



Anti-Fraud and Anti-Money Laundering: Proactive Detection Using Artificial Neural Networks with the Fraud Hexagon Approach to Strengthen the Stability of Indonesia's Financial Ecosystem

Kus Larisa Nathania Zita¹, Maureen Cahayli², Najwa Salsabila Azzahra³, Fatkhur Rohman^{4*}

¹⁻⁴ Accounting Department, Faculty of Economics and Business, Universitas Lampung, Indonesia

*Corresponding Author: fatkhurrohman@feb.unila.ac.id

Abstract. Fraud often serves as the initial stage before progressing to money laundering, making it a crucial global financial issue. Such fraudulent practices continue to occur in Indonesia, as reflected in the country's Corruption Perception Index score of 34/100 in 2022. This concern is further supported by a 2023 report from PPATK, which revealed more than 51,000 suspicious transactions with potential links to money laundering crimes (TPPU). In contrast, developed countries such as Singapore have managed to address fraud and money laundering by leveraging technological innovations, particularly detection tools based on artificial intelligence such as Artificial Neural Networks (ANN). The Association of Certified Fraud Examiners (ACFE) has also highlighted that 40% of fraud and money laundering cases stem from weak proactive detection by internal parties and regulators. The use of proactive detection technologies like ANN enables financial data to be updated in real time and suspicious patterns to be identified at an early stage. The primary advantage of ANN lies in its ability to detect suspicious transactions that conventional methods fail to recognize, thereby reducing the likelihood of fraud before it escalates into money laundering. Given the proven effectiveness and superiority of this detection system, it is recommended that the Financial Services Authority (OJK) enforce regulations requiring companies with annual revenues of $\geq$ Rp50 billion to adopt ANN-based mechanisms as an initial step to weaken fraud and prevent money laundering. This measure is expected to foster sustainable stability within Indonesia's financial ecosystem.

Keywords: Artificial Neural Network; Financial; Fraud; Money Laundering; Regulation.

1. BACKGROUND

Fraud in financial reporting is one of the forms of corporate crime that continues to rise in the Asia-Pacific region, including Indonesia. Between January 2022 and September 2023, the Asia-Pacific recorded 183 fraud cases, with an average loss of USD 575,000 per case. The region exhibits a high incidence of fraud but low reporting rates, indicating weaknesses in companies' internal early detection systems. This condition is dangerous because financial reports serve as the basis for stakeholders' decision-making. Moreover, the ACFE report highlights that 43% of detected fraud cases were uncovered through whistleblower reports, while internal audits and management reviews accounted for only about 27% of detections (ACFE, 2022; Wibisono, 2023). These facts reveal a significant gap in fraud detection systems, which have not yet been adequately supported by the application of robust and advanced technology.

With data manipulation in financial reporting still prevalent, audits can be strengthened through the Hexagon Theory framework (Voisinias, 2019), which encompasses stimulus, opportunity, rationalization, capability, arrogance, and collusion. Adequate and advanced digital detection systems—one of which is based on Artificial Neural Networks (ANN)—are

urgently needed for companies to enhance governance, detect fraud, and support OJK regulations in preventing fraud and money laundering, thereby fostering greater stability in Indonesia's financial ecosystem. Several studies have noted that ANN has been effectively applied to detect fraud in digital payment systems such as credit cards. However, recent trends indicate that ANN also holds significant potential for detecting anomalies in digital transaction recording systems, which are now widely adopted by large corporations across various countries. With algorithms capable of recognizing irregular transaction patterns in real time and analyzing correlations among financial variables often overlooked by conventional approaches, fraud detection systems can respond more adaptively to complex patterns. This makes ANN a highly relevant tool in digital-based financial supervision.

Nevertheless, Indonesia currently lacks specific regulations that mandate the adoption of digital recording systems as a core foundation of internal oversight, particularly for companies at high risk of fraud. Vulnerable entities are typically those with annual revenues exceeding Rp50 billion (based on the classification of large enterprises by the Ministry of Investment/BKPM), as the high volume of transactions creates broader opportunities for manipulation. Although POJK No. 12/POJK.01/2017 on the implementation of anti-fraud programs provides a general framework, no derivative regulation explicitly requires digital ERP systems as a prerequisite for automated detection mechanisms such as ANN.

Therefore, in this paper we propose regulatory updates to complement POJK No. 12 of 2024 by requiring companies with annual revenues above Rp50 billion to implement digital accounting systems (ERP/QuickBooks, etc.). This stage serves as the foundation for enabling automatic fraud detection through Artificial Neural Networks (ANN). ANN would be utilized to detect anomalies in financial transactions—both internal and external—in real time. Furthermore, as an incentive, companies that adopt this system and are proven to be free from fraud could receive option-based rewards, such as:

- a. Fraud-free certification from OJK for state-owned enterprises (BUMN) or publicly listed companies;
- b. Tax reductions for private entities;
- c. Priority funding/partnership opportunities for startups or pre-IPO entities.

This regulation is expected not only to serve as an effective fraud detection tool but also to promote accountability and strengthen public trust in business entities in Indonesia.

2. THEORETICAL STUDY

According to POJK No.12/POJK.01/2017, fraud is defined as any deliberate act of deception, manipulation, or concealment of information intended to mislead financial service providers, consumers, or other parties. Forms of fraud include corrupt practices such as abuse of authority, bribery, receipt of illegal gratuities, and coercive actions that harm institutions or customers. In addition, asset misappropriation—such as theft of cash, inventory, and manipulation of financial statements to mislead stakeholders—also falls under the category of fraud.

Within the fraud hexagon framework, six elements form the basis of fraudulent behavior: pressure, opportunity, rationalization, arrogance, capability, and collusion. Each has been shown to significantly influence financial statement fraud. Rationalization is reflected in practices such as the replacement of external auditors (Sagala, 2021; Poppy et al., 2023; Hartadi, 2022), while capability is evident in changes of directors that expose system vulnerabilities (Poppy et al., 2023). Arrogance is measured by the number of CEO photographs in annual reports, symbolizing the superiority of perpetrators who believe they cannot be caught due to their position or intelligence, thus daring to manipulate financial statements with schemes that are difficult to trace (Nadhiya et al., 2023; Octani et al., 2022). Collusion, proxied through government project cooperation, demonstrates the involvement of external parties in fraudulent practices (Sari & Nugroho, 2020).

In Indonesia's financial system, challenges remain in accurately and in real time detecting suspicious transactions. Money laundering, defined in POJK No.12/POJK.01/2017 as efforts to disguise the origin of funds derived from criminal activities, has become increasingly complex, particularly with the rise of financial technologies such as crypto assets. Although POJK No.8/POJK.04/2023 has strengthened oversight of AML-CFT (Anti-Money Laundering and Countering the Financing of Terrorism), its effectiveness remains weak. Therefore, a digital system capable of adaptively, automatically, and reliably detecting suspicious transaction patterns is urgently needed.

One proposed solution is the implementation of detection systems based on Artificial Neural Networks (ANN). This technology enables the processing of large volumes of transaction data in real time and adapts to emerging patterns, thereby detecting suspicious transactions that conventional methods fail to identify.



Figure 1. Working Mechanism of ANN.

In efforts to strengthen the stability of Indonesia's financial ecosystem, the use of Artificial Neural Networks (ANN) as a proactive detection tool against fraudulent transactions has become an increasingly relevant strategy. The integration of the Fraud Hexagon approach into ANN architecture enables the system not only to detect anomalies technically, but also to consider human and structural factors underlying fraudulent behavior. The detection process begins with the collection of transaction data, which involves gathering information from various sources such as banking transaction systems, e-commerce platforms, and companies' internal financial systems. The collected data includes transaction values, time, frequency, location, user identity, and the devices used. Following this, the data enters the processing stage, which consists of data cleaning, normalization, handling of missing values, encoding of categorical variables.

The next stage is feature extraction, where the system identifies relevant fraud indicators, including the six main elements of the Fraud Hexagon: pressure, opportunity, rationalization, capability, ego, and collusion. In addition, technical features such as transaction frequency, account relationships, and transaction timing are also analyzed as supporting variables.

The selected features are then fed into the ANN model, which consists of an input layer, several hidden layers, and an output layer, all interconnected through specific weights that are continuously updated during the training process. The model is trained using labeled historical data (fraud vs. non-fraud). Through the backpropagation mechanism, ANN adjusts these weights based on the error rate until the model achieves optimal accuracy.

After the training is completed, the model is used to probabilistically predict potential fraud in transactions, allowing the system to set certain thresholds according to the required sensitivity of detection. If the model detects potential fraud, the system will generate an output in the form of an early warning, either as a notification to the compliance team or as automatic blocking of suspicious transactions. Transactions identified as anomalies are then followed up through internal investigations, reporting to relevant authorities such as PPATK and OJK, and legal measures in accordance with Indonesia's Anti-Money Laundering (AML) and Anti-Fraud regulations. By combining the sophistication of ANN with the behavioral depth of the Fraud Hexagon, this approach creates a system that is responsive, adaptive, and resilient in addressing risks of fraud and money laundering. Broad implementation of this system is believed to strengthen public trust and safeguard the integrity of the national financial system.

3. METHOD

This study employs a conceptual approach and comparative analysis based on regulatory review, international case studies, and limited simulations, with the aim of exploring the potential application of Artificial Neural Networks (ANN) as an innovative regulatory technology tool to prevent fraud and money laundering in the financial sector, particularly in large companies. The study emphasizes a descriptive and analytical approach without directly testing hypotheses, but instead proposes conceptual solutions for OJK. The analysis is grounded in findings and insights drawn from existing academic literature, regulations from institutions such as OJK and the Financial Transaction Reports and Analysis Center (PPATK), as well as relevant global case studies where ANN has been applied for financial prediction and fraud detection. The combination of these sources provides a comprehensive foundation for designing the proposed system framework.

In this study, supporting data will also be collected through simulations using open-source financial transaction datasets to illustrate how the proposed system (ANN) operates in practice. The system design will adopt the Fraud Hexagon framework as an input mapping tool, in which financial reports are categorized into six key elements (stimulus, opportunity, rationalization, capability, arrogance, and collusion) before being processed through ANN layers (input, hidden, and output) to generate a probability score of fraud or money laundering. Comparative simulations will then be conducted to demonstrate the potential impact of implementing this digital detection software compared to conventional methods, with a focus on companies with annual revenues above Rp50 billion as the benchmark, since companies of this scale have larger and more diverse transaction volumes, thereby increasing the likelihood

of fraud. Entities at this level also have sufficient capacity to implement fraud detection technology without disrupting operational continuity. The results are expected to serve as a basis for designing regulatory recommendations that support the mandatory use of advanced digital monitoring systems for fraud prevention.

4. RESULTS AND DISCUSSION

Table 1. Summary of AI/ML (ANN) Implementation in Fraud and AML Detection.

No	Aspect	Key Findings	Quantitative Evidence	Implications
1	Detection Effectiveness	Artificial Neural Networks (ANN) are more effective than conventional rule-based systems in detecting fraud and AML patterns.	—	Improves detection accuracy and adaptability to evolving risk patterns.
2	Cost Efficiency	AI/ML-based systems significantly reduce compliance and operational costs.	Up to 60% reduction in compliance costs (Tookitaki, 2024; Silent Eight, 2025).	Enhances long-term financial efficiency and reduces operational burden.
3	False Positive Reduction	ANN reduces false positives compared to traditional systems.	40% decrease in false positives (Silent Eight, 2025).	Minimizes unnecessary investigations and reputational risk.
4	Fraud Risk Exposure	Systemic fraud risk without proactive detection is substantial.	3–7% of total U.S. federal expenditures (USD 233–521 billion annually) (GAO, 2024).	Highlights urgency of automated proactive detection systems.
5	Real-Time Processing Capability	ANN can process large transaction volumes with high speed and precision.	Processes up to 160 billion transactions per year in <50 milliseconds (Mastercard Decision Intelligence).	Enables real-time fraud prevention at global scale.
6	Revenue–Fraud Correlation	Higher company revenue correlates with higher fraud and AML risk.	Companies ≥ Rp50 billion annual revenue show higher transaction complexity (ACFE, 2022).	Supports regulatory threshold for mandatory digital system adoption.
7	Global Adoption Trend	AI/ML adoption in AML processes is rapidly increasing worldwide.	>60% financial institutions currently; projected 90% by 2025 (Sanctions.io, 2025; Silent Eight, 2025).	Digital transformation is becoming a regulatory and strategic necessity.

The use of software based on Artificial Intelligence (AI) and Machine Learning (ML), particularly Artificial Neural Networks (ANN), has proven to be a far more effective approach

in detecting fraud and anti-money laundering (AML) compared to conventional methods. ANN provides long-term added value through significant cost efficiency, as it can operate without the need for continuously creating new rules, thereby saving costs related to detection scenario development, manual training, and routine supervision. In addition, ANN reduces potential costs arising from detection errors, such as additional investigation expenses or reputational losses due to oversight. With continuous learning mechanisms and high scalability, ANN not only reduces dependence on human labor in investigations and audits but also produces more accurate and adaptive detection in response to changing risk patterns.

Implementation analysis of AI/ML-based digital systems has been shown to reduce compliance costs by up to 60% and decrease false positives by 40% (Tookitaki, 2024; Silent Eight, 2025). This has a direct impact on improving the accuracy of financial reporting as well as accelerating investigation and audit processes. Conversely, without digital system support, companies are vulnerable to delays and errors in reporting, which may result in fines and reputational damage (GAO, 2024). A study by the Government Accountability Office (GAO) also revealed that systemic fraud risks can reach 3–7% of total U.S. federal expenditures, equivalent to \$233–521 billion annually. If this condition is analogized to the private sector, the potential losses from fraud become highly significant, especially in the absence of proactive automated detection systems capable of identifying implicit fraud.

In real-time transaction fraud detection practices, ANN demonstrates particular advantages in environments with large data volumes and continuous monitoring needs. ANN can learn highly complex and non-linear behavioral patterns, such as anomalies in transaction timing, account relationship patterns, or override approval patterns, which are difficult to capture using traditional rule-based methods. For example, Mastercard's Decision Intelligence system, which employs ANN, is capable of processing up to 160 billion transactions per year in real time within less than 50 milliseconds. This system has been proven to drastically reduce false positives and improve fraud detection accuracy on a global scale.

Furthermore, data shows a positive correlation between company revenue and fraud potential, where companies with annual revenues of $\geq$ Rp50 billion tend to have more complex transaction volumes and higher risks of fraud and money laundering (ACFE, 2022). Therefore, the revenue threshold of Rp50 billion can serve as an initial hypothesis to encourage regulatory intervention, such as mandating the adoption of digital systems in large-scale companies. Global trends further reinforce this urgency, with more than 60% of financial institutions already implementing AI/ML in AML processes, a figure projected to rise to 90% by 2025 (Sanctions.io, 2025; Silent Eight, 2025). Digital transformation is thus no longer an option, but

a necessity to safeguard the integrity of the national financial system.

Artificial Neural Networks (ANN) have the ability to learn and recognize highly complex and not always explicit data patterns, including transactions that appear normal but actually contain hidden anomalies. ANN works adaptively by adjusting internal parameters, enabling the system to identify suspicious transactions that escape detection by conventional methods. This characteristic makes fraud detection systems more proactive. In addition, ANN is responsive to new *modus operandi*, which often change dynamically in the modern financial world. Thus, ANN is not only effective in detecting previously known fraud but also functions as a self-learning system capable of significantly reducing fraud risks through continuous monitoring and real-time data analysis.

As a form of technological investment, the implementation of ANN offers a combination of cost efficiency and improved fraud detection accuracy, making it a strategic solution for safeguarding transaction integrity within an increasingly complex and rapidly evolving financial ecosystem. ANN systems developed with the Fraud Hexagon approach have proven capable of accurately detecting fraud and money laundering practices through analysis of transaction patterns, audit trails, and user metadata. Amid rising digitalization, fraud risks have also increased, yet mitigation efforts remain suboptimal due to low adoption of automated detection systems. In this context, digitalization of financial reporting becomes a crucial aspect in supporting early detection and enhancing the accuracy of corporate financial reporting.

Therefore, it is recommended that the Financial Services Authority (OJK) encourage regulations requiring the use of digital software for financial reporting based on Artificial Neural Networks (ANN) in companies with annual revenues of $\geq$ Rp50 billion as an initial step. Such software should meet minimum standards, including the presence of audit trails, automatic detection capabilities, and comprehensive integration of financial reports. Implementation of this policy could be articulated through revisions or expansions of POJK No.13/POJK.02/2018 on the Application of Risk Management in the Use of Information Technology by Financial Service Institutions, and reinforced in POJK No.12/POJK.01/2017 on the Implementation of Anti-Money Laundering and Counter-Terrorism Financing Programs. Adding provisions related to the mandatory use of digital systems and ANN integration in financial reporting could become part of a national anti-fraud strategy that is adaptive in the digital era.

5. CONCLUSION AND SUGGESTIONS

Artificial Neural Networks (ANN) demonstrate strong capability in proactively detecting fraud and money laundering by recognizing complex, implicit transaction patterns through adaptive and continuous learning mechanisms. Compared to conventional methods, ANN-based systems are more responsive to evolving fraud schemes, reduce detection errors, and enhance real-time monitoring effectiveness. When integrated with the Fraud Hexagon approach, ANN not only improves the accuracy of fraud identification through analysis of transaction patterns, audit trails, and user metadata, but also strengthens the integrity of financial reporting in an increasingly digital financial ecosystem. Therefore, regulatory encouragement—particularly by the Otoritas Jasa Keuangan (OJK)—to mandate ANN-based digital financial reporting systems for companies with annual revenues of $\geq$ Rp50 billion would represent a strategic and adaptive step toward reinforcing national anti-fraud frameworks and ensuring long-term financial system stability.

REFERENCE

- Association of Certified Fraud Examiners. (2024). *Occupational fraud 2024: A report to the nations*. Association of Certified Fraud Examiners.
- Chandra, C., Khalila, S. Z., Sinaga, R. R., & Prasetya Mulya, U. (2023). Fraudulent financial reporting analysis using fraud diamond theory in Indonesia manufacturing industry. *Jurnal Riset Akuntansi dan Auditing*, 10(3), 27–44. <https://doi.org/10.55963/jraa.v10i3.579>
- Cressey, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement*. Free Press.
- Crowe Horwath. (2011). *Why the fraud triangle is no longer enough: The fraud pentagon*. Crowe Horwath LLP.
- Dechow, P. M., Sloan, R. G., & Sweeney, A. P. (1996). Causes and consequences of earnings manipulation: An analysis of firms subject to enforcement actions by the SEC. *Contemporary Accounting Research*, 13(1), 1–36. <https://doi.org/10.1111/j.1911-3846.1996.tb00489.x>
- Dorris, B. (2022). *Occupational fraud 2022: A report to the nations*. Association of Certified Fraud Examiners.
- Firly, Z. M., & Sutoyo. (2025). Pengaruh fraud hexagon terhadap financial statement fraud (Studi pada perusahaan sektor infrastruktur yang terdaftar di Bursa Efek Indonesia). *Jurnal Akuntansi*, 12(1), 41–60. <https://doi.org/10.25105/v12i1.22145>
- Hastuti, P. M. D., Rahayu, S., & Pratiwi, E. C. (2023). Fraud pentagon theory terhadap kecurangan laporan keuangan di sektor perusahaan manufaktur. *Jurnal Ekobistek*, 12(2), 614–621. <https://doi.org/10.35134/ekobistek.v12i2.602>
- Marks, J. (2012). *The mind behind the fraudsters crime: Key behavioral and environmental elements*. Crowe Horwath LLP.

- Octani, J., Dwiharyadi, A., & Djefris, D. (2022). Analisis pengaruh fraud hexagon terhadap fraudulent financial reporting pada perusahaan sektor keuangan yang terdaftar di Bursa Efek Indonesia selama tahun 2017–2020. *Jurnal Akuntansi, Bisnis dan Ekonomi Indonesia (JABEI)*, 1(1), 36–49. <https://doi.org/10.30630/jabei.v1i1.9>
- Otoritas Jasa Keuangan. (2014). *Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2014 tentang penerapan strategi anti fraud bagi lembaga jasa keuangan*. Otoritas Jasa Keuangan.
- Otoritas Jasa Keuangan. (2017). *Peraturan Otoritas Jasa Keuangan Nomor 12/PJOK.01/2017 tentang penerapan program anti pencucian uang dan pencegahan pendanaan terorisme di sektor jasa keuangan*. Otoritas Jasa Keuangan.
- Otoritas Jasa Keuangan. (2018). *Peraturan Otoritas Jasa Keuangan Nomor 13/PJOK.02/2018 tentang inovasi digital di sektor jasa keuangan*. Otoritas Jasa Keuangan.
- Otoritas Jasa Keuangan. (2023). *Peraturan Otoritas Jasa Keuangan Nomor 08/PJOK.04/2023 tentang penerapan program anti pencucian uang, pencegahan pendanaan terorisme dan pencegahan pendanaan proliferasi senjata pemusnah massal di sektor jasa keuangan*. Otoritas Jasa Keuangan.
- Sagala, S. G., & Siagian, V. (2021). Pengaruh fraud hexagon model terhadap fraudulent laporan keuangan pada perusahaan sub sektor makanan dan minuman yang terdaftar di BEI tahun 2016–2019. *Jurnal Akuntansi*, 13(2), 245–259. <https://doi.org/10.28932/jam.v13i2.3956>
- Shea, R., & Smith, J. B. (2024). *Fraud risk management: 2018–2022 data show federal government loses an estimated \$233 billion to \$521 billion annually to fraud, based on various risk environments*. GAO Reports.
- Skousen, C. J., Smith, K. R., & Wright, C. J. (2009). Detecting and predicting financial statement fraud: The effectiveness of the fraud triangle and SAS No. 99. *Corporate Governance: An International Review*, 17(1), 53–81. [https://doi.org/10.1108/S1569-3732\(2009\)0000013005](https://doi.org/10.1108/S1569-3732(2009)0000013005)
- Trompeter, G. M., Carpenter, T. D., Desai, N., Jones, K. L., & Riley, R. A. (2013). A synthesis of fraud-related research. *Journal of Accounting Literature*, 32(1), 1–34. <https://doi.org/10.2308/ajpt-50360>
- Vousinas, G. L. (2019). Advancing theory of fraud: The fraud hexagon. *Journal of Financial Crime*, 26(1), 372–381. <https://doi.org/10.1108/JFC-12-2017-0128>
- Wibisono, W. (2023). Preliminary study on corruption case in the Indonesian banking sector: Overview of the fraudster, loss, and fraud modes. *Asia Pacific Fraud Journal*, 8(1), 31–. <https://doi.org/10.21532/apfjournal.v8i1.263>
- Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal*, 74(12), 38–42.