S o u t h A s i a n J o u r n a l o f M a r k e t i n g & M a n a g e m e n t R e s e a r c h (S A J M M R)

(Double Blind Refereed & Peer Reviewed International Journal)

INVESTIGATING IDENTITY FRAUD MANAGEMENT PRACTICES IN E-TAIL SECTOR

Gulista Khan*

*Faculty of Engineering, Teerthanker Mahaveer University,
Moradabad, Uttar Pradesh, INDIA
Email id: gulista.engineering@gmail.com

ABSTRACT

Identity theft is becoming a bigger problem for internet retailers. The research on this topic is fragmented, and none of the studies take a comprehensive look at identity theft management methods in the online retail environment. As a result, the goal of this paper is to look at identity fraud management methods and provide a complete set of guidelines for the e-commerce industry. The research discovered that there is a lack of literature on identity fraud management methods. The results also show that businesses see identity fraud as a technical problem, which is one of the main causes for a lack of efficient identity fraud management. This research recommends that e-tailors should be created in technical, human, and organizational elements to cope with this problem as a management challenge. This research is restricted to data from publicly available sources. Studies based on actual data will be useful in bolstering this study's thesis; furthermore, future studies should cover a broad range of datasets. This research will assist e-commerce businesses in comprehending the whole identity fraud management process, as well as developing and implementing a complete set of practices at each step for successful identity fraud management. This research adds to the body of knowledge by integrating current literature at each step of fraud management and taking into account social, organizational, and technical factors. It would also assist academics in gaining a comprehensive knowledge of existing research and will offer up new avenues for future research.

KEYWORDS: *E-tailer, Fraud management, Identity fraud, Identity theft, Managerial practices.*

1. INTRODUCTION

E-commerce has revolutionized the way people conduct business by providing online merchants with limitless possibilities such as lower operating costs, more effective client relationships, and borderless services. However, these possibilities have also presented them with difficulties, particularly in the area of identity theft. When a fraudster utilizes personal information to impersonate someone else or establishes a false identity to make a transaction or start an account in order to defraud, this is known as identity fraud[1]. This scam has a negative impact on

industrialized nations such as the United States and the United Kingdom. In 2016, 15.4 million Americans were victims of identity theft, costing $16 billion; this was a 16 percent increase over the previous year. In the United Kingdom, the situation is almost same, with 172,919 instances of identity theft recorded by just Credit Industry Fraud Avoidance System (CIFAS) member companies in 2016, indicating a steady rise.

There are several research in the literature that look at different elements of identity fraud management. Some academics have proposed frameworks in the provided context to offer a complete picture of the identity fraud management process, however these studies lack in-depth insights into the fraud management actions at each process level inside the business. On the other hand, other studies concentrate on only one or a few fraud management actions and procedures. As a result, no research provides a complete picture of identity fraud management methods at all levels. Furthermore, nothing is known about the nature of the problem, such as if it is a technical or organizational issue.

Organizations are unable to properly control identity thefts in the absence of such research; thus these scams continue to grow. As a result, the difficulties of controlling identity frauds in the e-commerce sector need a comprehensive strategy that includes practices at each level of fraud management and investigates the grounds to successfully fight it. It was essential to consolidate the existing literature on techniques at each level of identity fraud management in order to achieve the goals of this study[2]. Five well-known databases were used to conduct the literature search. This research includes only peer-reviewed publications. The findings indicate that no thorough research of methods for successful identity fraud management in the e-tail setting has been conducted. There were many papers that focused on one or two elements of identity fraud management, but only a few academics suggested a framework for complete fraud management. As a result, this article makes a unique addition by integrating the disparate literature in order to create a complete set of practices.

With the increasing usage of internet business possibilities, the frequency of identity scams has risen. These statistics only include frauds reported by CIFAS member organizations; the actual number of identity-related scams in the United Kingdom is likely to be greater. The large number of identity thefts is a major source of worry for internet businesses in the UK, since they suffer the brunt of the losses[2].

This research compiles a substantial and representative sample of the existing literature into a single, complete study. It will aid academics in comprehending the state of the art in identity fraud management and will open up new research paths in the future. This research added to the existing literature by defining a set of complete organizational, social, and technical elements of identity fraud management, giving it a holistic perspective. Future studies will be able to take a wider perspective of identity fraud management. Much of the study, according to the literature, is focused on the function of the e-tailer inside the confines of their company[3]. Other stakeholders, such as consumers, banks, and identity issuing agencies, have a vital role to play in the management of these scams, which is often overlooked. As a result, this study encourages academics to involve additional stakeholders in the creation of an effective identity fraud management system.

Identity fraud management is a major issue for e-tailers all over the world. This research will assist e-commerce managers in gaining a comprehensive understanding of identity fraud management. Identity fraud management has always been thought of as a technical problem[4]. This research provides a complete set of management strategies for dealing with identity theft successfully. Managers will be able to examine organizational, social, and technical

arrangements for improved performance in the management of identity frauds if they have a broader perspective of identity fraud management. Identity theft is carried out mostly by e-tailers, according to literature, and most identity information is taken at the customer's end. As a result, e-tailers should go above and beyond to raise awareness and educate consumers in order to reduce the danger of such scams.

Because fraud is a long-standing practice, there is a wealth of literature focused on different elements of fraud management. Concerning the behavioral elements of fraud management, it is a well-established notion that the fear of being detected and penalized may discourage prospective fraudsters. The deterrence theory, which has been extensively researched in many settings and has been shown to be important in controlling aberrant behavior, inspired the idea of altering the behavior of prospective fraudsters. Fear appeal ideas are at the heart of deterrence theory.

Fear appeals affect fraudsters' attitudes, intentions, and behavior, and may even prevent a scam. The importance of this deterrent has been proven in a variety of settings, including accounting and auditing, as well as employee theft. Similarly, although there are many studies that concentrate on consumer education and threat as fraud deterrent methods, there are none that provide a holistic perspective of identity fraud deterrence techniques in the e-tail sector. As a result, further study is required to provide a comprehensive picture of managerial techniques for preventing identity theft in e-commerce businesses[5].Despite the use of deterrents, scams continue to be attempted. The presence of a chance to perpetrate a fraud in the Fraud Triangle Theory refers to the system's limitations in preventing and detecting frauds. As a result, in addition to deterrent, businesses should have mechanisms in place to prevent and identify fraud.

Effective prevention, which is based on information security systems and organizational structures, is a major instrument for safeguarding against fraud attempts[6]. A successful anti-fraud measure is a well-designed preventive strategy. Various studies have been conducted to prevent identity theft, but no major study has been discovered to propose a set of complete practices in identity theft prevention. Despite the fact that security safeguards exist to prevent identity fraud attempts, research shows that criminals utilize real customers' information, allowing some fraudulent transactions to slip through the cracks. As a result, as the next step beyond prevention, businesses must identify these transactions. According to the available literature, fraud attempts are simply the consequence of an assumption of lack of detection, therefore businesses should invest in a robust detection system that also serves to instill a fear of being discovered and penalized. Having an automated detection system and verifying suspicious transactions are methods that have been suggested by many academics in various situations.

Furthermore, some fraud detection investigations are solely technical in nature. There is yet to be a research that covers the whole spectrum of detecting techniques in the e-commerce sector. When fraud is discovered, the next step is to stop it before it is completed or to minimize the fraud's consequences and prevent it from recurring. This is referred to as the mitigation stage in the fraud management domain. Mitigation is a crucial step of fraud management that enables you to reduce the consequences of identified fraud to a bare minimum by checking and confirming client identifiers[7]. It also entails the retrieval of a customer's credit history as well as the exchange of information.After fraud has been discovered and mitigated, it is essential to determine the kind of fraud, the techniques and means used, and the reasons why it slipped through the cracks in the prevention system.

This collection of procedures is known as fraud analysis in the field of fraud management. Identity fraud analysis is a crucial step in developing rules and methods for successful fraud management. Although there are several studies on fraud analysis in the literature, none of them

have presented a complete set of methods for identity fraud analysis in the e-tail industry. Anti-fraud rules provide layers of security for the organization and its workers at each level of fraud management[8]. The creation of an anti-fraud policy would aid in the protection of personal information that might be exploited in identity fraud, and such rules are intended to enhance the efficiency of identity theft management. Although there are several studies in the literature, none of them provide a comprehensive perspective of identity fraud management strategies in the e-commerce industry.

The above-mentioned fraud management phases concentrate on measures taken before and during a fraud attempt, but successful identity fraud management requires further investigations and prosecution in order to recoup fraud losses and bring criminals to justice. Although law enforcement authorities are responsible for fraud investigations, companies also have a role to play[9]. The phases of fraud investigation and prosecution are important in fraud management. Successful prosecutions assist businesses in recouping fraud damages. Second, a successful prosecution will send out a warning message to prospective fraudsters that they will be discovered and punished (deterrence). Third, it aids businesses in defending their reputation from fraudsters, and lastly, it maintains a stronger client relationship[3]. Although there are several research on fraud detection and prosecution in the literature, a complete set of methods for identity fraud management in the e-commerce industry is unknown.

As the preceding section demonstrates, the literature on identity fraud management is dispersed. Because the articles in this area concentrate on just a few issues, the management of identity theft in the e-commerce industry is not well known. E-tailers are losing a large part of their sales due to identity fraud losses due to the lack of research that takes a comprehensive perspective of identity fraud management methods. Academics face a research problem in the absence of such research. In this case, a single empirical research may not be sufficient to fully comprehend identity fraud management. In addition, a single or a few articles may not cover all of the organizational, social, and technical elements of fraud management at each of the eight phases[10]. This research attempts to bridge this gap by reviewing the existing literature in order to comprehend and advance a holistic perspective of identity fraud management, as well as suggesting methods at each level of identity fraud management. This study will also draw academic attention and offer new paths for research in the present environment. This research may also aid e-tailer management in preventing such scams, reducing company losses, and establishing positive client relationships.

2. DISCUSSION

Identity fraud is often regarded as a technical problem in the internet commercial world. As a result, a significant percentage of publications are constrained by technical constraints. While the bulk of research have concentrated on one or two phases of fraud management, this paper examines the problem holistically to encompass all eight stages of fraud management and suggests organizational, social, and technical solutions. Various research on each step of fraud management may be found in the literature. Some research on deterrence have concentrated on both elements, i.e. consumer education and fear appeal, while the majority of studies have focused on either customer education or fear appeal.

Although there has been considerable study on many areas of deterrence, the least has been done in the area of identity fraud management in the e-tail environment. The bulk of the literature on the preventive stage focuses on information security and data breach, which are important aspects of identity fraud prevention, but more is required in this area. The majority of the research on preventing identity fraud focuses on information security and authentication. The

importance of detection in fraud management has piqued the interest of numerous academics. The significance of fraud detection is also shown by the huge number of publications on the subject (see Table V). Extant literature focuses on behavioral factors, biometric technology, and cue-based auto-detection systems for fraud detection. The existing research recommends real-time mitigation to reduce fraud losses and account recovery.

At present time, the majority of studies recommend that customers' records be kept and updated on a regular basis, since this will aid in verifying real client identities in the event of a questionable transaction. Some publications also recommend calling consumers to verify their identities. Knowledge exchange is also suggested by certain writers for successful mitigation. The majority of fraud analysis research are concerned with information security concerns. More study is required to better understand the importance of identity fraud analysis and associated procedures, particularly in the e-commerce industry. There is a substantial amount of literature on policy and related problems, although it is mainly in the context of information security. Despite the importance of policy in identity fraud management, no research in the e-tail environment were identified. The literature was also used to provide the details of management practices in policy creation, communication, awareness, and compliance.

Business companies should become engaged in private investigations and follow the prosecution process to achieve better outcomes, according to research on fraud investigations and prosecution. It is a widely held belief that law enforcement authorities are preoccupied with more pressing problems, thus e-tailers are recommended for private investigations and the establishment of tight cooperation with police. E-tailers need also be familiar with state laws surrounding fraud prosecution in order to prosecute effectively. The results indicate that although there are studies on each step of fraud management in the literature, none of them provide a complete picture of the problem and solutions.

These research are divided into three categories: technical, human, and organizational elements of identity fraud management. As a result, successful fraud control can be inferred as a combination of technical, human, and organizational approaches. Based on the existing literature, this research discovered that identity fraud management is a managerial problem that requires attention from all aspects of company operations, with an emphasis on top management. Top management, operational personnel, and strategic planning, as well as day-to-day company operations, would all need to contribute to the collected practices at each level. As a result, e-tailers should rethink their identity fraud management strategy and approach it as a managerial issue rather than a technical one.

3. CONCLUSION

Identity theft is a rising issue, particularly for online retailers across the globe. Every year, the frequency of identity thefts and the resulting losses rise. Some research on fraud management and associated problems have been published, although they are dispersed. As a result, none of the studies take a comprehensive look at identity fraud management and procedures. Due to the lack of such research, e-trailers are losing a substantial portion of their income to these scams. Identity frauds that are out of control may stymie the growth of e-commerce and result in substantial losses in the financial markets. Such a scenario presents a challenge for researchers and encourages academics to do study in this area in order to improve the real-world situation in the fight against identity theft. This research carefully analyzes the existing literature and provides a holistic perspective of identity fraud management as well as a complete set of associated practices to assist bridge this gap. We discovered that the majority of research are

focused on one or a few elements of fraud management, which may not cover the whole field. The majority of businesses, according to this study, regard identity theft as a technical problem.

deterrent, prevention, detection, mitigation, analysis, policy, investigation, and prosecution, are equally essential in managing identity frauds in the e-commerce industry. Only a few studies have fully focused on the organizational, social, and technical elements of fraud management, according to this research. Identity fraud is usually regarded as a technology problem, according to this study. Identity fraud management, according to this research, is a managerial rather than a technical problem, thus it should integrate technological, human, and organizational structures. This study synthesizes the existing fraud management literature, provides a holistic perspective of identity fraud management, and proposes managerial strategies at each step of the process. E-tail managers will also get guidelines on how to successfully handle identity theft, reduce losses, and build positive customer relationships. This study will also aid in the growth of e-commerce by increasing consumer confidence in online purchasing.

REFERENCES:

1. C. V. Amasiatu and M. H. Shah, "First party fraud: A review of the forms and motives of fraudulent consumer behaviours in e-tailing," *Int. J. Retail Distrib. Manag.*, vol. 42, no. 9, pp. 805–817, 2014, doi: 10.1108/IJRDM-05-2013-0112.

2. N. Caunter, "The Real Cost of Fraud to E-tailers," *Comput. Fraud Secur.*, vol. 2001, no. 8, p. 17, 2001, doi: 10.1016/s1361-3723(01)00817-x.

3. H. de B. Wijnholds and M. W. Little, "Regulatory Issues for Global E-Tailers: Marketing Implications - ProQuest," *Acad. Mark. Sci. Rev.*, vol. 2001, p. 1, 2001.

4. F. Kabuye, S. K. Nkundabanyanga, J. Opiso, and Z. Nakabuye, "Internal audit organisational status, competencies, activities and fraud management in the financial services sector," *Manag. Audit. J.*, 2017, doi: 10.1108/MAJ-09-2016-1452.

5. V. Van Vlasselaer, T. Eliassi-Rad, L. Akoglu, M. Snoeck, and B. Baesens, "GOTCHA! Network-based fraud detection for social security fraud," *Manage. Sci.*, vol. 63, no. 9, pp. 3090–3110, 2017, doi: 10.1287/mnsc.2016.2489.

6. J. West and M. Bhattacharya, "Intelligent financial fraud detection: A comprehensive review," *Computers and Security*, vol. 57. pp. 47–66, 2016, doi: 10.1016/j.cose.2015.09.005.

7. T. Allan and J. Zhan, "Towards fraud detection methodologies," 2010, doi: 10.1109/FUTURETECH.2010.5482631.

8. R. J. Bolton and D. J. Hand, "Statistical fraud detection: A review," *Statistical Science*, vol. 17, no. 3. pp. 235–255, 2002, doi: 10.1214/ss/1042727940.

9. C. Cody, V. Ford, and A. Siraj, "Decision tree learning for fraud detection in consumer energy consumption," in *Proceedings - 2015 IEEE 14th International Conference on Machine Learning and Applications, ICMLA 2015*, 2016, pp. 1175–1179, doi: 10.1109/ICMLA.2015.80.

10. J. Mendling *et al.*, "Blockchains for business process management - Challenges and opportunities," *ACM Trans. Manag. Inf. Syst.*, 2018, doi: 10.1145/3183367.