services companies consists of several stages: prevention; detection; investigation, reporting, and sanctions; and monitoring, evaluation, and follow-up (OJK 2020). Of the four stages, prevention is the most efficient stage because fraud has not occurred yet (Ghazali et al., 2014; Yusti et al., 2021).

Based on the Fraud Triangle Theory, including its subsequent developments such as Fraud Diamond, Fraud Pentagon, and Fraud Hexagon, the psychological aspect is a crucial aspect that triggers someone to commit fraud. Pressure can arise due to the influence of psychological factors and external situational factors (Anindya & Adhariani, 2019; Maulidi, 2020). The drive or motivation to commit fraud can occur due to the influence of situations that can be mapped based on the demographic profile of the fraudsters. For example, employees who are married and have children will experience different psychological conditions from those who are not married. Demographic profile of employees can be used as an indicator to predict the possibility of fraud (Ngosa & Mwanza, 2021). In addition to demographic profiles, fraud can also be predicted through analysis of performance anomaly data.

Data collection regarding the profile of fraudsters was carried out to find out the perpetrator's data based on demographic aspects, such as gender, years of service, and age (Association of Certified Fraud Examiners (ACFE), 2022; KPMG, 2011; Varma & Khan, 2016). Anomaly data is also one of the parameters for detecting fraud (Dataiku, 2020; Pourhabibi et al., 2020). The demographic profile of fraudsters is the result or output of data analysis and is not yet a predictor variable used to detect or prevent fraud. Meanwhile, anomaly data is used to see if there are unusual transactions that are considered fraud.

The profile of fraudsters can be used to see the tendency of perpetrators based on their demographic conditions such as age, years of service, and number of dependents. These three attributes can be regarded as factors that can motivate the occurrence of fraud. However, there is a concern that the analysis could be biased if only using demographic attributes, with the consideration that if there are two people with the same profile, but only one person commits fraud. Therefore, the demographic profile of fraudsters needs to be supplemented with other data, such as employee performance anomaly data, to improve data accuracy.

The combination of demographic profiles and employee performance anomaly data can be analyzed to detect and predict fraud. This study aims to analyze the effect of demographic profiles and performance anomalies on employees who commit fraud. This research takes a case study on a retail financing company that has a large number of employees and a fairly wide distribution of marketing networks throughout Indonesia.

2. LITERATURE REVIEW AND HYPOTHESIS

Fraud Handling Strategy

Fraud is an action that must be handled properly and seriously because it can have an impact on the company as a whole. There are at least three stages of a fraud handling strategy: prevention, detection, and follow-

up or response. Prevention is the most important stage to reduce the possibility of financial and non-financial impacts caused by fraud (Rahman & Anwar, 2014; Yusti et al., 2021). Fraud can be prevented through effective internal monitoring and control. Fraud can be detected through complaint channels and audit checks. Finally, incidents of fraud must be responded to or followed up through investigations and curative actions (Chartered Institute of Management Accountants (CIMA), 2008; Deloitte, 2021).

For finance companies, the fraud handling strategy includes four pillars: prevention; detection; investigation, reporting, and sanctions; and monitoring, evaluation, and follow-up (Otoritas Jasa Keuangan/OJK), 2018). The implementation of anti-fraud strategies for financing companies includes implementing anti-fraud awareness programs, identifying vulnerabilities, and knowing your employees (Otoritas Jasa Keuangan / OJK), 2018). Identification of vulnerabilities can be done by analysing performance anomaly data. Meanwhile, the "know your employee" strategy is implemented through demographic profile analysis. It is hoped that these two data can help improve the effectiveness and efficiency of the fraud prevention and detection process.

Fraud Theories

The most prominent theory explaining why someone commits fraud was initiated by Donald Cressey in 1953, known as the Fraud Triangle Theory, where there are three factors that encourage someone to commit fraud: pressure, opportunity, and rationalization. This theory was then developed into the Fraud Diamond Theory with the addition of the capability factor. Capability is the support of knowledge, authority, the ability to deceive the internal control system, the ability to commit fraud and so on (Utami et al., 2019; Yusti et al., 2021). The Fraud Diamond Theory was then further developed into the Pentagon Fraud Theory by incorporating the factor of arrogance. Arrogance is superior behavior over the authority possessed. He thinks that the internal control system does not apply to him (Yessi Puspitha & Wirawan Yasa, 2018). Arrogance is usually accompanied by an extravagant lifestyle and greed (Ramadhan, 2020). The theory was further developed into the Fraud Hexagon Theory which consists of six factors: stimulus, capability, opportunity, rationalization, ego, and collusion (SCORE) (Achmad et al., 2022).

Of all the theories that have been described, the Fraud Triangle Theory is still relevant to explaining why someone commits fraud. This theory can also be used to analyze all levels of employees in the corporate structure, with the scope of fraud committed by staff levels with limited authority. Pressure factors can also be divided into several sub-factors such as money, ideology, coercion, and ego (MICE) (Puspitha & Yasa, 2018).

Anomaly Data

Anomaly data indicates abnormalities due to irregularities or inconsistencies that lead to fraud (Pinto & Sobreiro, 2022). Analysis of anomaly data can be done in several ways, such as graphical analysis and machine learning methods (Massa & Valverde, 2014; Pourhabibi et al., 2020). The crucial stage in analyzing anomaly data is how to identify patterns of deviations that occur compared to the conditions that should be (Dataiku, 2020; Massa & Valverde, 2014). The expected output from anomaly data analysis is classification in both quantitative and qualitative forms (Massa & Valverde, 2014).

3. METHODS

Research Objects and Objectives

The object of this research is a case study of fraud perpetrator data at a retail financing company. The fraud perpetrator data is then supplemented with demographic profile data and performance anomaly data (deviations/variations). Every company certainly has set targets and goals to be achieved. Target variations must be

managed properly so as not to exceed the tolerance limit. Deviations can occur due to several factors, one of which is fraud.

This study aims to examine the effect of performance anomalies and demographic profiles on fraud. The results of this study are expected to determine the red flag criteria for performance anomalies and employee demographic profiles so that an action plan can be developed to prevent and detect fraud.

The expected contribution from this article is that the profile of internal fraudsters (occupational fraudsters) can be used as material for analysis in the process of preventing and detecting fraud, especially for financing companies, financial companies and other industries.

Data Attributes

Performance Anomalies

Performance anomaly is data processing that refers to the performance of retail finance company employees. The parameters used are the achievement of sales and the achievement of abnormal financing risks (far different from the average). The output of performance anomaly data processing is the risk level of each employee which includes clean, medium, high, and very high. The data used is the period from 2019 to 2022. This risk level is generated from the parameter of achieving high sales and a high above average credit risk level. The anomaly data is an indication that there is a possibility that the operational processes being carried out are not in accordance with applicable company regulations. Anomaly data can be one of the fraud detection parameters. However, to improve the accuracy of predictions, it is necessary to add other parameters or variables that are relevant to the fraud detection process.

Fraudsters Profile

The fraudster profile is employee demographic data consisting of age, years of service, and number of dependents. The years of service are divided into five ranges (KPMG, 2011), while the age range is divided into six parameters. The number of dependents calculated is employee, spouse, and number of children. Previous research stated that the majority of fraudsters are in the age range of 36-45 years (KPMG, 2011) and 31-45 years (Varma & Khan, 2016). Factors that cause acts of fraud are meeting family needs and greed (Varma & Khan, 2016). Years of service also influence employees to commit fraud. 29% of fraud is committed by employees with 3-5 years of service, 27% with 6-10 years of service, and 33% with >10 years of service (KPMG, 2011). Length of services indicates opportunity, capability, and rationalization factors that motivate employees to commit fraud (Varma & Khan, 2016). Other demographic attributes, such as gender and education level, have no significant effect because almost all fraudsters are male and have an undergraduate degree (Bachelor's Degree).

Analysis Method

The data used in this study is fraudsters data reported during the period 2019 - 2022 consisting of 318 data with staff position level (entry level). The parameters used are:

a. Risk Level based on Data Anomaly
   - Very High
   - High
   - Medium
   - Clean

b. Age
   - 00-25 years old
   - 25-30 years old
   - 30-35 years old
   - 35-40 years old
   - 40-45 years old
   - 45-55 years old

c. Years of Services
   - 00-01 year
   - 01-02 years
   - 03-05 years
   - 05-10 years
   - >10 years

d. Number of Dependents
   - S0 (Singles with no children)
   - S2 (Single with 2 children)
   - S3 (Single with 3 children)

- M0 (Married without children)
- M1 (Married with 1 child)
- M2 (Married with 2 children)
- M3 (Married with 3 children)

This study uses a descriptive analysis method to look at the portions of each parameter or several parameters for all fraudsters. Descriptive analysis is applied because the data used is fraudster data with static characteristics: committing fraud and will not change. These results are expected to provide insight that can assist the process of preventing and detecting fraud in retail financing companies with a large number of employees.

4. RESULTS AND DISCUSSION

Anomaly

Based on the graph above, the percentage of anomaly parameter is as follows: Very High (68.24%), Clean (13.52%), High (11.32%), and Medium (6.92%). Analysis of anomaly data is quite good in providing predictions of fraud with the largest percentage in the "Very High" category. However, further analysis is needed regarding inaccurate predictions (false positives), in which based on anomaly data, a person is considered "Clean", but in fact he is committing fraud.

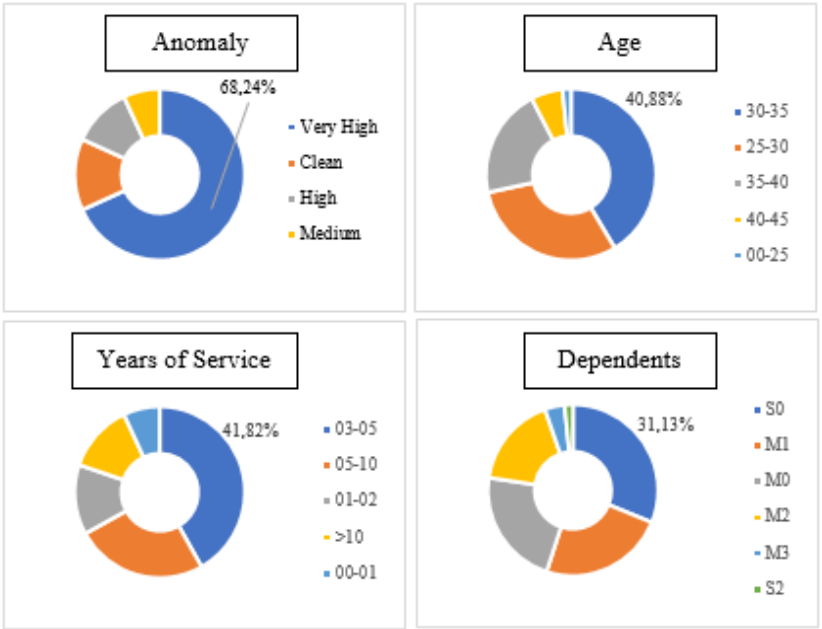
Age

The percentage of age range of fraudsters is as follows: 30-35 years old (40.88%), 25-30 years old (29.87%), 35-40 years old (20.44%), 40-45 years old (5.97%), 00-25 years old (1.57%), and 45-55 years old (1.26%). The age range from 30 to 35 years occupies the largest number. This finding reinforces the results of research conducted by Varma & Khan (2016), that the largest fraud perpetrators are in the range of 31-45 years. Age 30 to 35 years is the age when someone starts to get married and have a family, which means increasing the necessities of life.

Years of Service

The percentage of fraudsters' years of service is as follows 03-05 years (41.82%), 05-10 years (25.16%), 01-02 years (13.21%), >10 years (12.89%), and 00-01 year (6.92%). This data is similar to the results of a KPMG survey that 56% of internal fraud perpetrators had a working period of between 3 and 10 years. This finding also reinforces the notion that long working period can increase the potential for committing fraud (Varma & Khan, 2016). It should be noted that all perpetrators of fraud are staff level (entry level), which

Figure 1. **Percentage of Parameter**



Source : Data Processed

means that there is no career advancement during the tenure.

The Number of Dependents

The more the number of dependents, the higher the needs that must be met. The percentage of dependents is as follows: S0 (31.13%), M1 (23.90%), M0 (22.33%), M2 (17.30%), M3 (3.77%), and S2 (1.57%). Even though they are still single and have no dependents, they (S0) have the highest percentage of fraud perpetrators (31.13%). Meanwhile, those (M3) who already have five dependents are only at 3.77%. So it can be concluded that fraud occurs not because of the need factor, but rather the greed or lifestyle factor (Varma & Khan, 2016).

Contingency Table

To deepen the analysis of anomaly data and fraudster profiles, the two parameters are combined in the form of a contingency table. The first table shows the relationship between anomaly and the number of dependents (Table 1). Meanwhile, the second table shows the relationship between age and years of service (Table 2). The combination is based on the results of the interpretation of the proportion of parameters.

The preparation of the contingency table aims to deepen the analysis of anomaly data and demographic profiles of fraudsters. Based on the two contingency tables, it can be explained that the "Very High" risk level of anomaly data with single status has a high potential for committing fraud, because historical data shows a portion of 20.75%. Meanwhile, employees with an age range of 25 - 35 years old with 3 - 10 years of service need to be of concern, because, based on the data, the age range and years of service account for 50% of fraudsters.

Motivation to Commit Fraud

The "Very High" risk level of anomaly data means that there is an abnormality in the performance concerned. Abnormalities can be detected because the level of financing risk or sales achievement is far above average. The relationship between financing and sales risk is included in the

Table 1. **Relationship between Anomaly and Number of Dependents**

Anomaly	Number of Dependents						
	S0	M1	M0	M2	M3	S2	Total
Very High	**20.75%**	15.09%	15.41%	12.89%	3.14%	0.94%	**68.24%**
Clean	4.40%	4.72%	2.52%	1.57%	0.00%	0.31%	**13.52%**
High	4.09%	1.26%	3.46%	2.20%	0.00%	0.31%	**11.32%**
Medium	1.89%	2.83%	0.94%	0.63%	0.63%	0.00%	**6.92%**
Total	31.13%	23.90%	22.33%	17.30%	3.77%	1.57%	100.00%

Source : Data Processed

Table 2. **Relationship between Age and Years of Service**

Age	Years of Service					
	00-01	01-02	03-05	05-10	>10	Total
30-35	2.20%	5.66%	**17.92%**	**13.52%**	1.57%	40.88%
25-30	2.83%	5.35%	**18.55%**	3.14%	0.00%	29.87%
35-40	0.94%	1.26%	5.03%	7.23%	5.97%	20.44%
40-45	0.00%	0.31%	0.00%	1.26%	4.40%	5.97%
00-25	0.94%	0.63%	0.00%	0.00%	0.00%	1.57%
45-55	0.00%	0.00%	0.31%	0.00%	0.94%	1.26%
Total	6.92%	13.21%	41.82%	25.16%	12.89%	100.00%

Source : Data Processed

"Very High" category because there is distribution of financing to parties who are not eligible. In other words, fraud perpetrators manipulate data so that consumers who are not eligible become worthy. This condition explains that the motivation of the perpetrators to commit fraud is due to pressure, greed, or lifestyle, considering that the majority of perpetrators are still single.

Factors that cause a high percentage of fraudsters with 3 - 10 years of service are opportunity, rationalization and capability. 3 years of service or more is enough time to know the situation and conditions of the work environment, both internal and external, including the company's business partners. In the context of this article, the capability factor is the close relationship between the fraud perpetrator and the source of the sales order. In addition, they also understand internal conditions, so they can give inappropriate orders by taking advantage of situations or conflicts of interest due to proximity to sources of order. With the capabilities they have, they should have been able to make a bigger contribution to the company, but instead they used their capabilities to take personal advantage by committing fraud. The longer years of service also allow perpetrators to see and create opportunities to commit fraud. In addition, considering that all actors are staff level (entry level), it can be said that for 3 - 10 years they have not received any career advancement. This condition can trigger the factor of rationalization that leads to fraudulent acts.

5. CONCLUSION

This article aims to provide an overview of how analysis of performance anomaly data and demographic profiles of fraudsters (consisting of data on age, years of service, and number of dependents) can explain the factors that motivate someone to commit fraud. The expected contribution is how the profile of fraudsters can be analyzed or combined with performance anomaly data or other data that is relevant to the stages of fraud prevention and detection. Accurate data analysis can become red flags that can predict the possibility of fraud so that early prevention can be carried out.

Based on the analysis of anomaly data and demographic profiles of fraudsters, employees with the "Very High" category and "Single" marital status can become red flags for fraud perpetrators. In addition, employees aged 30-35 years with 3-5 years of service can also be red flags for fraud perpetrators.

Data analysis showing potential fraud tendencies (red flags) is the first step that needs to be followed up. Data analysis as described in this study can be supplemented by other relevant data. It is necessary to take advantage of technology, such as data analysis applications, and statistical methods to get accurate results. Utilization of technology in the analytical context can be combined with an interpersonal approach (human approach). This can be input for human resource management regarding how to meet career advancement expectations. In addition to the problem of career advancement, an interpersonal approach is also needed to assess how the lifestyle is lived, whether it is appropriate or even beyond capabilities.

For managerial implications, this research is expected to provide an analytical method based on historical data to identify patterns of fraud behavior so that it can be detected and prevented. In addition, this data analysis can be combined with a personal approach as a follow-up to the results of data analysis, such as lifestyle analysis or career advancement programs.

It is suggested that further research add other parameters related to anomaly data and internal fraudsters demographic profiles. In addition, it is also suggested that further research adds data sources by taking data that is not static, such as data on employees who commit fraud and those who do not commit fraud. This data can be analyzed using statistical methods to see the correlation or influence of employee demographic profiles and anomaly data on fraudulent behavior.

REFERENCES

ACFE. (n.d.). *https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud*.

Achmad, T., Ghozali, I., & Pamungkas, I. D. (2022). Hexagon Fraud: Detection of Fraudulent Financial Reporting in State-Owned Enterprises Indonesia. *Economies*, *10*(1). 10.3390/economies10010013.

Anindya, J. R., & Adhariani, D. (2019). Fraud risk factors and tendency to commit fraud: analysis of employees' perceptions. *International Journal of Ethics and Systems*, *35*(4), 545–557. 10.1108/IJOES-03-2019-0057.

Association of Certified Fraud Examiners (ACFE). (2022). *Occupational Fraud 2022: A Report to the Nations*. https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf

Bănărescu, A. (2015). Detecting and Preventing Fraud with Data Analytics. *Procedia Economics and Finance*, *32*, 1827–1836. 10.1016/S2212-5671(15)01485-9.

CIMA. (2008). *Fraud Risk Management: A Guide To Good Practice*. Chartered Institute of Management Accountants

Dataiku. (2020). *Fraud and Anomaly Detection in Banking A Step-by-Step Guide to Incorporating Machine Learning Into Models*. www.dataiku.com

Deloitte. (2020). *Covid 19 and Fraud Risk: Managing and responding in times of crisis*.

Deloitte. (2021). *Managing fraud risk: prevent, detect, and respond*.

EY Building a Better Working World. (2020). *COVID-19 Implications: Internal Fraud Minds Made For Protecting Financial Services*. Ernst & Young Global Limited.

Ghazali, M. Z., Rahim, M. S., Ali, A., & Abidin, S. (2014). A Preliminary Study on Fraud Prevention and Detection at the State and Local Government Entities in Malaysia. *Procedia-Social and Behavioral Sciences*, *164*, 437–444. 10.1016/J.SBSPRO.2014.11.100.

KPMG. (2011). *Who is the typical fraudster?*

Massa, D., & Valverde, R. (2014). A Fraud Detection System Based on Anomaly Intrusion Detection Systems for E-Commerce Applications. *Computer and Information Science*, *7*(2). 10.5539/CIS.V7N2P117.

Maulidi, A. (2020). When and why (honest) people commit fraudulent behaviours?: Extending the fraud triangle as a predictor of fraudulent behaviours. *Journal of Financial Crime*, *27*(2), 541–559. 10.1108/JFC-05-2019-0058.

Mustika, N. I., Nenda, B., & Ramadhan, D. (2021). Machine Learning Algorithms in Fraud Detection: Case Study on Retail Consumer Financing Company. *Asia Pacific Fraud Journal*, *6*(2), 213–221. 10.21532/apfjournal.v6i2.216.

Ngosa, P. B., & Mwanza, J. (2021). Study of Profiling the Typical Fraudster in the General Education Sector in Zambia. *International Journal of Advances in Scientific Research and Engineering*, *7*(8), 82–90. 10.31695/IJASRE.2021.34061.

OJK. (2018). *POJK Nomor 35/POJK.05/2018 tentang Penyelenggaraan Usaha Perusahaan Pembiayaan*. Otoritas Jasa Keuangan

POJK Nomor 44/POJK.05/2020 tentang Penerapan Manajemen Risiko Bagi Lembaga Jasa Keuangan Nonbank, (2020) (testimony of Otoritas Jasa Keuangan (OJK)).

Pinto, S. O., & Sobreiro, V. A. (2022). Literature Review: Anomaly Detection Approaches on Digital Business Financial Systems. *Digital Business*, *2*(2), 100038. 10.1016/J.DIGBUS.2022.100038.

Pourhabibi, T., Ong, K. L., Kam, B. H., & Boo, Y. L. (2020). Fraud detection: A systematic literature review of graph-based anomaly detection approaches. *Decision Support Systems*, *133*, 113303. 10.1016/J.DSS.2020.113303.

PricewaterhouseCoopers (PWC). (2020). *COVID-19 and the Indonesian Banking Industry: Issues and actions to consider*. http://www.pwc.com/structure

Rahman, R. A., & Anwar, I. S. K. (2014). Effectiveness of Fraud Prevention and Detection Techniques in Malaysian Islamic Banks. *Procedia-Social and Behavioral Sciences*, *145*, 97–102. 10.1016/J.SBSPRO.2014.06.015.

Ramadhan, D. (2020). Root Cause Analysis Using Fraud Pentagon Theory Approach (A Conceptual Framework). *Asia Pacific Fraud Journal*, *5*(1), 118–125. 10.21532/apfjournal.v5i1.142.

Schwab, K. (2016). *The Fourth Industrial Revolution*. World Economic Forum. www.weforum.org.

Utami, I., Wijono, S., Noviyanti, S., & Mohamed, N. (2019). Fraud Diamond, Machiavellianism And Fraud Intention. *International Journal of Ethics and Systems*, *35*(4), 531–544. 10.1108/IJOES-02-2019-0042.

Varma, T. N., & Khan, D. A. (2016). Greed an Attribute of Fraudster. *AIMS International Journal of Management*, *10*(2), 83–99.

Yessi Puspitha, M., & Wirawan Yasa, G. (2018). Fraud Pentagon Analysis in Detecting Fraudulent Financial Reporting (Study on Indonesian Capital Market). *International Journal of Sciences: Basic and Applied Research*, *42*(5), 93–109.

Yusti, M., Triyadi, T., & Ramadhan, D. (2021). Analysis of the Root Causes of Fraud Using Risk Causal and Fraud Diamond Matrix: A Case Study on Retail Financing Company. *Asia Pacific Fraud Journal*, *6*(1), 159–170. 10.21532/apfjournal.v6i1.202.