

ANALYSIS FRAUD VICTIM PROFILS IN VARIOUS REGION FOR ANTI-FRAUD CONTROL

Annisa Nur Hanifah¹

¹Faculty of Economy and Business Education, Universitas Pendidikan Indonesia, Jalan Dr. Setiabudi No.229

E-mail: annisanurhanifah09@gmail.com

ABSTRACT

The purpose of this study is to analyze and explain the profile of fraud victims in various regions and their relationship to anti-fraud controls. This type of research is a qualitative descriptive study to analyze the trend of fraud victim profiles in various regions. The observation period for the fraud victim profile is based on the ACFE (Association of Certified Fraud Examiners) Report 2012-2024. The results of the study indicate that profit-oriented organizations have experienced higher frequency and average losses of fraud cases compared to non-profit organizations over the past ten years. Smaller organizations with 100 employees or less are at higher risk of fraud compared to larger organizations. The financial and banking industries have consistently had the highest frequency of workplace fraud cases over the past decade. Most of the anti-fraud controls that companies around the world need to pay attention to are internal controls, organizational culture, reward and punishment systems, as well as anti-fraud socialization and education.

Key words: *Fraud Victim Profile; Anti-Fraud Control; ACFE (Association of Certified Fraud Examiners)*

INTRODUCTION

Fraud is a big problem in business and finance, and it can mess up how things work, harm a company's name, and lead to big money losses. It means on purpose using trickery to get things or advantages that someone isn't actually entitled to. Some companies might choose to do dishonest things because they think it's not very likely someone will find out, which makes it seem like a good option (Christian et al., 2023). On the other hand, people and groups tend to downplay the risks of being cheated out of money through scams. This action involves tricking someone on purpose to get something they don't deserve, which hurts the person being tricked and helps the person doing the tricking.

In recent years, the Association of Certified Fraud Examiners has been putting out reports on fraud cases that happen all over the world. This is a topic that needs to be talked about because fake behaviors are happening more often and showing up in different ways. After the COVID-19 pandemic, fraud increased because the economy had difficulties and companies didn't have strong enough systems in place, which made it easier for fraudsters to do their harmful activities. The Association of Certified Fraud Examiners says that asset misappropriation is the most common type of fraud, happening in 86% of the cases. According to the ACFE in 2020, financial statement fraud leads to the highest average loss, about \$954,000, which is more than the losses from other types of fraud. Even though financial statement fraud occurs less frequently than other types of fraud, it still requires more focus because it affects how trustworthy and truthful an organization's financial reports are.

To know how fraud occurs, you should understand what makes a person a target for fraud. Victimology is still the most studied area when it comes to understanding financial fraud. The person or group that gets hurt by the fraud can be a single person or a company. Research conducted by Prasetyo in 2014 showed that the size of a company can influence how quickly or easily fraud in financial statements is detected. He mentioned that companies with less money are usually better at staying honest and avoiding unfair behavior. On the other hand, some companies with a lot of assets may try to lower their reported profits by moving some income from the current period to a later period, so they can avoid paying taxes or follow new rules. This action makes the financial statements incorrect and shows a profit that is lower than the real amount.

Knowing who gets scammed is really important. Studying the profile of someone who was scammed can help a company figure out how easy it might be for that person to be targeted by fraud. This is from looking at previous fraud cases, as researched by Deliema and others in 2020. By checking this profile, you can learn which industries are most likely to face workplace fraud, as found by Sofianti et al. in 2018. In this study, the author explores how various kinds of organizations, depending on their size and type, are impacted by fraud and looks at their role in committing fraudulent activities. This study looks at the characteristics of people who have been tricked by scammers in various places around the world. The goal is to learn how fraud can occur by studying the characteristics of the person who was tricked.

METHOD

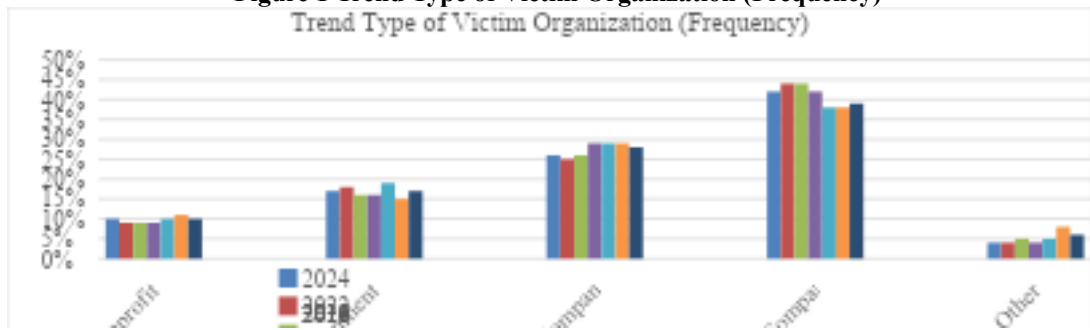
This research looks at how the kinds of people who get scammed have changed over the past decade. It gets its information from reports by the ACFE, which have been published every year from 2012 through 2024. A qualitative descriptive method is used to examine these profiling trends. By gathering information carefully from the ACFE reports, a full set of data is created for more in-depth analysis. To make sure the research is correct and trustworthy, they use a method called triangulation to see if the results match up and support each other. This method makes the research more trustworthy, as mentioned by Sugiyono in 2019. In this study, triangulation is done by including additional secondary data, like books and journal articles.

The researcher started the study by making a trend of fraud victim profiles around the world, using reports from the ACFE from 2012 up to 2024. This trend is made based on the features of an organization. Starting with the smallest companies and moving up to the largest ones, the different types of companies include public companies, private companies, non-profits, and government organizations. Next, the kind of business or industry the company is in, like banking, mining, or manufacturing, etc. Once the fraud victim profile trend is created, the next step is to apply the right anti-fraud measures for each company, based on that trend.

RESULTS AND DISCUSSION

This study investigates victim profile trends to identify the types of organizations targeted by fraudsters, including company size, industry type, and anti-fraud programs implemented. The "Report to the Nation" provides a comprehensive analysis of actual occupational fraud cases reported by the ACFE.

Figure 1 Trend Type of Victim Organization (Frequency)



According to the data in Figure 1, profit-oriented organizations have experienced a higher frequency of fraud cases compared to non-profit organizations over the past ten years. Public and private companies are the most affected, while non-profit organizations experience fewer fraud cases. This suggests that the likelihood of fraud is lower in non-profit and government organizations than in public and private companies.

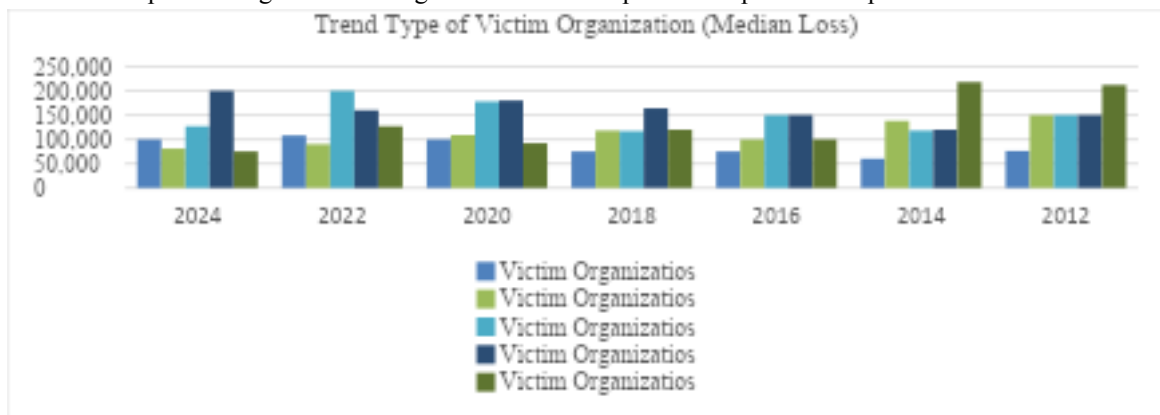


Figure 2 Trend Type of Victim Organization (Median Loss)

Looking at Figure 2, it's clear that businesses and government agencies that focus on making profits are more likely to face fraud and lose more money on average. Private companies usually experience the highest average loss when compared to other types of organizations. The main reasons for a lot of fraud in businesses that are focused on making money are usually pressure and the opportunity to commit fraud. Pressure comes when companies set financial targets that are too difficult to reach. This makes workers feel like they have to lie or cheat in order to meet those goals. At the same time, the risk of fraud can happen when there are weak internal controls and not enough teamwork between people inside and outside the organization. Besides that, the Fraud Diamond Theory suggests that people who work in these companies often have more knowledge about money issues, which makes them more likely to engage in fraudulent behavior (Kranacher & Riley, 2020).

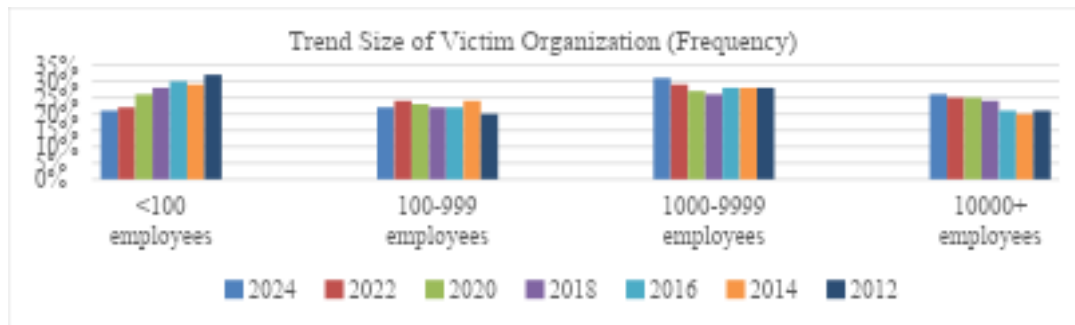


Figure 3 Trend Size of Victim Organization (Frequency)

Figure 3 shows that an organization's vulnerability to occupational fraud is highly influenced by its size. Smaller organizations, with 100 employees or less, are at higher risk of fraud compared to larger organizations. Data from 2012 to 2018 indicates that fraud cases are most common among organizations with less than 100 employees. Conversely, large organizations with more than 10,000 employees experienced the third-highest number of fraud cases during the same period.



Figure 4 Trend Size of Victim Organization (Median Loss)

Figure 4 shows that smaller companies usually have higher total average losses than bigger companies when looking at the median loss. Looking at profiles of people who were victims of fraud, it shows that most fraud cases in the past ten years happened in companies that had fewer than 100 workers. These small organizations end up losing the most money because of fraud when compared to bigger companies. The opportunity factor is seen as the main reason fraud happens in small companies, according to the Fraud Triangle Theory and Fraud Diamond Theory.

Small businesses are easier targets for fraud because they often lack strong internal controls. Because there aren't enough people or money, it's hard to set up strong control systems that can prevent fraud from occurring. According to the ACFE in 2022, this often causes owners or executives to trust their employees more than they should, especially when there's a close personal relationship. Because of this, managers may give many tasks to workers, which can lead to more opportunities for dishonest actions. When a company doesn't have strong internal controls and supervision, and when they hire people poorly, it becomes simpler for fraud to occur in small businesses (Bunn et al., 2019). Even though strong anti-fraud programs can prevent fraud, the high cost might make small companies avoid them since they trust their employees a lot, which leaves them more likely to be cheated.

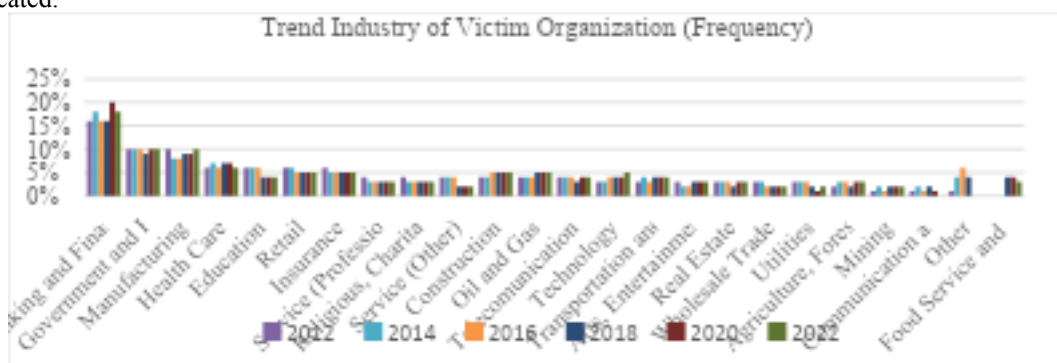


Figure 5 Trend Industry of Victim Organization (Frequency)

Figure 5 illustrates how various industries face different amounts of risk related to workplace fraud. In the last ten years, the financial and banking industries have had more cases of workplace fraud than any other sectors. In the last ten years, the financial and banking industries have experienced the most frequent kind of fraud done by workers, which creates a big danger that can be really harmful if not managed properly (Kranacher & Riley, 2020). The banking sector is vulnerable to internal issues, so it requires unique methods to handle risks in order to prevent fraud and keep the business running smoothly (Suh et al., 2019). The financial and banking sectors are facing major issues, such as corruption coming from within the organizations themselves, as found by Ben Ali et al. in 2020. Corruption here is closely tied to the bank's main role of distributing money. This threat comes from two sides. On the supply side, bank employees might receive money to approve risky loans. Some people who take out loans may give gifts to workers to avoid being punished if they are unable to repay the money they borrowed.

Corruption in the financial and banking sectors can eventually stop things from working smoothly, as found by Ben Ali and others in 2020. So, the best way to prevent fraud is by using a system that detects suspicious transactions, called a Fraud Detection System. This system uses technology like real-time fraud detection, analyzing user behavior, and monitoring transactions to spot unusual activities such as money laundering or tampering with data. This system can suggest things to do, like stopping a transaction, letting someone know about it, or starting a deeper check. Moreover, it's really important to use Know Your Customer (KYC) and Anti-Money Laundering (AML) processes to properly identify customers and keep track of their transactions. This helps stop money laundering and other illegal financial activities, as stated by the Basel Committee on Banking Supervision in 2001.

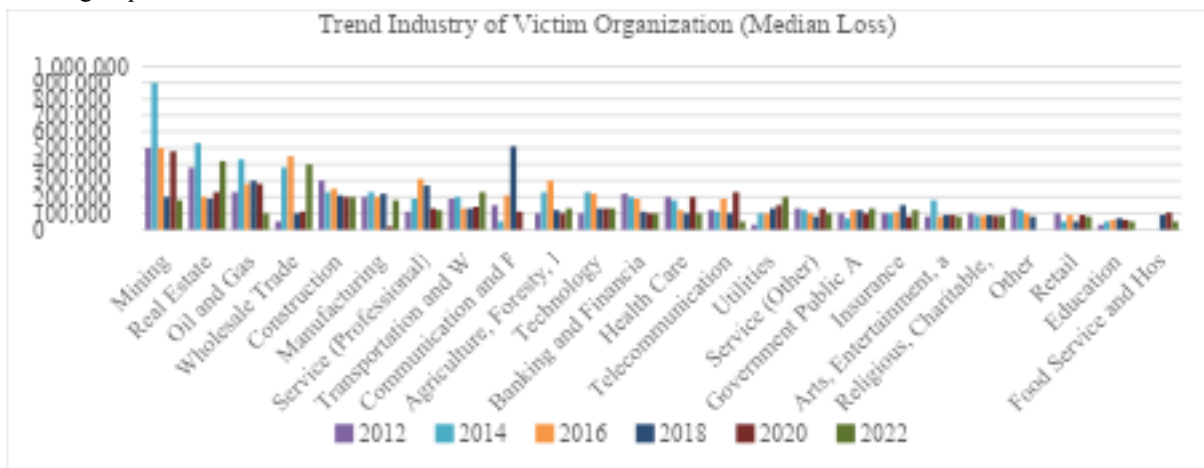


Figure 6 Trend Industry of Victim Organization (Median Loss)

Figure 6 shows the mining industry has the highest median loss despite having the lowest frequency of workplace fraud incidents from 2012 to 2022. This industry faces a high risk of fraud, especially in the form of production data manipulation, asset theft, bribes, and corruption. Therefore, anti-fraud controls must be adapted to the operational and geographical characteristics of this industry. The recommended control is the application of a Risk-Based Internal Control system, with a special focus on key risks in the mining sector, such as managing mining output, logistics, and procurement. Control over logistics and procurement is implemented through operational and physical, periodic inventory audits of the mining process, mineral stock, and heavy equipment management to prevent theft, production data manipulation, or false reporting. The mining industry has a high risk of fraud, especially in the form of production data manipulation, asset theft, bribes, and corruption. Therefore, anti-fraud control must be adapted to the operational and geographical characteristics of this industry.

In addition to risk-based internal controls, digital technology is crucial for preventing the risks of asset theft and production data manipulation. This technology includes the use of real-time IoT (Internet of Things) systems for long-distance production monitoring, which also increases cost efficiency and productivity. Furthermore, whistleblower systems and work ethics must be strengthened, particularly since many mines are located in remote areas. Companies should provide safe and easily accessible reporting channels and offer ethics and integrity training. A well-managed whistleblower system must be capable of conducting safe investigations, providing fair punishment to perpetrators, and protecting the reporter's privacy, thereby encouraging employees to report violations without hesitation. Generally, robust internal control is a primary concern for every company, which involves three lines of defense: operational management, the compliance monitoring function, and the internal auditor.

The anti-fraud control that every company needs to pay attention to is internal control. According to The Institute of Internal Auditor (2013), the responsibility for implementing risk management and internal control falls on 3 (three) lines of defense within the organization. Operational management is the first line of defense, fully responsible for running all organizational policies by continuously implementing internal control at all

stages of activities. The second line of defense is tasked with monitoring and maintaining compliance with the implementation of internal control and providing input to the first line. The third line of defense is the internal auditor, tasked with providing an assessment and objective monitoring of internal control.

Improving organizational culture is an important thing that companies must do to prevent fraud (Wicaksono and Urumsah 2016). The implementation of reward and punishment systems are equally important to encourage employees to improve the quality of their performance. Anti-fraud socialization and education aim to build an individual's ability to make ethical and integrity-driven decisions, and to foster an organizational culture that does not tolerate fraudulent acts.

CONCLUSION

Based on the analysis of trends in fraud victim profiling, several key findings emerged: private and public companies, especially smaller organizations (with employees), are the most frequently targeted victims of fraud and bear the most significant losses, generally due to weak internal controls. Meanwhile, based on industry, the financial and banking sector has the highest fraud frequency, demanding specific risk management, while the mining industry incurs the highest average loss. To mitigate these risks, companies are advised to focus on strengthening internal controls, organizational culture, implementing a reward and punishment system, and anti-fraud socialization and education. The results of this study are expected to have significant implications for organizations across various industries and sizes. These findings can help organizations improve their internal controls to prevent occupational fraud and reduce the losses it can cause. The profiling trends can also be used to develop fraud prevention and detection programs within organizations as part of their broader strategy. Finally, there are several limitations to this study. This research focused on occupational fraud and analyzed global trends in fraud victims over the last decade. Based on the limitations of this study, several suggestions can be made for future studies. First, future research should consider the limitations of this study and use them as a point of innovation for their studies. Second, future analysis can expand the profiling analysis by incorporating non-occupational fraud and increasing the duration of the trend analysis.

REFERENCES

- ACFE. (2012). *Report to the Nations on Occupational Fraud and Abuse*.
- ACFE. (2014). *Report to the Nations on Occupational Fraud and Abuse*.
- ACFE. (2016). *Report to the Nations on Occupational Fraud and Abuse*.
- ACFE. (2018). *Report to the Nations on Occupational Fraud and Abuse*.
- ACFE. (2020). *Report to the Nations on Occupational Fraud and Abuse*.
- ACFE. (2022). *Occupational Fraud 2022: A Report To The Nations*.
- ACFE. (2024). *Occupational Fraud 2022: A Report To The Nations*.
- Basel Committee on Banking Supervision. (2001). Disclosure survey
- Ben Ali, M. S., Fhima, F., & Nouira, R. (2020). How does corruption undermine banking stability? A threshold nonlinear framework. *Journal of Behavioral and Experimental Finance*, 27, 100365. <https://doi.org/10.1016/j.jbef.2020.100365>
- Bunn, E., Ethridge, J., & Crow, K. (2019). Fraud in Small Businesses: A Preliminary Study. *Journal of Accounting and Finance*, 19(3). <https://doi.org/10.33423/jaf.v19i3.2030>
- Christian, N., Fedelia, J., Te, J., & Vellin, M. (2023). Analisis kasus PT. Asabri (Persero) dengan teori dasar fraud. *Jurnal Multilingual*, 3(3), 315–329.
- Deliema, M., Shadel, D., & Pak, K. (2020). Profiling Victims of Investment Fraud: Mindsets and Risky Behaviors. *Journal of Consumer Research*, 46(5), 904–914. <https://doi.org/10.1093/jcr/ucz020>
- Kranacher, M.-J., & Riley, R. A., Jr. (2020). *Forensic Accounting and Fraud Examination* (2nd ed.).
- Prasetyo. (2014). Pengaruh Karakteristik Komite Audit dan Perusahaan Terhadap Kecurangan Pelaporan Keuangan. *Jurnal Akuntansi dan Auditing*, vol. 11, no. 1, pp. 1-24, Nov. 2014.
- Sofianti, Wardayat, S., Liyati, E., & MS, A. (2020). Profiling Selebriti Fraud: Analisis Profil Koruptor di Indonesia. *Jurnal Akuntansi Dan Pajak*, 20. <https://doi.org/10.29040/jap.v20i2.874>
- Sugiyono. (2019). *Metode Penelitian Kuantitatif, Kualitatif, dan R&D* (2nd ed.). Alfabeta.
- Suh, J. B., Nicolaidis, R., & Trafford, R. (2019). The effects of reducing opportunity and fraud risk factors on the occurrence of occupational fraud in financial institutions. *International Journal of Law, Crime and Justice*, 56(June 2018), 79–88. <https://doi.org/10.1016/j.ijlcj.2019.01.002>
- The Institute of Internal Auditor. (2013). *Internal Auditor Magazine*
- Wicaksono, AP., dan D. Urumsah. (2016). Factors Influencing Employees To Commit Fraud In Workplace Empirical Study In Indonesian Hospitals. *Asia Pasific Fraud Journal* Volume 1 No.1: 1-18. doi: 10.21532/apfj.001.16.01.01.01