

# Utilisation of Fraud Management System in Prevention of Financial Scam in the Banking Sector

**Dr. J. Santosh Rupa**

Associate Professor, Welingkar Institute of Management, India  
\*Corresponding Author Email: santoshrupa.jaladi@welingkar.org

## Abstract

In this research article, many different types of strong and sustainable viewpoints about fraud management systems will be highlighted appropriately, to make proper understandings. Moreover, it will be signified in this paper that, Fraud is characteristic of many approaches, it is an overall emphasis in the search for patterns for the detection of fraud. Data scientists, on the other hand, can prevent insurance fraud using algorithms to detect patterns and irregularities. In addition, Premium misallocation fraud, which is a mix-up of premiums, can entail fraud.

## Keywords

Corporate disclosure, Financial department measurements, Fraud management system,

## INTRODUCTION

Money laundering may lead to loan fraud, but this sort of fraud isn't simply restricted to firms submitting misleading information on their mortgage applications. Moreover, if someone submits fraudulent information to secure a loan that is called loan fraud. Likewise, if a theft robs the identity of someone and requests a loan on their behalf, it is another form of loan fraud. Furthermore, if one has a bank loan and a scammer pulls money from such a line, it's in this classification. This research article will highlight many different kinds of strong and sustainable viewpoints such as risk management, developments, implementation, and benefits. The purpose of this study is to make proper justifications about fraud amendment's utilization process as it supports the financial sectors in a proper manner.

### Concept about Fraud management system

The detection of fraud is a series of actions followed to prevent in a proper manner the collection of money or property by false pretenses. The detection of fraud is utilized in various areas including banking and insurance. In banking, fraud may involve checking or credit cards being stolen. Other fraud can be caused by exaggerated losses or the only purpose of an accident. As mentioned by Romanov (2018), the detection can be challenging with an endless and increasing number of methods in which someone might conduct fraud. Activities such as restructuring, reduction of the capacity move to new informatics, or a breach of cybersecurity might decrease the ability of a company to identify fraud. On the other hand, this implies it is recommended to use measures such as in-time fraud surveillance such as financial fraud, location, devices utilized, sessions launched and authentication methods should be looked at by the organisms (Ruth *et al.*, 2017).

Fraud is typical of many repeated techniques; it is a general focus for detecting fraud in the search for patterns. On the other hand, data scientists can avoid fraud from insurance via

algorithms to discover trends and abnormalities. As suggested by Spink *et al.* (2016), fraud in insurance may be the excessive trade of the stockbrokers to increase charges. Fraud may involve premium misallocation fraud that is an embezzling of premiums. Other kinds of fraud included asset diversion, payment for workers, vehicle crashes, stolen or damaged cars, as well as domestic fire fraud. Financial profits are the reason behind all money laundering. There are a variety of ways in which fraud may occur in various contexts such as fraud in banking, insurance, state, and pharmaceutical sectors, for instance, can be conducted.

### Risks of financial scams in the banking industry and their impact

The *Fraud Risk Management Approach* is a fraud-management model that identifies, evaluates, mitigates, monitors, and reports on fraud to top executives across all processes. An effective strategy for fraud management can have a considerably favorable effect on the bank's total expenses of fraud. The 2019 KPMG Worldwide Banking Fraud Survey has recently issued findings of the global viewpoint in dealing with fraud risks by banks and financial institutions. The study contains answers from 43 banks across the world; one part of the survey is how schools and banks arrange their processes to control fraud. 52% of banks presently do not track the whole costs of managing fraud risk. However, that is extremely unexpected because the fraud level has grown from 95% in 2017 to 1.53% in 2018 as the percentage of revenue (Abdallah *et al.*, 2016). This data shows that it is not only vital to the investment client to have risk management programmed in place but also how the industry as a whole is affected.

Visibility into fraud-management procedures contributes to better choice on fraud detection. Moreover, an effective fraud risk management strategy increases knowledge of risks, responsibility, and openness of how banks and other financial institutions actively handle fraud. It also identifies the fraud as soon as it occurs and ultimately reacts efficiently to the

fraud events, according to Deloitte, allowing organizations to carry out checks that first prevent the fraud. A robust risk management platform provides a company-wide picture of suspicious behavior in all channels of transactions; helps mitigate illegal conduct in real-time and keep fraud inside this appetite for risk of the Bank.

### METHODS AND TECHNIQUES

In order to represent the proper methods and systems is important for the researcher and the study topic. Moreover, strong and sustainable methods and techniques allow the researcher to make proper justifications about the research topic of *“Fraud management’s utilization process”*. As mentioned by Sanusi *et al.* (2015), experts interested in processes in that particular area or who read the research are particularly interested in acquiring new knowledge that they may apply individually in this section. There are many different kinds of methods and techniques presented such as research approach, research design, and data collection methods.



**Figure 1: Methods & Techniques**  
(Source: Sanusi *et al.*, 2015)

As per this paper, researchers adopt *descriptive research design* as it helps to recreate proper informational data in a proper manner. In addition, a descriptive search approach is adopted by the researcher to make proper research valid as it supports the next researcher to make proper understanding in a proper manner. Moreover, the researcher also adopts secondary *qualitative research design* in order to make proper research analyses as it supports the trey arch to make proper justification about many different kinds of risk management such as financial frauds.

### RESULTS AND DISCUSSION

#### Development of Fraud management system

Proper protection against fraud implies that a company may find a solution to the difficulties that face immediately while minimizing the negative impact on business income. The biggest income crusher in the e-commerce business is having legitimate consumers banned. Finally, security

against fraud must be balanced with the requirement to pass more orders that are important for the business. A lot of aspects have to be taken into account while comparing tools. Although not all of these things will have an equal influence on company business, people ought to contribute to their decisions. As per the words of Floştoiu (2019), companies take action to defend themselves from fraudsters, as the organizations must guarantee they accept genuine transactions exclusively and give authentication processes immediately to make their anti-fraud approach effective. Once such activities are organized, customer experience without friction may be achieved while the danger of fraud-related losses can be minimized.

Software for detecting fraud analyzes and allocates risk rates for each of the operations. Processing actions with properties not deviating from the standard are permitted. If even one aspect of the transaction suggests suspected activities, the system stops or refuses it immediately and gives the user a warning. In order to improve efficiency, many of these systems apply both rules and machines. As mentioned by Power (2019), ML-friendly systems for fraud detection examine incoming information continually. Moreover, effective data collection also implies that most orders are no longer to be reviewed by workers. "Some enterprises spend large amounts of money manually analyzing scam transactions. They have a big staff devoted to this work as the overhead for human fraud checks may be significantly reduced or even removed with a system based on ML fraud detection.

### IMPLEMENTATION

Fraud protection and detection are all about speed for today's financial institutions. However, most companies usually have a window shorter than a second to locate a transaction that might be fraudulent. The use of analytics to discover odd trends in accordance with loan robbery, bank fraud or laundering can aid automated fraud prevention systems. Therefore, with numerous channels and thousand activities a day, a fraud detection system is needed very swiftly to handle transactions. If only 0.3% of the panes are missing, big banks can lose \$10 million or more a year. As suggested by Floştoiu (2019), in order to process and analyze transactions quicker, in addition to an exceptionally fast CEP, companies' fraud detection and prevention systems depend on in-house data storage. With the company's fraud prevention and detection, solution businesses may retain the rules regarding potential fraudulent conduct in mind rather than need the system to image just a database for every transaction, in order to cut time complexity and costs due to fraud.

Some verticals or regions might become more fraud-prone, but no company is completely risk-free. Therefore, all traders should take steps to prevent possible breaches from occurring. A company may suffer from high quantities of fraud, leading both to loss of income and reputation. Companies will work actively to avoid fraud, instead of using

a purely reactive strategy, through partnerships with an experienced payment service provider such as merchantman as they discuss major techniques to fraud prevention in the upcoming chapters. As suggested by Tworek (2019), before this happens, it is better to deal with fraud than afterward as traders may halt fraud in their paths by maintaining this attitude and must not worry about continuing the damage limitation. Furthermore, there are a number of measures to detect fraud, including day-to-day traffic tracking and monitoring declining purchases from certain regions.

### BENEFITS

A PSP with a series of fraud detection technologies is the most efficient approach for traders to prevent fraud. It makes sense to monitor and aggressively identify fraudulent conduct by the firm that processes customer payments. As mentioned by Floștoiu (2019), fraud rules all work to achieve the proper mix between decreasing company risks of fraud significantly and continuing to enable large traffic levels; their rules should be a filter rather than a barred door. It can be tending to limit traffic for the sake of preventing fraud, but companies should be able to reach a lucrative compromise via experience and working with a reputable payment partner. For example, a gaming operator should be mindful that there are many cellular payments or payments using digital wallets. For illustration, the rules that should be set for the risk engine should be relevant to a particular vertical region.



**Figure 2:** Benefits of Fraud management systems  
(Source: Floștoiu, 2019)

In addition, these rules should come from a comprehensive study of current fraud information that allows you to identify and avoid patterns of fraudulent activity. If risk criteria are specified, the IP address or whether 3D Secure 2 has been applied is useful to a geo-location factor. Fraud may sneak beneath the radar or process of transactions without real-time monitoring. At merchantpay, the value of their data is maximized in order to avoid fraud before it occurs and their 24/7 continuous monitoring helps to control corporate fraud.

On the other hand, companies can control all the tradesmen's accounts using various processes and rules to improve the identification of questionable behaviour patterns utilizing advanced real-time fraud protection technologies. It might be difficult in the e-commerce industry to determine whether a consumer is who this is. It is thus necessary that methods are developed to compare and validate the identification of the card, such as links between computers, location, and anonymised personal data. It will also evaluate if the device utilized was hacked or has been previously fraud-related.

### CONCLUSION

As a strong and sustainable conclusion, it can be stated that the Fraud Risk Management Framework can be applied that discovers, assesses, mitigates, watches and exposes fraud to senior officials throughout the whole process. Fraud organizational structure provides an efficient theft management program may significantly advantageously affect the total fraud expenditure of the bank. The Worldwide Financial Crime Survey 2019 has just published results about the higher source on banks' or commercial banks' fraudulent threats. Therefore, fraud detection is a number of steps that have been taken to ensure that funds or property are not properly collected by fraudulent pretext. In numerous industries, including financial services, the detection of fraud is used. Fraud in banking may include checks or the theft of credit cards. Other fraud might be due to excessive losses or to an accident's only aim.

### REFERENCES

- [1] Abdallah, A., Maarof, M.A. and Zainal, A., 2016. Fraud detection system: A survey. *Journal of Network and Computer Applications*, 68, pp.90-113.
- [2] Dabbagoglu, K., 2018. Fraud in businesses and internal control system. *Journal of Modern Accounting and Auditing*, 8(7), p.983.
- [3] Floștoiu, S., 2019. The relationship between internal audit and fraud. *Bulletin Scientific*, 17(1).
- [4] Mohd-Sanusi, Z., Khalid, N.H. and Mahir, A., 2015. An evaluation of clients' fraud reasoning motives in assessing fraud risks: From the perspective of external and internal auditors. *Procedia Economics and Finance*, 31, pp.2-12.
- [5] Power, M., 2019. The apparatus of fraud risk. *Accounting, Organizations and Society*, 38(6-7), pp.525-543.
- [6] Romanov, D.V., 2018. The concept of anti-fraud management in international logistics. In *Антропоцентрические науки: инновационный взгляд на образование и развитие личности* (pp. 323-324).
- [7] Skoczylas-Tworek, A., 2019. The application of the three lines of defense concept in risk management and fraud risk on the example selected listed companies. *Economic and Social Development: Book of Proceedings*, pp.190-202.
- [8] Spink, J., Moyer, D.C. and Speier-Pero, C., 2016. Introducing the food fraud initial screening model (FFIS). *Food Control*, 69, pp.306-314.
- [9] van Ruth, S.M., Huisman, W. and Luning, P.A., 2017. Food fraud vulnerability and its key factors. *Trends in Food Science & Technology*, 67, pp.70-75.