International Journal of Religion
2024
Volume: 5| Number 10 | pp. 2355 – 2367
ISSN: 2633-352X (Print) | ISSN: 2633-3538 (Online)
ijor.co.uk
DOI: https://doi.org/10.61707/h0tnfd21

Management of Antifraud in the Era of Banking Digitization

Ramon Arthur Ferry Tumiwa[1], Jan Horas Veryady Purba[2], Akhmad Nur Zaroni[3], Loso Judijanto[4], Gama Pratama[5], Alfiana[6], and Andiyan[7]

Abstract

This phenomena undoubtedly confers advantages onto financial services companies in Indonesia, notably by augmenting the degree of financial inclusion. Phenomenology is a research methodology that places significant emphasis on the act of observing. Within the realm of science, there exists a fundamental essence that underlies the concept of existence, a genuine reality that lies underneath surface appearances, and a profound knowledge of intentionality known as noema that is concealed behind observable occurrences. The result of the research showed that the approaches used by several banks have successfully satisfied the four primary components of the anti-fraud strategy as specified in Bank Indonesia Circular Letter No. 13/28/DPNP, according to the conclusions of this research. Nevertheless, the rapid integration of digital technology also has the risk of becoming harmful, due to the growing and varied dangers of financial crime. According to the 2020 Report to the Nations research conducted by the Association of Certified Fraud Examiners (ACFE), Indonesia has the highest number of financial fraud cases among the 16 Asia Pacific nations included in the study. Indonesia had 36 financial fraud instances in a year, surpassing China's 33 cases and Australia's 29 cases. The bank utilizes the dissemination of anti-fraud strategy materials, the endorsement of the anti-fraud declaration, and the establishment of the whistleblowing system to execute the four fundamental principles of the anti-fraud strategy. Financial institutions must have a fraud detection system capable of analyzing and identifying many forms of fraudulent activities.

Keywords: *Digital Technology, Anti-Fraud, Financial Crime, ACFE.*

INTRODUCTION

Security is a crucial issue when it comes to banking. Banking security include safeguarding both the client and highly confidential personal information. Financial institutions, including banks, establish anti-fraud departments with the specific responsibility of preventing, detecting, and managing any kind of fraudulent activity. In recent years, the integration of digital technology in the banking sector and other financial service providers has seen significant growth. This phenomenon is closely linked to the growing prevalence of internet access and tech-savvy mobile phone users in the nation(Bank Mandiri, 2022).

According to the 2020 Report to the Nations research conducted by the Association of Certified Fraud Examiners (ACFE), Indonesia has the highest number of financial fraud cases among the 16 Asia Pacific nations examined. Indonesia had a surge in financial fraud instances, with a total of 36 incidents within a year. This number surpasses both China's 33 cases and Australia's 29 difficulties(Lubis, Harahap, & Nuraini, 2021).

Previous research (Mohan, Rajasekar, & Agriyanto, 2023) The Fintech revolution has accelerated and democratized access to financial services. Due to advancements in technology, individuals with traditional

[1] Department of Management, Faculty of Economics and Business, Universitas Negeri Manado, Manado, North Sulawesi, Indonesia 95618. Email: ramontumiwa@unima.ac.id, Orcid: 0000-0001-9746-1732

[2] Department of Management, Faculty of Business, Institut Bisnis dan Informatika (IBI) Kesatuan,Bogor,West Java, Indonesia 16123. Email: janhorasvpurba@gmail.com, (Corresponding Author), Orcid: 0000-0002-8867-0214

[3] Department of Sharia Economics, Faculty of Economics and Islamic Business, Universitas Islam Negeri (UIN) Sultan Aji Muhammad Idris, Samarinda, East Kalimantan, Indonesia 75251. Email: akhmadnurzaroni@gmail.com, Orcid: 0000-0002-6094-237X

[4] Indonesia Palm Oil Strategic Studies (IPOSS), Bekasi,Indonesia 17131. Email: losojudijantobumn@gmail.com, Orcid: 0009-0007-7766-0647

[5] Department of Sharia Economics, Faculty of Economics and Islamic Business, Universitas Islam Bunga Bangsa Cirebon, Cirebon, Indonesia 45153. Email: gamapratama0@gmail.com, Orcid: 0000-0001-7530-4373

[6] Department of Management, Faculty of Economics and Business, Universitas Muhammadiyah Bandung, Bandung, West Java, Indonesia 40614. Email: alfiana.dr@umbandung.ac.id, Orcid: 0000-0003-4168-4763

[7] Department of Architecture, Faculty of Science and Engineering, Universitas Faletehan, Bandung, West Java, Indonesia 40192 E-mail: andiyanarch@gmail.com Orcid: 0000-0002-9999-5874

accounts may now do their routine banking tasks from any location. Additionally, financial transactions now need the use of financial technology. Smartphone applications and online technologies have made it possible for those without bank accounts to conveniently use crucial financial services, like peer-to-peer lending and digital payments. Based on the findings of earlier studies (Shaymardanov & Vavrenyuk, 2022), Numerous charges, transactions, and logins occur on a daily basis. We were assigned the responsibility of developing an anti-fraud system to facilitate decision-making during the processing of bank payments. This report delineates the many issues encountered by several enterprises worldwide on a regular basis. The text outlines the architectural aspects of the solution's design patterns, as well as addressing the system's fault tolerance and scalability concerns. Other prior investigators (Dewi, Suharman, Koeswayo, & Tanzil, 2023) The research findings indicate a strong and statistically significant relationship between digital security, fraud brainstorming, and compliance management in preventing credit card fraud. Specifically, the t-statistic values for these variables are 6.161, 5.079, and 5.98, respectively, at a significance level of 5%.In addition, the moderating effect was tested and resulted in t-statistic values of 7.330, 4.161, and 7.694. Competency outcomes that are positively and significantly influential modify the association between these characteristics and the prevention of credit card theft. These results have significant implications for the policies of financial institutions and government agencies aiming to combat credit card theft by deploying preventive techniques (Sehrawat, Kumar, Nigam, Singh, & Goyal, 2020).

The significance of this research lies in the digitalization of the financial services sector, driven by the advancement of technology in the current era. This has led to the transformation of conventional banking systems into digital platforms. However, the emergence of various digital banks that heavily rely on information technology has also resulted in an increase in fraudulent activities, causing financial losses for customers. Therefore, it is necessary to establish regulations that protect customers from fraud and ensure the feasibility and security of products and services in digital banking transactions. Additionally, digital banks must adhere to compliance requirements as organizers. The incidence of fraudulent activities in electronic banking is increasing annually. Cybercrime experts are constantly monitoring and validating network infrastructure and transaction systems. Organizations use dedicated Computer Security Incident Response Teams (CSIRTs) to safeguard security and counteract cyber assaults (Srokosz, Bobyk, Ksiezopolski, & Wydra, 2023).

The objective of the study is to examine the legal protection system overseen by the competent authority, with a focus on electronic risks and the implementation of management practices including the phases of prevention, detection, handling, and monitoring. Monitoring involves the supervision of the feasibility of Digital Bank transaction activity products and/or services by the competent authority in the Financial Services Sector. The effectiveness of protection and supervision is contingent upon the compliance of Digital Banks with the various provisions imposed on their operations (Bank BRI, 2021). An analysis was conducted on the antifraud systems market. An investigation was conducted on ensemble approaches for resolving classification problems, as well as ways for reducing dimensionality (Domashova & Zabelina, 2021).

RESEARCH METHODOLOGY

The research methodology used in this study is doctrinal research. The author employs this research methodology to examine regulations and written laws that pertain directly to the legal protection of customers, supervision of digital banks, and compliance by digital banks. In this doctrinal study, the author examines and evaluates the content of the law by using legal theories. Legal doctrines are used to discover, create, or rebuild rules or principles in the field of law. This study employs a descriptive-analytical typology, whereby the descriptive aspect tries to provide a detailed account of a certain subject within a given area and timeframe. In this case, the researcher focuses primarily on the topic of law At a certain point in time, the researcher has a comprehensive understanding of the topic to be investigated, based on the collection of original data.in the form of raw data pertaining to the topic under investigation. This research employs a statutory methodology, which involves examining all laws pertaining to the legal matters being investigated (Puluhulawa, Puluhulawa, & Swarianata, 2022).

RESULTS AND DISCUSSION

Are you aware that the majority of financial fraud occurs in the internet realm? According to the Financial Crime Report Q2 2021, about 93% of fraudulent activities connected to banking take place on the internet. Hence, it is essential for all financial institutions to endeavor in adopting an anti-banking fraud strategy, while simultaneously upholding the fundamental benefit of digital technology, which is an effortless and user-friendly client experience (Rohall, 2022).

Anti-Fraud Refers to Measures and Strategies Used to Prevent and Detect Fraudulent Activities

Banking anti-fraud encompasses a range of specialized approaches and procedures aimed at mitigating risk. Financial institutions are often targeted by fraudsters owing to their direct access to cash and their capacity to move them. Therefore, it is essential for banks and other financial institutions to possess cutting-edge and resilient fraud detection and prevention mechanisms in order to safeguard their assets, systems, and clientele. Fraud detection primarily concerns the identification of fraudulent activities carried out by individuals, while fraud prevention aims to hinder such activities from occurring in the first place. In practice, these two approaches are essentially interchangeable, since they are closely interconnected (Rohall, 2022).

The Significance of Anti-Fraud Measures in the Banking Sector

The function of anti-fraud measures in the banking industry is crucial, particularly in the context of technological advancements. Cyberfraud continues to be a significant obstacle encountered by consumers and financial organizations in the current digital age. The absence of appropriate decision support tools for efficient resource allocation hinders the effectiveness of crime prevention efforts (Akinbowale, Mashigo, & Zerihun, 2024).

Below are many crucial functions performed by anti-fraud measures in the banking industry:

Fraud Prevention

The main function of anti-fraud measures is to deter and thwart fraudulent activities. Financial institutions use sophisticated technologies to oversee transactions and detect anomalous tendencies.

Figure 1. Digital Bank Fraud Detection and Prevention

Source: finance-monthly.com

If there is any atypical or questionable transaction activity detected on a customer's account, the anti-fraud department will promptly address and resolve the issue.This study focuses on the creation of a technology that enhances access control efficiency by incorporating user behavior monitoring into a software system's user interface(Magomedov, Gusev, Ilin, & Nikulchev, 2021).

Early Detection

When fraudulent activities take place, the anti-fraud department is responsible for promptly identifying and detecting such actions. The task will be expedited to promptly halt the fraudulent activity and minimize financial damages.

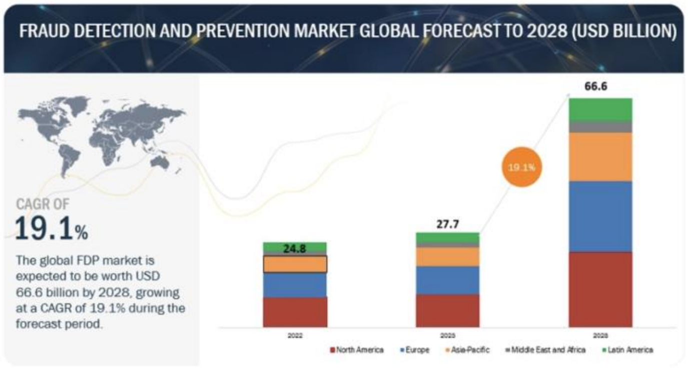


Figure 2. Attractive oppertunities in the fraud deetction and prevention market

Source: marketsandmarkets.com

Investigation

Upon detection of fraud, the anti-fraud department will proceed with further investigation. At this step, banks will gather evidence, identify the culprits, and cooperate with law enforcement agencies.

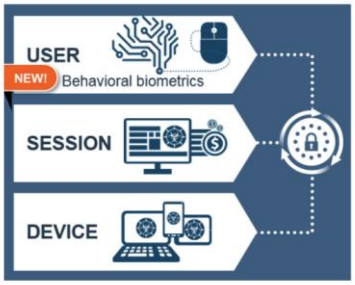


Figure 3. Digital Identity Fraud

Source: altoros.com

Compliance

Anti-fraud banks are also obligated to guarantee that the bank adheres to all regulatory and reporting requirements pertaining to financial crime.

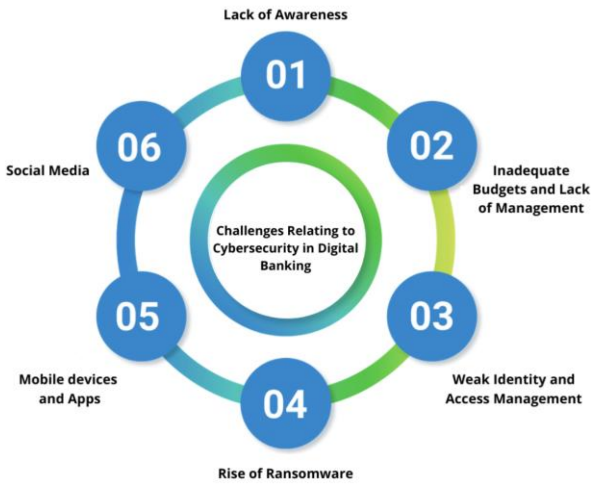

Challenges Relating to Cybersecurity in Digital Banking
01
Lack of Awareness
02
Inadequate Budgets and Lack of Management
03
Weak Identity and Access Management
04
Rise of Ransomware
05
Mobile devices and Apps
06
Social Media

Figure 4. The Challenges Relating to Cybersecurity in Digital Banking

Source: enterslice.com

Personal Data Protection

Anti-fraud measures also serve to safeguard customers' sensitive data. The anti-fraud team is responsible for ensuring the safe storage of client data, preventing illegal access.

Figure 5. Fraud Risk in a Digitized Fintech ecosystem

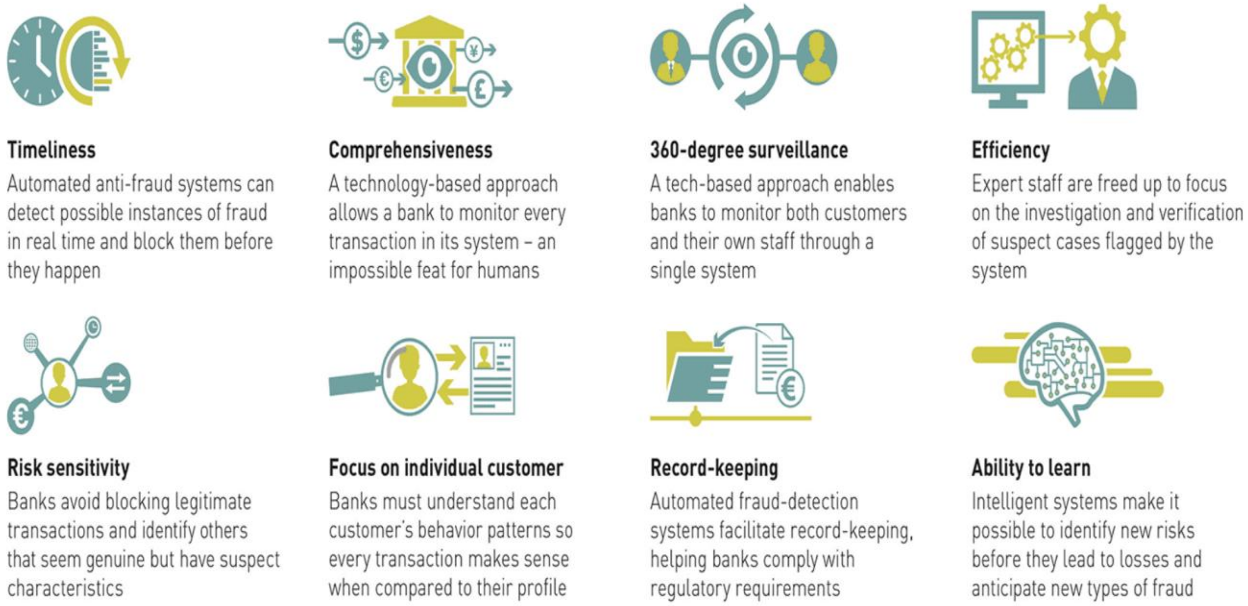
Source: in.worldline.com

Customer Education

Anti-fraud measures not only detect fraudulent activities but also contribute to educating customers about the hazards associated with fraud. The anti-fraud team disseminates information to clients about prevalent fraudulent practices used by criminals. Banks may mitigate the risks of fraud by enhancing client awareness.

Technology Security

The anti-fraud team works closely with the bank's IT department to enhance technological security. The anti-fraud team detects weaknesses in the financial system that may be used by criminals and seeks solutions to mitigate these risks.



Timeliness
Automated anti-fraud systems can detect possible instances of fraud in real time and block them before they happen

Comprehensiveness
A technology-based approach allows a bank to monitor every transaction in its system – an impossible feat for humans

360-degree surveillance
A tech-based approach enables banks to monitor both customers and their own staff through a single system

Efficiency
Expert staff are freed up to focus on the investigation and verification of suspect cases flagged by the system

Risk sensitivity
Banks avoid blocking legitimate transactions and identify others that seem genuine but have suspect characteristics

Focus on individual customer
Banks must understand each customer's behavior patterns so every transaction makes sense when compared to their profile

Record-keeping
Automated fraud-detection systems facilitate record-keeping, helping banks comply with regulatory requirements

Ability to learn
Intelligent systems make it possible to identify new risks before they lead to losses and anticipate new types of fraud

Figure 6. Eight reasons why it wins

Source: Net Guardians

Research and Development

The Anti-fraud department is actively engaged in research and development to create innovative methods and technology for detecting and preventing fraud. This is done with the aim of enhancing consumer comfort.

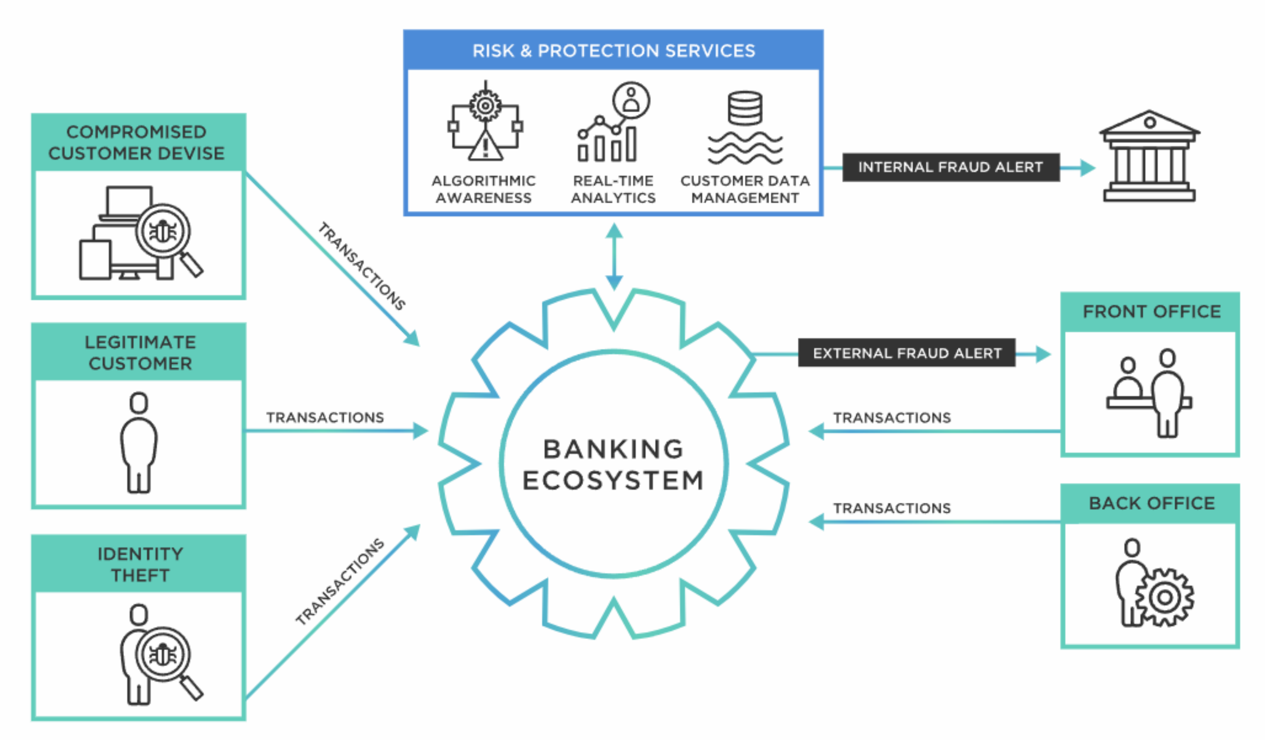


Figure 7. Banking Ecosystem

Source: tibco.com

The anti-fraud team collaborates with many entities, such as cybersecurity firms, to remain in the vanguard of combating criminal activities in the banking sector. Anti-fraud plays a crucial function in the banking industry by safeguarding the integrity of the banking system and shielding clients from many fraudulent dangers. Hence, combating fraud is a crucial element inside the banking industry within the digital age. The anti-fraud team has the responsibility of proactively preventing, identifying, and managing instances of financial fraud.

The anti-fraud team plays a crucial role in safeguarding the security and integrity of the financial system and ensuring the protection of clients via an effective strategy. Anti-fraud measures play a crucial role in the banking industry by ensuring the integrity of the financial system and safeguarding clients from a wide range of fraudulent threats(Bank Mandiri, 2022). Hence, combating fraud is a crucial aspect inside the banking industry within the digital age. The anti-fraud team has the responsibility of proactively preventing, identifying, and managing instances of financial fraud. By using an effective strategy, the anti-fraud team actively safeguards the security and integrity of the financial system, ensuring the safety of clients (Bank Mandiri, 2022). Ethics prevents societal strife. Thus, millennials must develop their character. Millennials must also adjust to Society 5.0. Society 5.0, which complements Industrial Revolution 4.0, should focus on the millennial generation's role in national growth. Society 5.0 is a technology-based human-centered society(Nurjamin et al., 2023).

The Primary Challenge Faced by Banks Is the Detection and Prevention of Large-Scale Fraudulent Activities

Bank fraud concerns may be broadly categorized into three main groups, which include:

Customer Orientation

Digital onboarding of new clients poses risks for banks, mostly owing to regulatory requirements like KYC (Know Your Customer) and AML (Anti Money Laundering). These are regulatory mandates aimed at verifying a user's identification and mitigating the risk of their engaging in financial malfeasance(Rohall, 2022). Criminals use counterfeit or artificially created identification documents to deceive the system and initiate the establishment of bank accounts. Verifying identification is a costly process, projected to reach a total expenditure of $35.2 billion by the year 2020. Neobanks and challenger banks have significant challenges in swiftly and effortlessly acquiring new clients (Rohall, 2022). Based on Wah and his discussion, he was surprised to find evidence of the studies developing Islamic economics and its principles, welfare, and economic democracy based on Pancasila (Guritno et al., 2023).

Credit Card Fraud Prevention

The bank must be informed promptly of any suspicious transaction or withdrawal. Identifying trends is challenging due to the restricted availability of data points, which are only comprised of currency, quantity, category, and merchant name (Rohall, 2022).

Implementing measures to prevent fraudulent payments based on these factors might result in a high proportion of false positives, causing frustration for legitimate cardholders. In addition, there are legal obligations, such as the implementation of Strong Customer Authentication (SCA), and the verification of the legitimacy of the money' origin (Rohall, 2022).

Account Protection

Account takeover refers to the unauthorized acquisition of login credentials belonging to genuine users by criminals. The unauthorized use of the account by individuals has detrimental effects on the bank's customer relations and facilitates many forms of fraudulent activities and criminal behavior (Rohall, 2022).

Hence, it is essential for banks to use every possible measure to safeguard their customers' accounts. To meet the needs of the public, the government has provided an official financial institution, which is subject to a certain series of administrations with all the calculations (Sungkawaningrum et al., 2022).

Furthermore, the overarching concern is that fraud exhibits adaptability. Consequently, fraudsters will promptly identify when their operations are obstructed and proceed to use other methods. Therefore, it is essential for solutions like as AML software and KYC systems to possess both versatility and efficiency (Rohall, 2022).

Strategy to Counteract Fraud in Digital Banking

As fraudsters become more sophisticated in their methods, banks should be cognizant of the following anti-fraud strategies:

Watch for Internal Fraud

To successfully prevent fraud, begin the process by thoroughly screening and auditing the staff of your firm. It is possible that some personnel whom you consider reliable may be illicitly trading client account information on underground online platforms. It is imperative that you treat this matter with utmost seriousness. Microsoft research indicates that groups such as LAPSUS$, an expanding faction of cybercriminals, are progressively infiltrating target firms by recruiting personnel in return for financial compensation (Rohall, 2022).

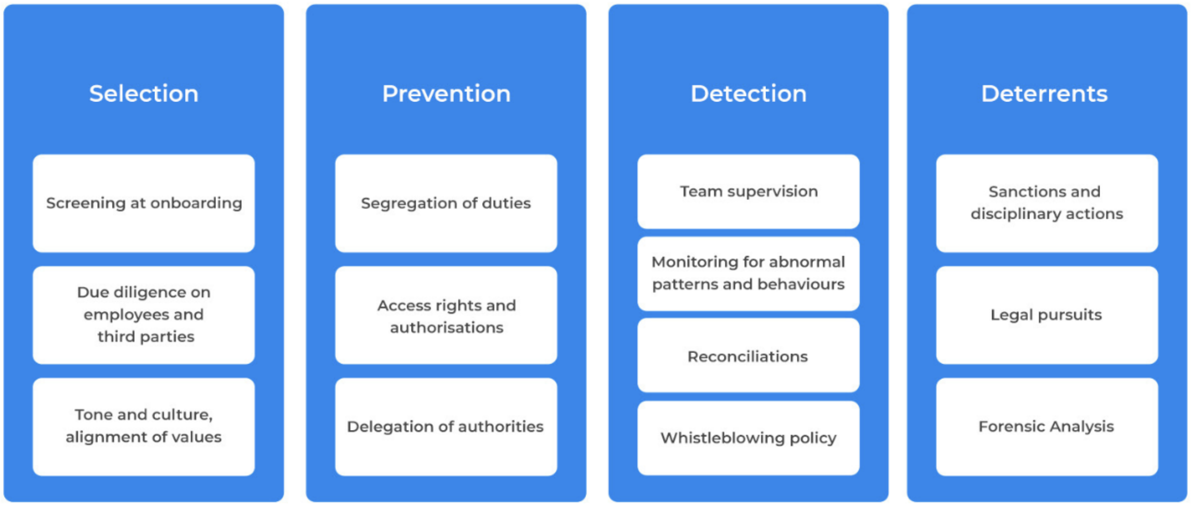

Selection
Screening at onboarding
Due diligence on employees and third parties
Tone and culture, alignment of values
Prevention
Segregation of duties
Access rights and authorisations
Delegation of authorities
Detection
Team supervision
Monitoring for abnormal patterns and behaviours
Reconciliations
Whistleblowing policy
Deterrents
Sanctions and disciplinary actions
Legal pursuits
Forensic Analysis

Figure 8. Internal Fraud Management

Source: analystprep.com

Research provided by Clari5 reveals that 70% of banking fraud is effectively executed by insiders, highlighting the urgent need to prioritize internal fraud surveillance.

Educate your Customers

Informing clients about the hazards they encounter, what to be vigilant for, and strategies for secure transactions is an effective method to mitigate the likelihood of fraud. Furthermore, this method enhances the confidence that your consumers have in your bank (Rohall, 2022).

If your goal is to educate your clients, ensure that you distribute press releases. The use of popular media may effectively capture news, resulting in the generation of free exposure, increased awareness, and enhanced trust for your digital bank (Rohall, 2022).

Monitor Transactions

Monitoring transactions to avoid money laundering and terrorist funding is mandatory in some situations, which includes the need to notify any suspicious behavior when an issue arises(Rohall, 2022). The transition towards digitalization and a cashless economy poses significant challenges to the current IT infrastructure in terms of security and fraud prevention measures. In order to transition from a conventional to a cashless economy, banks must enhance their security systems to combat fraud more effectively(Attigeri, MM, Pai, & Kulkarni, 2018).

Monitoring consumer behavior on a conventional website or institution may provide significant advantages, including the prevention of penalties and regulatory non-compliance, as well as the identification and investigation of possible instances of fraud (Rohall, 2022). It is highly recommended that small company owners modify their business model to conform to technological sustainability standards and capitalize on the digital revolution and social media platforms to enhance sales, establish connections, and provide better service to stakeholders (Colon, 2022).

An examination of legal data pertaining to offenses associated with corruption is provided. The research on countering corruption in the era of digitization adopts an institutional approach. This approach involves conducting a thorough analysis of the state's involvement, both as a whole and through its individual institutions, in the development and implementation of security policies. It also examines the legal framework governing this sphere and its position within the broader system of powers exercised by the authorities in the areas of domestic and foreign policy, as well as its relationship to individual activities (Markov & Velezev, 2021). Using the Gone and means-ends scheme theories is appropriate for anti-corruption accounting, all the more so since Sharia accounting values are essential for anti-corruption accounting (Arwani et al., 2022).

Use Real-Time Data Enrichment Tools

Real-time data enrichment is a process that supplements client KYC data with extra datasets acquired from diverse sources, including open-source databases, digital services, and social networks (Rohall, 2022).

This significantly enhances fraud detection by providing further information to facilitate more educated risk assessments. Furthermore, it enables you to get a comprehensive understanding of your consumers without requiring them to provide their personal information (Rohall, 2022).

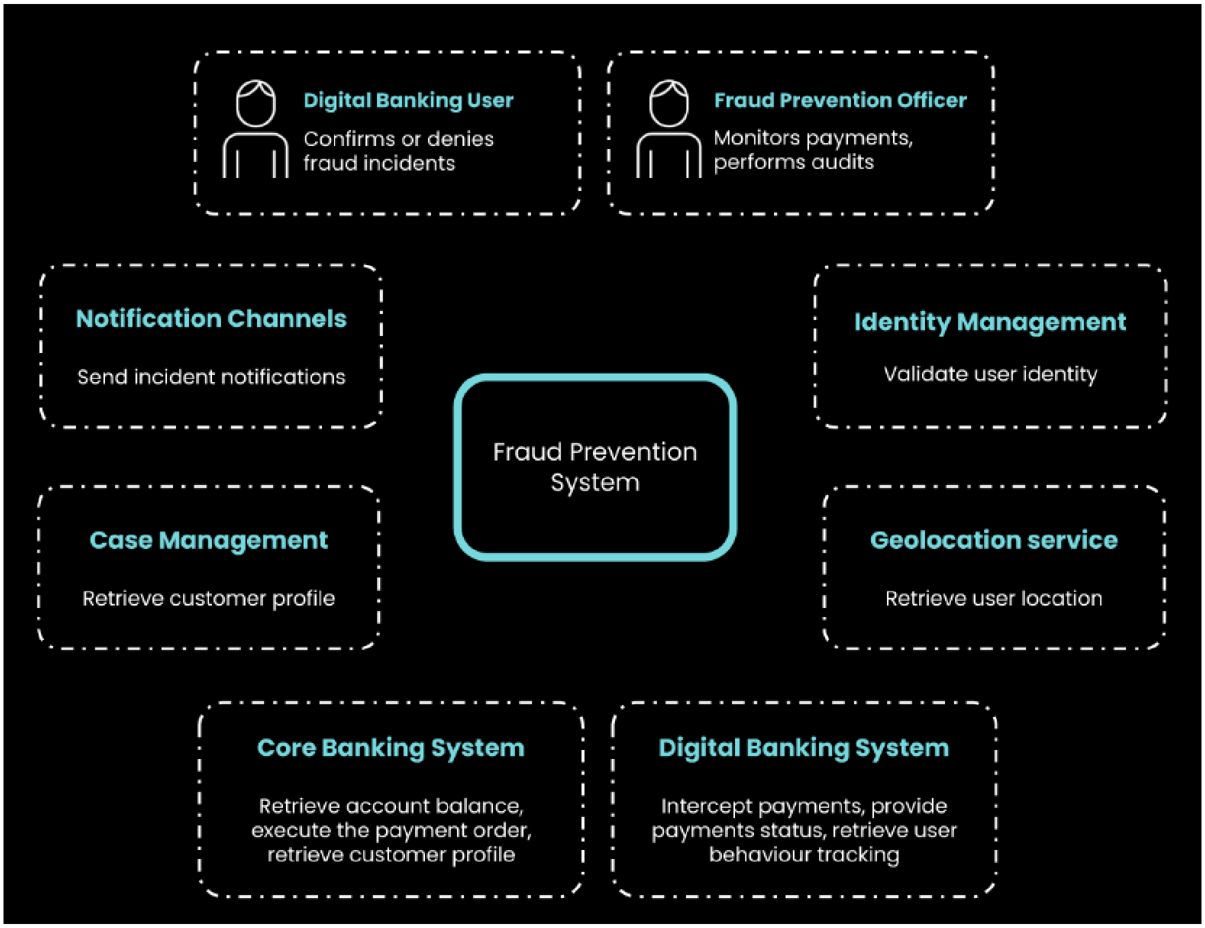

Digital Banking User
Confirms or denies fraud incidents
Fraud Prevention Officer
Monitors payments, performs audits
Notification Channels
Send incident notifications
Identity Management
Validate user identity
Fraud Prevention System
Case Management
Retrieve customer profile
Geolocation service
Retrieve user location
Core Banking System
Retrieve account balance, execute the payment order, retrieve customer profile
Digital Banking System
Intercept payments, provide payments status, retrieve user behaviour tracking

Figure 9. Real-time Fraud Prevention

Source: Inventio.io

Consequently, you may combat fraudulent activities without compromising a seamless client experience. These alternative digital signals may be used for credit scoring and underwriting purposes. They serve as reliable indicators to identify both risky users and valuable clients(Rohall, 2022).

Machine Learning

Although fraudsters may attempt to input inaccurate data during the KYC verification procedure, the use of machine learning algorithms and thorough risk evaluations may effectively detect and apprehend them (Rohall, 2022).

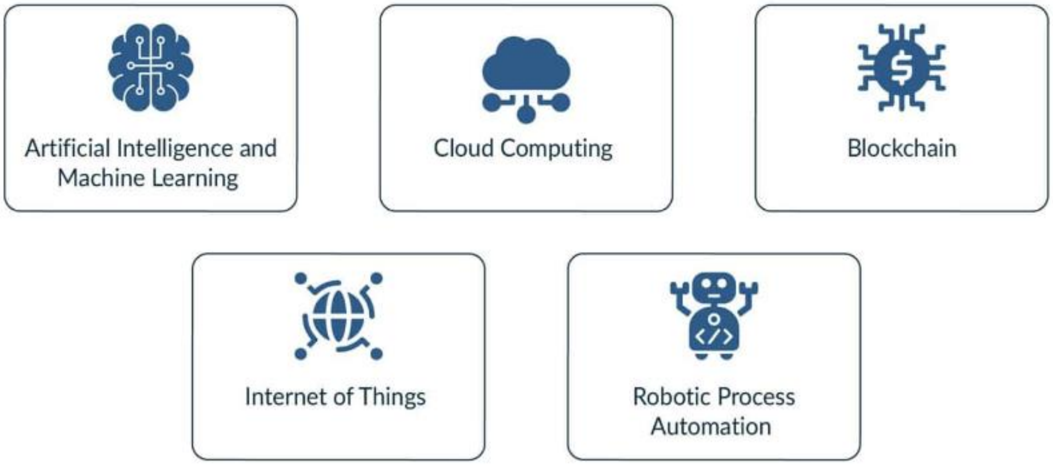

Artificial Intelligence and Machine Learning
Cloud Computing
Blockchain
Internet of Things
Robotic Process Automation

Figure 10. Key Banking Technologies

Source: inoxoft.com

Use Biometric System

Biometric systems are increasingly being used for identity verification in the banking sector as an effective anti-fraud measure. Additionally, clients really appreciate the simplicity and assurance provided by this technology.

Enhanced Customer Experience Through AI Technologies
Open Banking and Collaboration
The Rise of Biometric Authentication
Expanded Use of Blockchain
Emphasis on Data Privacy
Operating Like Tech Companies

Figure 11. Digital Banking Trends

Source: inoxoft.com

CONCLUSION

We have made revisions to these provisions to align with the requirements of POJK No. 39/POJK.03/2019, which mandates the implementation of anti-fraud strategies for commercial banks. These changes are also aimed at enhancing our internal control policy. This is also implemented in all policies, including Standard Operating Procedures (SOP), Technical Operating Instructions (TOI), and other legislation. The Anti Fraud Strategy has four main pillars, which are(Bank Mandiri, 2021a):

Pillar 1 (Prevention)

Reducing the possibility for fraud is a duty shared by all levels of the Bank, since it is an integral aspect of the Fraud Control System. The programs undertaken within this pillar encompass; (a) Anti-fraud awareness initiatives include the development and dissemination of an Anti-fraud Statement, an Employee Awareness

Program, and a Customer Awareness Program. Fraud awareness has been promoted throughout the year by sending email blasts to all staff and using social media to educate consumers about fraud(Bank Mandiri, 2021a); (b) The identification of vulnerabilities involves using Risk Management concepts to ensure that all policies and processes are created with consideration for internal control. Additionally, the use of GCG (Good Corporate Governance) and Compliance principles is also important. The job description of each employee delineates the execution of tasks by workers in accordance with their authority and obligations, and is then endorsed by the individual in question. Furthermore, all workers have duly signed the Annual Disclosure at the beginning of the year(Bank Mandiri, 2021a); © The Know Your Employee (KYE) policy includes Pre-employee Screening, System Qualification Selection Program, and Know Your Employee Screening. The adoption of the KYE (Know Your Employee) process has been carried out throughout employee recruiting procedures handled by the Human Capital department, as well as during employee recruitment procedures conducted directly by the respective work units(Bank Mandiri, 2022).

Pillar 2 (Detection)

All units, including the 1st line, 2nd line, and 3rd line of defense, have the duty to identify and detect fraud in the bank's commercial operations as part of the fraud control system(Bank Mandiri, 2022): (a) The process of whistleblowing management involves the oversight and control of reporting by an impartial third party, aiming to reduce conflicts of interest and instill a feeling of safety for the whistleblower (Bank Mandiri, 2021b); (b) A Fraud Detection System has been established to assist the Bank in detecting fraudulent activity in retail channel transactions and retail loans, including Micro, Consumer, and SME sectors(Bank Mandiri, 2021b); (c)The deployment of Surprise Audit is prioritized in business units that have a high risk or susceptibility to fraud; (d) The purpose of implementing the Surveillance System is to oversee and evaluate the efficiency of the internal control system, which includes the fraud control system(Bank Mandiri, 2021b).

Pillar 3 (Investigation, Reporting, Sanctions and Due Process)

The Fraud Control System is responsible for managing and addressing instances of fraud via investigations. The outcomes of these investigations are then reported to the President Director, Board of Commissioners, and Regulators. This includes recommendations for imposing fines and initiating legal actions against the perpetrators of fraud(Bank Mandiri, 2021b). In order to strengthen the function of the Third Pillar, there has been a delegation of authority to conduct investigations and impose sanctions to each region to accelerate the process of case handling and recovery(Bank Mandiri, 2021a).

Pillar 4 (Monitoring, Evaluation and Follow-up) The Fraud Control System includes monitoring the progress of investigations and assessments of fraud occurrences to identify flaws and enhance the Internal Control System, so preventing the recurrence of fraud resulting from similar vulnerabilities. Written reports are submitted in a systematic way to the President Director and Board of Commissioners to oversee the implementation of predetermined follow-up activities(Bank Mandiri, 2021a).

REFERENCES

Akinbowale, Oluwatoyin Esther, Mashigo, Polly, & Zerihun, Mulatu Fekadu. (2024). Development of a Heuristic Based Mixed Integer Linear Programming Model for Resources Allocation During Cyberfraud Mitigation. Operations Research Forum, 5(1), 1–27. Springer.

Arwani, Agus, Wijaya, Suparna, Laitupa, Muhammad Fadila, Mustafa, Muh Sabir, Chakim, Mochamad Heru Riza, Pattinaja, Elna M., & Andiyan, Andiyan. (2022). Contribution of Sharia Accounting Characters in Anti-Corruption Culture. Journal of Intercultural Communication, 22(4), 77–85. https://doi.org/10.36923/jicc.v22i4.46

Attigeri, Girija, MM, Manohara Pai, Pai, Radhika M., & Kulkarni, Rahul. (2018). Knowledge base ontology building for fraud detection using topic modeling. Procedia Computer Science, 135, 369–376.

Bank BRI. (2021). Digitalization: Go Smaller, Go Shorter, Go Faster. Retrieved from chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ir-bri.com/newsroom/049b92e0f2_df374fb157.pdf?cv=1

Bank Mandiri. (2021a). Enhancing Digital Banking Transformation & Innovation. Retrieved from chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://vpr.hkma.gov.hk/statics/assets/doc/200048/ar_21/ar_21_eng.pdf?cv=1

Bank Mandiri. (2021b). Transformasi yang Berkelanjutan Menuju Bank Digital Terbaik Sustainable Transformation Towards the Best Digital Bank. Retrieved from chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://bankmandiri.co.id/documents/38265486/0/SR_Bank+Mandiri+2021_lowres.pdf/?cv=1

Bank Mandiri. (2022). Digital Transformation with Excellent Results. Retrieved from chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.bankmandiri.co.id/documents/38265486/0/AR+BMRI+versi+inggris+-+28+FEBRUARY.pdf/c9f592ed-9986-e9f7-2c27-78a2acd5ba94?cv=1&t=1677580707044

Colon, Eunice. (2022). Technology Strategies to Sustain Small Business Enterprises Beyond 5 Years. Walden University.

Dewi, Yuli, Suharman, Harry, Koeswayo, Poppy Sofia, & Tanzil, Nanny Dewi. (2023). Actors influencing the effectiveness of credit card fraud prevention in indonesian issuing banks.

Domashova, Jenny, & Zabelina, Olga. (2021). Detection of fraudulent transactions using SAS Viya machine learning algorithms. Procedia Computer Science, 190, 204–209.

Guritno, Bambang, Dewi, Ratna Sari, Arianti, Farida, Utama, Andrew Shandy, Norvadewi, Norvadewi, Anggara, Oki, & Andiyan, Andiyan. (2023). Culture of Islamic Economic Principles and Democracy and Welfare Based on Pancasila Ideology. Journal of Intercultural Communication, 23(1), 55–65. https://doi.org/10.36923/jicc.v23i1.43

Lubis, Erni Triyani, Harahap, Juliandi, & Nuraini, Nuraini. (2021). Analysis Of Potential Fraud Control At Metta Medika Hospital Sibolga. Science Midwifery, 10(1, October), 240–332.

Magomedov, Shamil, Gusev, Alexander, Ilin, Dmitry, & Nikulchev, Evgeny. (2021). Users' reaction time for improvement of security and access control in web services. Applied Sciences, 11(6), 2561.

Markov, V. P., & Velezev, S. I. (2021). Corruption counteraction: theoretical and practical aspects. Engineering Economics: Decisions and Solutions from Eurasian Perspective, 163–168. Springer.

Mohan, N., Rajasekar, G., & Agriyanto, Ratno. (2023). Anti-Fraud AI for Banking and FinTech Used in a Proactive Banking Strategy to Thwart SIM Phishing. In The Impact of AI Innovation on Financial Sectors in the Era of Industry 5.0 (pp. 171–183). IGI Global.

Nurjamin, Asep, Masita, Ella, Lisetyo, Ariyanti, Dharta, Firdaus Y., Mumfangati, Titi, Saputra, Nanda, & Andiyan, Andiyan. (2023). The Millennial Generation and the Caption Language of Social Media. Migration Letters, 20(8), 157–168.

Puluhulawa, Jufryanto, Puluhulawa, Mohamad Rusdiyanto U., & Swarianata, Vifi. (2022). Liability Limitation of PeduliLindungi Applications in the Convergence Dynamics of Telematics Law. KnE Social Sciences, 100–111.

Rohall, PJ. (2022). Fraud Detection and Prevention in Banking Explained. Retrieved January 20, 2024, from seon website: https://seon.io/resources/banking-fraud-detection-and-prevention/?cv=1

Sehrawat, Neeraj, Kumar, Amit, Nigam, Narander Kumar, Singh, Kirtivardhan, & Goyal, Khushi. (2020). Test of capital market integration using Fama-French three-factor model: Empirical evidence from India. Investment Management & Financial Innovations, 17(2), 113.

Shaymardanov, Timur A., & Vavrenyuk, Aleksandr B. (2022). Development of an Anti-fraud System with Real-Time Analytics. 2022 Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), 436–438. IEEE.

Srokosz, Michal, Bobyk, Andrzej, Ksiezopolski, Bogdan, & Wydra, Michal. (2023). Machine-Learning-Based Scoring System for Antifraud CISIRTs in Banking Environment. Electronics, 12(1), 251.

Sungkawaningrum, Fatmawati, Hartono, Sri, Holle, Mohammad H., Gustiawan, Willson, Siskawati, Eka, Hasanah, Niswatun, & Andiyan, Andiyan. (2022). Determinants of Community Decisions To Lend Money To Loaners. International Journal of Professional Business Review, 7(2), e0510–e0510. https://doi.org/10.26668/businessreview/2022.v7i3.510.