Economic Affairs, Vol. **69**(02), pp. 1059-1068, June 2024
DOI: 10.46852/0424-2513.3.2024.29

REVIEW PAPER

A Postmortem of Financial Frauds: The 5S Approach

M. Daniel Rajkumar[1] and Amith Donald Menezes[2*]

[1]Program Coordinator (DE-Management Program) & Asst. Professor, Directorate of Online and Distance Education, SRMIST., Kattankulathur, Chennai, Tamil Nadu, India
[2]Assistant Professor, Mangalore Institute of Technology and Engineering, Moodabidri, Dakshina Kannada, Karnataka, India

*Corresponding author: amithmnzs@gmail.com (**ORCID ID:** 0000-0003-0505-668X)

Received: 17-12-2023 **Revised:** 05-02-2024 **Accepted:** 25-02-2024

ABSTRACT

Modern world, saturated with innovations and digital technologies, opens numerous opportunities for development and convenience. However, along with these opportunities, the likelihood of becoming a target of fraud rises. Financial crimes are becoming more pronounced and sophisticated, utilizing new technical and social methods of influence. With these changes, existing risks, including fraud risk, have significantly increased. In spite of extensive endeavors to eliminate fraudulent actions, apparently fraud in its different forms persists and is escalating in both occurrence and magnitude. Identifying fraud schemes is a crucial aspect of fraud detection. Detecting fraud risks at an early stage can bolster investor protection, enhance investment returns, prevent costly legal battles, and promote efficient operation. This study concentrates on the various facets of fraud. It examines the pre and post-effects of fraud. It also involves extensive research on the available literature on financial and non-financial frauds and has come out with a conceptual model that helps to give an overall 360-degree view of the concept of fraud. This work gives a theoretical insight into fraud. It reveals a five-part comprehensive approach termed as the 5S approach to analyze and view the concept of fraud, namely the Segregation of fraud, Schemes used to commit these frauds, Stimulus for committing these types of frauds, the Significant Consequences or the resultant effects of fraud and finally the ways of reducing or countering these frauds or the specific remedies to negate or overcome these frauds.

HIGHLIGHTS

- Financial crimes or frauds are becoming more pronounced and sophisticated, utilizing new technical and social methods of influence.
- Despite extensive endeavours to eliminate fraudulent actions, apparently fraud in its different forms persists and is escalating in both occurrence and magnitude.
- Understanding the symptoms and causes of fraud plays a crucial role in both preventing and detecting fraudulent activities.
- A proper approach of systematically identifying these frauds and finding out the causes or motives and how to prevent these frauds from happening or likely reduction in the intensity of frauds is being discussed in this study with focus on the proposed 5S approach.

Keywords: Frauds, 5S approach, Schemes, Segregations, Stimulus, Significant Consequences, Specific remedies

In every organization that produces goods or provides services, management activities are inseparable (Hashim *et al.* 2020). Through effective management, all existing organizational resources can be planned, organized, directed, and monitored to achieve organizational goals in the right manner (Abbas *et al.* 2020). Currently, public and private sector organizations worldwide are facing rapid economic changes, such as globalization, advancing

How to cite this article: Daniel Rajkumar, M. and Menezes, A.D. (2024). A Postmortem of Financial Frauds: The 5S Approach. *Econ. Aff.*, **69**(02): 1059-1068.

Source of Support: None; **Conflict of Interest:** None

technology, changes in industries and businesses, and the challenges and intricacies associated with information or data governance (Perols, 2011; Sanad and Al-Sartawi, 2021).

Modern world, saturated with innovations and digital technologies, opens numerous opportunities for development and convenience. However, along with these opportunities, the likelihood of becoming a target of financial fraud rises (Mandal, 2023). Financial crimes are becoming more pronounced and sophisticated, utilizing new technical and social methods of influence. With these changes, existing risks, including fraud risk, have significantly increased (Meyer, 2016; Chen 2023).

In spite of extensive endeavors to eliminate fraudulent actions, apparently fraud in its different forms persists and is escalating in both occurrence and magnitude (Wolfe and Hermanson, 2004). Fraud is recognized in the capacity of a worldwide phenomenon, with its presence permeating corporations to such an extent that no country remains immune, though developing nations bear the brunt the most (Okoye and Gbegi, 2013; Chimonaki *et al.* 2023). Presently, fraud and related illicit activities are commonplace in both sectors.

Businesses' moral duty involves upholding accountability to all stakeholders while pursuing success (Power, 2013; Liao *et al.* 2019). Nevertheless, fraudulent activities within a business present a notable threat, causing harmful repercussions for both the business and its stakeholders. Fraud represents a critical challenge in the corporate realm, resulting in considerable financial losses for organizations annually (Smith, 2008).

Conceptual Framework

Hall (2017) states that fraud is an act that displays material facts in the form of false representations made by one party to another to deceive and persuade the other party by relying on detrimental facts. Fraud is defined as "wrongful or criminal deception that leads to financial or personal advantages" (Usman & Shah, 2013). Researchers on fraud have identified common elements in all fraudulent activities: a perceived pressure, an identified opportunity, and a means to rationalize the fraud as acceptable and aligned with one's personal ethical standards (Albrecht *et al.* 2016).

Pustylnick (2009) suggests that in the era before internet, safeguarding information with passwords was straightforward due to the absence of public network-access points. However, in subsequent decades, the evolution of computer-based environments has led to increased sophistication, as well as a rise in fraudulent crimes targeting these infrastructures.

Accounting or financial fraud has played a pivotal role in the decline of numerous financial and non-financial entities globally (Gerety and Lehn, 1997; Ozili, 2020). Fraud is additionally characterized as "any offense that relies on deceit as its primary mode of operation, encompassing various illicit behaviors by individuals and organizations, not all of which are necessarily criminal but are considered 'morally questionable'" (Ghazali *et al.* 2014).

Identifying fraud schemes is a crucial aspect of fraud detection (Yuri *et al.* 2022). Detecting fraud risks at an early stage can bolster investor protection, enhance their investment returns, prevent costly legal battles, and promote the efficient operation of capital markets (Mangala & Kumari, 2015). Moreover, there is an ongoing need for additional, effective fraud indicators and detection models (Wolfe and Hermanson, 2004; Rahman and Jie, 2024) to aid auditors and other stakeholders in accurately forecasting the probability of fraudulent financial reporting (FFR) and facilitating informed economic decision-making (Zhou & Kapoor, 2011). Nonetheless, pinpointing fraud schemes remains a daunting endeavor due to their increasing complexity and sophistication, facilitated by advanced technology and the deceptive nature inherent in fraud. This complexity results in losses and damages to the financial sector (Ruankaew, 2016).

Understanding the symptoms and causes of fraud plays a crucial role in both preventing and detecting fraudulent activities (Rezaee, 2005; Young, 2020). Fraud can manifest in three distinct ways: through inadvertent actions due to a lack of awareness (errors), through conscious awareness combined with rationalization to mitigate negative emotions (where an individual's intuition supports fraudulent behavior), or through conscious awareness alongside a rational cost-benefit analysis (where an individual's intuition is unclear) (Murphy & Dacin, 2011).

Hence, given the evolving nature of fraudulent activities, it's imperative for all organizations, particularly those in both public and private sectors, to recognize the importance of implementing measures for detecting and preventing fraud within their operations (Segal, 2016; Murrar, 2022). Drawing on the events and research outlined earlier, the aim of this study is to assess the level of employee awareness concerning fraud within sampled companies across both public and private sectors. Furthermore, the study seeks to investigate the utilization of methods and technology in detecting and preventing fraud within companies, thereby enhancing organizational performance.

Methodology

Since this is a conceptual paper the methodology is a through literature review on various aspects of fraud that has a bearing on implication on the analysis part. It's a review paper which concentrates on developing an approach to analyse the fraud and ways to prevent them from occurring. The methodology used here is a comparative analysis type, wherein various literature on fraud is analyzed and compared to give an overall idea of the various facets of fraud related to financial and non- financial aspects.

FINDINGS AND DISCUSSION

Based on the theoretical framework it is clear that we need to analyse the concept of fraud through a holistic approach. Various literature reviews has paved way to look at the concept of fraud from different dimensions. Hence the researcher proposes the 5S model or approach to analyse frauds and its scope.

The 5S Approach

This approach to analyse fraud has five elements in it (Fig. 1), namely;

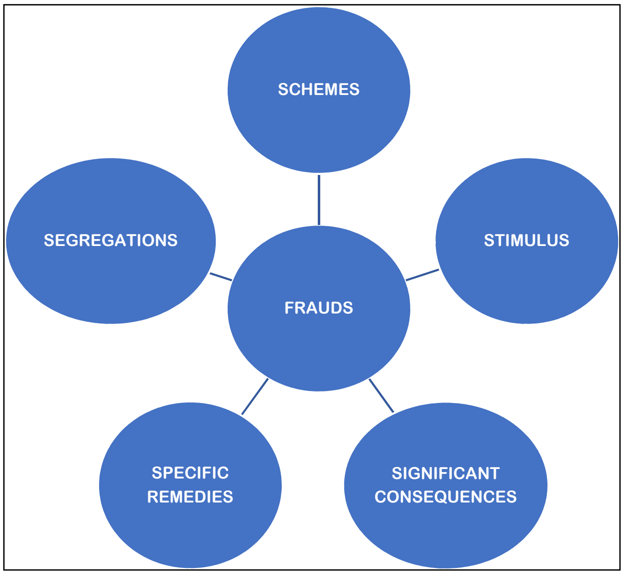
(a) Segregations

(b) Schemes

(c) Stimulus

(d) Significant Consequences, and

(e) Specific Remedies



Source: *Developed by the researcher.*

Fig. 1: The 5S Approach to Fraud

SEGREGATIONS

Frauds can be segregated into different types and on different basis. Each researcher has a different view of the same. Let us list down the various types of segregations of fraud that are popularly used in this modern business era.

One view of fraud segregates it into three main types which are as below:

- Financial Statement fraud also known as Financial Fraud
- Misappropriation of Assets and,
- Corruption

Debreceny and Gray, (2010) segregate frauds based on the person who commits these frauds also known as the source. Hence frauds are divided or segregated as below;

1. Internal Sources:

- **Employees:** Individuals within an organization may commit fraud, including embezzlement, financial statement fraud, or misuse of company resources.
- **Management:** In some cases, top-level executives or managers may orchestrate fraud schemes, such as financial manipulation or insider trading.

2. External Sources:

- **Customers/Clients:** Fraud can be committed by external parties, such as customers engaging in payment fraud, deceptive practices, or exploiting product return policies.
- **Suppliers/Vendors:** Fraud can originate from suppliers or vendors through invoice fraud, delivery of substandard goods, or collusion with employees.

3. Cybercriminals:

- **Hackers:** Cybercriminals can engage in various types of fraudthrough hacking into systems.
- **Phishers:** Fraudsters may use phishing techniques to trick individuals into providing sensitive information, leading to identity theft or financial fraud.

4. Organized Crime:

- **Criminal Organizations:** Organized crime groups may be involved in large-scale fraud, including financial scams, insurance fraud, and cybercrimes.

5. Individuals:

- **Fraudsters:** Individuals with the intent to deceive may engage in various types of fraud, such as investment scams, lottery frauds, or Ponzi schemes.
- **Identity Thieves:** Individuals seeking to profit from stolen personal information may engage in identity theft and related fraudulent activities.

6. Corruption:

- **Bribery and Corruption:** Fraud can result from corrupt practices, including bribery of public officials, kickbacks, and other forms of corrupt transactions.

7. Insiders and Employees:

- **Insiders:** Individuals with inside information, such as employees or contractors, may exploit their privileged positions for fraudulent activities, including insider trading or leaking sensitive information.

8. Government Entities:

- **Government Officials:** Corruption within government entities can lead to various forms of fraud, including embezzlement of public funds or misuse of government resources.

9. Financial Institutions:

- **Insiders in Financial Institutions:** Employees within financial institutions may engage in manipulating accounts and facilitating other fraudulant transactions.

10. Online Platforms:

- **Fake Websites and Scams:** Fraud can originate from fake websites, online scams, and social engineering techniques aimed at tricking individuals into providing personal or financial information.

11. Healthcare Industry:

- **Healthcare Professionals:** Fraud can occur in the healthcare industry through billing fraud, overcharging for services, or providing unnecessary treatments.

12. Government Programs:

- **Beneficiaries of Government Programs:** Individuals may engage in fraud by providing false information to obtain government benefits, subsidies, or assistance.

SCHEMES

Fraud schemes can take various forms and the contexts can vary. The major fraud schemes that are in trend are as below:

- **Identity Theft:** to impersonate someone else for financial gain by stealing their personal data.
  - *Stolen Identity:* using other's personal data, to commit fraud without their consent or awareness.
  - *Synthetic Identity Theft:* Creation of fictitious identities by combining real and fake information for fraudulent activities.
- **Investment Fraud:** a deceptive way of making people invest in the wrong schemes
  - *Ponzi Schemes:* A deceptive investment scheme wherein profits are distributed to

initial investors through funds contributed by subsequent investors, rather than generated from legitimate earnings.

- *Pyramid Schemes:* Similar to Ponzi schemes, these involve recruiting investors, and profits are generated by recruiting more investors rather than from actual products or services.
- *Recovery Room scheme:* victims of an investment scheme are given a counter offer to recover their lost money by further investing in another alternative.

- **Insurance Fraud:** Falsifying information or events to gain benefits from insurance policies, such as submitting false claims or staging accidents.
  - *Health Insurance Fraud:* False claims or exaggeration of medical conditions to obtain unjustified insurance payouts.
  - *Auto Insurance Fraud:* Deliberate exaggeration or fabrication of auto accidents to claim insurance benefits.
- **Securities Fraud:** Misleading investors with false information or manipulating the stock market for financial gain.
  - *Pump and Dump schemes:* fraudsters manipulate the stock prices by investing in some not so strong securities and influence potential investors to invest in it and subsequently would dump their holdings and the share prices would fall drastically.
  - *Microcap Fraud:* fraudsters offer these micro or not so well established companies stock to investors as fast growing and make money.
- **Advance Fee Scam:** is where the fraudsters ask people to pay or advance payments for certain job offers, lotteries, and loans etc. which actually do not exist.
- **Bank Fraud:** Deceptive practices by individuals, banks, or financial institutions to acquire funds, assets, or other belongings under the ownership or custody of a financial institution
  - *Credit Card Fraud:* Utilization of credit card details without permission for making purchases or withdrawals.
  - *KYC Fraud:* fraudulent messages or calls are done in the name of banks and ask for personal details for updating KYC of banks else threatening to block the accounts.
  - *UPI Related Frauds:* fraudsters send fake link or URL to infect the phone and steal money and personal information through inputting viruses or screen mirroring tools.
- **Mortgage Fraud:** Submitting inaccurate information on mortgage applications in order to obtain a loan or more favorable conditions.
  - *Application Fraud:* Providing inaccurate information on mortgage applications in order to obtain a loan.
  - *Foreclosure Rescue Scams:* Exploitative practices targeting homeowners facing foreclosure.
- **Forgery:** Creating or altering documents with the intent to deceive or defraud.
- **Wire Fraud:** Using electronic means, such as email or phone, to deceive someone for financial gain.
  - *Quishing:* is deception by sending QR code and causing monetary loss as well as stealing personal data.
  - *Vishing:* involves fraudulent phone calls to steal persona data
  - *Smishing:* duplicitous text messages are sent to fraudulently access personal data.
  - *Twishing:* opening a fake twitter account of a known person and swindling money or personal data.
  - *Ghosting:* hacking into known peoples emails and sending fraudulent money requests or investment advices.
  - *Mass Marketing Frauds:* sending spam emails or calls to steal money or personal information for fraudulent activities.
  - *SIM Swap Fraud:* fraudsters use fake papers or documents and apply for swap of SIM and get access to all the banking details including the OTPs and other alerts.
- **Cybercrime:** Various fraudulent activities conducted online, including hacking, ransomware attacks, and online scams.

- *Phishing:* Fraudulent efforts to obtain sensitized data, such as usernames, by impersonating a reliable entity
- *Ransomware:* Malware designed to encrypt a user's documents and demand remittance for their decryption.
- *Online Scams:* Various deceptive practices conducted on the internet, such as lottery scams, romance scams, and fake online auctions.
- *Pig Butchering:* is a scheme of fraud wherein the fraudster acts like a potential friend or partner and lures to make an investment or pay for a job which is non existing.

- **Counterfeiting:** Producing fake goods or currency with the intent to deceive and gain financial advantage.
- **Corporate Fraud:** Fraudulent activities within a company, such as financial statement manipulation, embezzlement, or insider trading.
  - *Financial Statement Fraud:* Alteration of financial documents to portray an inaccurate depiction of a company's financial well-being.
  - *Embezzlement:* Misappropriation of funds by individuals entrusted with financial responsibilities within an organization.

Consumer Fraud

- *Product Fraud:* Sale of counterfeit or substandard goods, misrepresentation of product features, or deceptive advertising.
- *Telemarketing Fraud:* Deceptive telemarketing practices aimed at extracting money or personal information from consumers.

Government Fraud

- *Welfare Fraud:* Misrepresentation of information to receive government assistance or benefits.
- *Public Corruption:* Abuse of public office for personal gain, including bribery and kickbacks.

Healthcare Fraud

- *Billing Fraud:* Overcharging or billing for services not provided in the healthcare industry.
- *Prescription Fraud:* Fraudulent acquisition, distribution, or use of prescription medications.

Tax Fraud

- *Tax Evasion:* Deliberate underreporting of income, inflating deductions, or other fraudulent actions to evade taxes.
- *Identity Theft for Tax Fraud:* Filing fraudulent tax returns using stolen personal information.

STIMULUS

In order to analyse any frauds we need to study the reason behind committing such frauds or simply put what are the motives of people that made them to defraud people (Sharma and Panigrahi 2013; Kakati and Goswami, 2019). These reasons or causes are termed as "Stimulus" in this 5S approach, which will go a great way to try and prevent or reduce frauds in the future. The various stimuli to frauds are as below:

- Greediness of money
- Pressure of job itself
- Trying to manipulate situations
- Providing for the growing needs of family
- Make use of the available opportunity or perceived opportunity
- Help in creating a better political friends
- Rationalising the fraudulent act as a moral way.
- Perceived pressure to make money.
- Manager's personal gain or benefits.
- Covering up for bad performances.
- Lack of transparency in the system
- Negligible management involvement
- Dwindling Moral values
- Management encourages cheating
- The lack of punishment
- Lower rates of fraud detection
- Unintentional engagement in fraudulent activity due to a lack of awareness or understanding.
- Lack of awareness about fraud risks and inadequate training on ethical behaviour.
- Organizations that do not prioritize and foster a culture of ethics and integrity may inadvertently encourage fraudulent behavior.

- Employees may face pressure to meet performance targets
- Inadequate background checks and poor hiring practices
- If organizations do not provide clear channels for reporting suspected fraud or if there is a fear of retaliation
- The rapid evolution of technology introduces new avenues for fraud
- Economic instability or financial crises
- Lax regulatory oversight or weak enforcement mechanisms
- Overwhelming debts, mounting financial pressures, or the fear of financial ruin
- To sustain or enhance their lifestyle
- To meet performance targets, quotas, or expectations.
- Fear of job loss, pressure from superiors, or the desire for career advancement.
- Individuals struggling with addiction or substance abuse issues
- Psychological motivations, such as a sense of entitlement, lack of empathy, or a disregard for ethical norms
- Form of revenge or retaliation against perceived wrongs
- To cover their tracks and avoid detection or legal consequences
- Sustain their gambling habits
- Social pressure, whether from peers, family, or societal expectations
- Opportunities due to weak internal controls, inadequate supervision, or a lack of oversight
- During economic crises or downturns
- Misguided sense of loyalty to an organization
- Inadequate internal controls and deficient corporate governance practices
- Shortcomings in the performance of external auditors

SIGNIFICANT IMPACT

Fraud has a significant effect of environment and it also affects the environment, whether it is internal environment of the organisation or the external one (Mirinaviviene, 2014; Meyers, 2016). As per Sadka (2006), the involvement of a company in accounting fraud will impact not only the entire industry but also societal welfare (Dukic et al., 2023).Hence let us see the various kinds of impact or consequences of fraud:

- Fraud causes damage or loss to the victim of the fraud.
- Fraud significantly impacts the business environment
- There is an intent to deceive or knowledge that someone's statement is false.
- The false presentation is a significant factor relied upon by the injured party.
- The fact must be a significant factor in inducing someone to act.
- There is a false statement or it is not disclosed.
- Company inaccurately claims to possess a competitive edge, rival firms may erroneously opt for unprofitable investments and/ or suboptimal organizational structures in reaction".
- False financial reporting may lead to securities being overvalued and excessive borrowing by a company.
- It can lead to a decline in shareholder value as investors react to negative news, loss of trust, and uncertainty about the organization's financial stability.
- Insurance companies may increase premiums or impose stricter conditions on policyholders after instances of fraud, leading to higher costs for individuals and businesses.
- Fraud can negatively impact credit scores, affecting individuals' ability to secure loans or obtain favorable interest rates.
- Contribute to market instability and disrupt the broader economy.
- Fraud erodes trust in individuals, organizations, and even entire industries.
- Organizations may suffer reputational damage.
- May face legal action, including lawsuits from affected parties, regulatory fines, and potential criminal charges against individuals responsible for the fraud.

- Can disrupt normal business operations.
- This will have repercussions on the entire industry and also on social welfare.
- Disruption can lead to loss of productivity and increased recovery costs.
- Incur additional expenses to implement or enhance compliance measures following instances of fraud to meet regulatory requirements and prevent future occurrences.
- Erodes trust in societal institutions.
- Divert resources away from productive activities
- Victims may experience emotional distress, anxiety, and a loss of personal security.
- Can negatively impact the overall well-being of affected individuals, leading to health issues and a reduced quality of life.
- Lead to the misuse of personal information and bring about financial and reputational harm.
- Victims may need to engage in legal processes to recover losses
- Downtime, increased recovery costs, and potential damage to critical infrastructure.
- Contribute to economic instability.
- Divert societal resources away from productive activities
- More stringent regulations and compliance requirements for businesses.
- Global cooperation and coordinated efforts are required to address transnational fraud

SPECIFIC REMEDIES

Having seen the segregations of the frauds and the type of schemes people use to commit these frauds, it is imperative to see as to why people commit these frauds, which is what is the motivation or broadly put as the stimulus for committing fraud (Sorunke, 2016). After which we need to list down the various consequences of such frauds, having done that the last aspect of this 5S approach is to prevent these frauds from happening for which we need to jot down the various preventive measures or simply put as the specific remedies to solve these frauds or stop them from occurring in the future. A detailed remedy is as below;

- Separation of responsibilities
- Adequate authorization and approval procedures
- Implementation of physical security measures like locks and surveillance cameras
- Routine examinations and assessments
- Establishment of channels for reporting suspicious behaviour
- Adoption of a proper Code of Conduct
- Training programs to raise awareness about fraud
- Safeguards for whistle-blowers
- Enforcement of consequences for fraudulent conduct
- Identifying and evaluating potential areas of risk through risk assessment
- A pre-employment screening
- Following a robust ethics policy
- Random check on transaction data
- Data mining tools
- Random check on employees' email
- Notification by third parties
- External audit
- Management information system (MIS)
- Implement strict authorization procedures for financial transactions and other critical processes.
- Conduct regular training sessions to educate employees about the risks of fraud
- Establish confidential reporting mechanisms
- Use forensic accounting techniques to investigate suspicious activities.
- Enhanced clarity in financial reporting
- Precisely delineate roles and responsibilities to prevent any individual from exerting undue influence over a process or transaction.
- Employ cybersecurity measures to protect against data breaches and cyber threats.
- Deploy fraud detection mechanisms leveraging artificial intelligence (AI)
- Implement biometric authentication methods for access to sensitive systems and data
- Use encryption and multi-factor authentication to secure sensitive information

- Conduct thorough background checks on customers, clients, and vendors to verify their identities and legitimacy.
- Implement strong KYC procedures, especially in industries prone to fraudulent activities
- Establish collaboration and information-sharing mechanisms with law enforcement agencies to report and investigate fraud
- Cooperate in legal actions against perpetrators
- Establish cross-functional teams involving members from different departments to review and analyze financial transactions and processes
- Advocate for strict legal consequences for individuals and organizations involved in fraudulent activities
- Monitor changes in behavior, spending patterns, or work habits among employees
- Scrutinize documents, invoices, receipts, and other financial records for inconsistencies, forgeries, or alterations that may indicate fraudulent activities
- Implement document authentication techniques to verify the legitimacy of documents
- Launch public awareness campaigns to educate citizens about common types of fraud

CONCLUSION AND FUTURE RESEARCH SCOPE

In conclusion, fraud remains a persistent threat in various sectors, evolving alongside advancements in technology and changes in societal behaviours. As we navigate an increasingly digital landscape, emerging trends in fraud pose complex challenges, requiring proactive and adaptive strategies for mitigation. From traditional forms of fraud such as identity theft and financial scams to newer threats like deepfake technology and synthetic identity fraud, the landscape of fraudulent activities continues to expand.

Addressing these challenges necessitates a multifaceted approach that combines the 5S approach by analysing the segregations and schemes along with the stimulus for committing these frauds. Leveraging advanced technical capabilities, enables quicker identification of suspicious activities and patterns along with its significant impact and the specific remedies to overcome these frauds.

Looking ahead, as fraudsters continue to adapt and refine their tactics, staying ahead of the curve will require on-going collaboration and innovation. By fostering a dynamic ecosystem that fosters information sharing, collaboration, and technological advancement, we can strive towards a future where fraud is effectively mitigated, safeguarding individuals, businesses, and society at large.

REFERENCES

Abbas, D.S., Eksandy, A., Hakim, M.Z. and Syam, I. 2020. Pengaruh Indikasi Kecurangan Terhadap Kecurangan Laporan Keuangan Dalam Perspektif Fraud Pentagon. *Journal Ekonomi, Sosial & Humaniora*, **1**(10), 55-64.

Albrecht, C.C., Sanders, M.L., Holland, D.V. and Albrecht, C. 2016. The debilitating effects of fraud in organizations. In *Crime and Corruption in Organizations* (pp. 163-185). Routledge.

Chen, Q. 2023. Study of Financial Fraud in Guangzhou Longkey Based on Fraud Risk Factors. *Frontiers in Business, Economics and Management*, **12**(1): 194-198.

Chimonaki, C., Papadakis, S. and Lemonakis, C. 2023. Perspectives in fraud theories–A systematic review approach. *F1000 Research*, **12**: 933.

Debreceny, R.S. and Gray, G.L. 2010. Data mining journal entries for fraud detection: An exploratory study. *International Journal of Accounting Information Systems*, **11**(3): 157-181.

Dukić, T., Pavlović, M. and Grdinić, V. 2023. Uncovering Financial Fraud: The Vital Role of Forensic Accounting and Auditing in Modern Business Practice. *Economic Themes*, **61**(3): 407-418.

Gerety, M. and Lehn, K. 1997. The causes and consequences of accounting fraud. *Managerial and Decision Economics*, **18**(7-8): 587-599.

Ghazali, M.Z., Rahim, M.S., Ali, A. and 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.

Hall, X.M. 2017. *Fraud detection and the internal auditor* (Doctoral dissertation, Utica College).

Hashim, H.A., Salleh, Z., Shuhaimi, I. and Ismail, N.A.N. 2020. The risk of financial fraud: a management perspective. *Journal of Financial Crime*, **27**(4): 1143-1159.

Kakati, S. and Goswami, C. 2019. Factors and motivation of fraud in the corporate sector: A literature review. *Journal of Commerce & Accounting Research*, **8**(3): 86-96.

Kizyma, T. and Kizyma, A. 2019. Identifying causes and potential consequences of financial fraud. *Herald of Economics*, **2**(92): 47-56.

Liao, L., Chen, G. and Zheng, D. 2019. Corporate social responsibility and financial fraud: Evidence from China. *Accounting & Finance*, **59**(5): 3133-3169.

Mandal, A. 2023. Fathoming fraud: unveiling theories, investigating pathways and combating fraud. *Journal of Financial Crime*.

Mangala, D. and Kumari, P. 2015. Corporate fraud prevention and detection: Revisiting the literature. *Journal of Commerce & Accounting Research*, **4**(1): 35-45.

Meyers, D.T. 2016. *Victims' stories and the advancement of human rights*. Oxford University Press.

Mirinaviciene, S. 2014. Internal control and fraud prevention: Prior research analysis. *Science and studies of accounting and finance: problems and perspectives*, **9**(1): 173-179.

Murphy, P.R. and Dacin, M.T. 2011. Psychological pathways to fraud: Understanding and preventing fraud in organizations. *Journal of Business Ethics*, **101**: 601-618.

Murrar, F. 2022. Fraud schemes during COVID-19: a comparison from FATF countries. *Journal of Financial Crime*, **29**(2): 533-540.

Ozili, P.K. 2020. Advances and issues in fraud research: a commentary. *Journal of Financial Crime*, **27**(1): 92-103.

Perols, J. 2011. Financial statement fraud detection: An analysis of statistical and machine learning algorithms. *Auditing: A Journal of Practice & Theory*, **30**(2): 19-50.

Power, M. 2013. The apparatus of fraud risk. *Accounting, Organizations and Society*, **38**(6-7): 525-543.

Pustylnick, I. 2009. Combined algorithm for detection of manipulation in financial statements. *Available at SSRN 1422693*.

Rahman, M.J. and Jie, X. 2024. Fraud detection using fraud triangle theory: evidence from China. *Journal of Financial Crime*, **31**(1): 101-118.

Rezaee, Z. 2005. Causes, consequences, and deterence of financial statement fraud. *Critical Perspectives on Accounting*, **16**(3): 277-298.

Ruankaew, T. 2016. Beyond the fraud diamond. *International Journal of Business Management and Economic Research*, **7**(1): 474-476.

Sadka, G. 2006. The economic consequences of accounting fraud in product markets: Theory and a case from the US telecommunications industry (WorldCom). *American Law and Economics Review*, **8**(3): 439-475.

Sanad, Z. and Al-Sartawi, A. 2021. Financial statements fraud and data mining: a review. In *European, Asian, Middle Eastern, North African Conference on Management & Information Systems* (pp. 407-414). Cham: Springer International Publishing.

Segal, S. 2016. Accounting frauds–review of advanced technologies to detect and prevent frauds. *Economics and Business Review*, **2**(4): 45-64.

Sharma, A. and Panigrahi, P.K. 2013. A review of financial accounting fraud detection based on data mining techniques. *arXiv preprint arXiv: 1309.3944*.

Smith, R.G. 2008. Coordinating individual and organisational responses to fraud. *Crime, Law and Social Change*, **49**: 379-396.

Sorunke, O.A. 2016. Personal ethics and fraudster motivation: The missing link in fraud triangle and fraud diamond theories. *International Journal of Academic Research in Business and Social Sciences*, **6**(2): 159-165.

Usman, A.K. and Shah, M.H. 2013. Critical success factors for preventing e-banking fraud. *Journal of Internet Banking and Commerce*, **18**(2): 1-15.

Wolfe, D.T. and Hermanson, D.R. 2004. The fraud diamond: Considering the four elements of fraud.

Young, S.D. 2020. Financial statement fraud: motivation, methods, and detection. In *Corporate Fraud Exposed: A Comprehensive and Holistic Approach* (pp. 321-339). Emerald Publishing Limited.

Yuri, I.A. and Sari, M.R. 2022. Fraud Awareness and Fraud Detection-Prevention Methods in The Indonesian Private and Public Sector. *Global Financial Accounting Journal*, **6**(1): 100-107.

Zhou, W. and Kapoor, G. 2011. Detecting evolutionary financial statement fraud. *Decision Ssupport Systems*, **50**(3): 570-575.