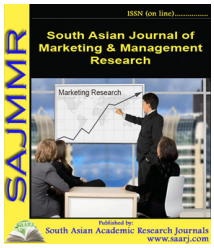
ISSN: 2249-877X Vol. 11, Issue 10, October 2021, Impact Factor: SJIF 2021= 7.642

South Asian Journal of Marketing & Management Research (SAJMMR)

(Double Blind Refereed & Peer Reviewed International Journal)



DOI: 10.5958/2249-877X.2021.00088.6

CONSUMER IDENTITY THEFT: INTRODUCTION AND FRAUD SOURCES AND DETECTION

Naheed Bi*

*Faculty of Education, Teerthanker Mahaveer University,
Moradabad, Uttar Pradesh, INDIA
Email id: nahid.education@tmu.ac.in

ABSTRACT

The purpose of this paper is to investigate consumer behaviour as it relates to identity theft and fraud. The components are physical prevention measures, account monitoring, agency monitoring, password security, and risky behaviour avoidance. These components were found to be almost orthogonal, implying that consumers tend to "buy into" a particular component of behaviour. The proposed model of consumer behaviour, while statistically significant, did not have high predictive value. Consumers use all the behaviours in one component without regard to other components. This can leave "holes" in consumer defense against identity theft and fraud. Consumer education on identity theft and fraud needs to stress that consumers need to employ all behaviours that can minimize risk and loss. This paper puts forward an initial model of consumer behaviours as it relates to identity theft and fraud. The derivation of the orthogonal components of behaviour is a new and important finding.

KEYWORDS: *Consumer Behaviour, Financial Crime, Fraud, Identity Theft, Identity Fraud, Theft.*

1. INTRODUCTION

Identity fraud is a growing concern especially for online retail organisations throughout the world. Every year the number of identity frauds and their losses are increasing. There have been some studies on fraud management and related issues but are scattered. Hence, none of the studies presents a holistic view of identity fraud management and practices in detail. In the absence of such studies, e-tailers are losing a significant amount of their revenues in these frauds[1]. Uncontrolled situation of identity frauds may also hinder the development of e-commerce and significant loss in capital markets. Such a situation is also a challenge for researchers and invites academics to research in this field to change the real-world situation against identity frauds.

To help bridging this gap, this study systematically reviews the extant literature and presents a holistic view of identity fraud management and forwards a comprehensive set of related

practices. We found that most of the studies are focused on one or some aspects, which may not cover the whole of fraud management. This study also found that most firms treat identity frauds as a technological issue. We found that the eight stages of fraud management named as deterrence, prevention, detection, mitigation, analysis, policy, investigation and prosecution, are equally important to manage identity frauds in e-tail sector.

Fraud is an old activity, so the literature is rich focusing on various aspects of fraud management. Regarding the behavioural aspects of fraud management, it is a well-established argument that the potential fraudsters can be deterred by the fear of being caught and punished[2]. The concept of changing the behaviour of potential fraudsters is derived from the deterrence theory, which has widely been studied in various contexts and is proved to be significant to control the deviant behaviour. The root of deterrence theory lies in the fear appeal theories. The fear appeals influence attitude, intention and behaviour of fraudsters and may prevent a fraud. So far, the significance of this deterrence has been confirmed in various contexts mainly in accounting and audit and employee theft. Similarly, there are numerous studies focused on customer education and threat as measures of fraud deterrence, but there are no studies presenting a comprehensive view of identity fraud deterrence practices in relation to the e-tail industry. Therefore, research is needed to present a holistic picture of managerial practices for identity fraud deterrence in e-tail organisations. In spite of deterrent practices, frauds are still attempted[3]. One of the major reasons, in Fraud Triangle Theory is the existence of an opportunity of committing a fraud, which refers to the system's weaknesses to prevent and detect frauds. What follows is that in addition to deterrence, organisations should also have systems to prevent and detect frauds.

This study found that identity fraud is generally treated as a technological issue, only a few studies have comprehensively focused to include organisational, social and technological aspects of fraud management. This study suggests that identity fraud management is a managerial issue rather than a technological, so it should include technological, human and organisational arrangements. This research synthesises the extant literature on fraud management, presents a holistic view of identity fraud management and suggests managerial practices at each stage of identity fraud management. Guidelines are also given for e-tail managers to effectively manage identity fraud, control losses and develop favourable customer relationship[4]. This research will also help in building customers' trust on online shopping, which will lead to e-commerce development.

The quintessential crimes of the information age are identity theft and the use of stolen identity to commit identity fraud. Management of identity fraud is a significant challenge for e-tailers throughout the globe. This study will help e-tail managers to understand a holistic view of identity fraud management. Generally, identity fraud management has been regarded as a technological issue. This study presents a comprehensive set of managerial practices to effectively manage identity frauds. Broader view of identity fraud management will also help managers to consider organisational, social and technological arrangements towards better performance in the management of identity frauds[5]. E-tailers are the ultimate bearers of identity frauds and literature suggests that mostly identity information is stolen at customer side. Therefore, e-tailers should go beyond the boundaries to create awareness and educate customers to minimise the risk of such frauds.

The responsibility for identity theft prevention can be said to fall on three groups: the consumers that provide the information, the organisations (including businesses and governments) that collect and use the information, and legislative bodies (including national and regional governments) that regulate the handling of personal information. The Organisation for Economic

Cooperation and Development, for example, emphasises regulation and calls for the standardisation of definitions and statistics, the enactment of legislation to provide legal remedies for the victims, and deterrence and enforcement for the perpetrators. The privacy commissioner for the province of Ontario stresses the importance of the role of organisations in protecting personal information.

Despite all the efforts of legislators and organizations, however, the consumer still has a vital role in protecting his or her personal data. Carelessness or lack of attention on the part of the consumer such as neglecting to protect passwords, disposing of identity information in regular trash, failing to secure regular mail or access to personal laptops, or responding to "phishing" attacks, can undo all the preventative work of governments and businesses. These groups recognize this reality and have encouraged consumer education regarding identity theft and fraud. Consumers, now and in the future, will play a critical role in identity theft prevention and identity fraud detection. Without a concerted program of customer education, legislation and technical solutions cannot prevent identity theft and fraud.

Although measures are there to prevent identity fraud attacks, the literature findings reveal that fraudsters use genuine customers' information, as a result, some fraudulent transactions still pass through the security net[6]. Therefore, organisations need to detect these transactions as the next stage after prevention. The extant literature suggests that fraud attempt is merely a result of an assumption of the lack of detection, so organisations should have an effective detection system that also helps to create the fear of being caught and punished. The practices of having automated detection system and verification of suspicious transactions are recommended by various researchers in different contexts.

Once the fraud is detected, the next stage is to stop it before completion or to minimise the fraud effects and prevent it from reoccurring, in the fraud management domain, it is called mitigation stage. Mitigation is a significant stage of fraud management that allows keeping the effects of detected fraud to the minimum by verifying and validating the customer identifies. It also includes the recovery of customer credit history and information sharing[7]. Once fraud has been detected and mitigated, it is necessary to identify its type, methods and means used, and the reasons why it passed through the prevention system. In fraud management, this set of practices is called fraud analysis. Analysis of identity frauds is a critical stage that helps to develop policies and strategies for effective fraud management.

At each stage of fraud management, anti-fraud policies create layers of protection for the organization and its employees. Development of an anti-fraud policy would help to protect the personal information that may be used in identity fraudsand such policies are meant to improve the effectiveness of identity theft management[8]. The extant literature has some studies, but none of these presents a holistic view on identity fraud management policies in e-tail sector.This paper examines the precursors and attitudes that relate to the behaviours that consumers use to prevent and detect identity theft and fraud. Specifically, does past experience with identity theft and fraud relate to the level of concern about being a victim? And does the level of concern affect consumer behaviours?

Identity theft is the unauthorized access to personal information or documents; while identity fraud is a crime involving the use of false identity. Generally, most identity fraud relating to financial and credit accounts is categorized as existing account or new account. Existing account fraud involves the illegal use of an existing account or credit relationship[9]. New account fraud entails the creation of a new credit account using a fraudulent identity and subsequent illegal use. There is some discussion as to whether credit card theft and subsequent fraud should be

considered identity crimes. In most cases, the loss of a credit card and its subsequent fraudulent use is less damaging to the customer than the loss of cash. No personal information other than name and number is divulged, the card is usually replaced promptly, and the customer is not usually responsible for any fraudulent use.

Despite the importance of the role of consumers and significant survey work, there has been little analytical work done on the behaviour of consumers to prevent, detect and mitigate the effects of identity theft and fraud. identity fraud would exist in equilibrium, balancing the cost of increased fraud against the cost of increased conclusiveness in identification. In addition to these "macro" models, there are some "micro" models that address specific aspects of consumer behaviour concerning identity theft; for example, personal information disclosure, the effects of privacy seals, and behaviour in the online environment[9]. There appear to be no general theoretical models proposed for the behaviour of consumers in preventing and detecting identity theft and mitigating the effects of identity fraud. This paper explores the relationships between consumer experience, attitude and behaviour in relation to identity theft and fraud. In particular, it investigates the kind of theft/fraud experienced in the past in relation to the level of concern and change in the level of concern about identity theft, and the effects of concern on the behaviours of consumers. This approach very loosely follows the theory of reasoned action (TRA)[8].

At a high level, TRA proposes that beliefs affect attitudes which precede intentions which in turn result in behaviours. Within this study, behavioural data are captured and attitudes are operationalized as concerns over identity theft. Owing to the limitations of the data collected, intentions and beliefs are unavailable. There are, however, some data which may be antecedents of attitudes, i.e. past experience with identity theft and fraud. A high-level model diagram of the relationships, indicating that the level of concern is expected to have an impact on the behaviour components. Given the financial and emotional costs of identity theft and fraud, one might expect that those who have experienced identity theft and fraud would have a different attitude and be more concerned with the possibility of being a victim of identity theft in the future[10]. In particular, recent victims of identity theft and fraud may be expected to change their levels of concern.

Owing to the different characteristics of credit card fraud, the response in concern level could be at variance with those experiencing other identity fraud. There are many behaviours that consumers exhibit in preventing and detecting identity theft and fraud. It is useful to group these behaviours using factor analysis. Few researchers, however, have done so. This paper groups both online and offline identity theft and fraud prevention and mitigation behaviours into behavioural components.

2. DISCUSSION

The difference in concern level by those who experienced credit card theft and fraud and from those who experienced new account, existing account and other identity theft and fraud indicates that, in the view of consumers, credit card crime is distinct. This is probably due to the fact that credit card companies, and not consumers, take the risk for credit card fraud, provided that consumers notify their credit card issuers when credit cards are stolen, lost, or unauthorized payments are detected in the accounts. Indeed, the finding that consumers who have never been victims of identity theft are intermediate in level between the consumers that have been victims of credit card fraud and those who have been victims of other identity fraud, indicates the differences in attitudes of the two groups that have been victimized.

The effect of the timing of the experience of identity theft on the level of concern is somewhat surprising. When respondents were victims in the most recent year, whether it was credit card or other fraud, their concern levels were lower than those who were victims previously. On the other hand, a large number of victims in the most recent year reported their concern level was higher than the previous year. The implication of these two findings is that victims of identity theft and fraud in the most recent year previously had below average levels of concern. This suggests that consumers with low levels of concern are more likely to be victims. The five-component solution to the principal component analysis produces a logical categorization of identity theft prevention behaviours.

The final components of physical security, password security, avoidance of risky behaviours, and monitoring of accounts and agencies make intuitive sense. It is remarkable perhaps that the items loaded so cleanly. There is no reason other than general vigilance, for example, to expect that someone who shreds confidential documents would also use a locked mailbox. Conceivably, the most surprising finding is that the components are almost orthogonal. The correlations between most components are quite low. For example, individuals who monitor their bank accounts and credit cards do not necessarily also use physical security or avoid risky behaviours. It appears as if individuals "buy into" a form of identity theft protection and use all the behaviours associated with that form without reference to other forms. Consumers act selectively in the types of behaviours they employ.

3. CONCLUSION

This selectivity can have significant consequences for consumers. Consumers need to be encouraged to use all forms of defensive and detection behaviours if identity theft is to be avoided and if costs are to be minimized when identity fraud does occur. The effect of level of concern on identity theft and fraud prevention and mitigation behaviours is statistically significant but small. The reason is suggested by the fact that the behaviours of those who are not at all concerned about being victims are statistically the same as those who are extremely concerned. Those who take identity theft and fraud very seriously may use measures that they believe protect them from victimization.

Concern may thus be moderated by the perceived effectiveness of behaviours intended to prevent identity theft. Similar results were obtained for changes in behaviour. While changes in concern had statistically significant effects on the changes in most behaviours surveyed, the effect was small. Again, the changes in concern may have resulted from the perceived effects of changes in behaviour. While concern about being a victim of identity theft and fraud is influenced by and in turn influences consumer behaviours, the relationships are not strong or linear. Other attitudes may be more effective in explaining consumer behaviour. Rather than concern, perhaps better attitudes to measure would be the perceived prevalence and/or perceived seriousness of identity theft.

The contribution of this research is largely the identification of the principal components of consumer behaviours that are intended to reduce exposure to identity theft and fraud. The finding that the components are almost orthogonal adds a new dimension to the understanding of the ways consumers handle the threat of these offences. For practitioners, this highlights the need to educate consumers in the necessity of employing all forms of identity theft protection. This research also fills a "hole" in models between the macromodels that explain the overall functioning of identity theft and fraud, and "micro" models that concentrate on specific aspects of identity theft.

Identity theft and fraud are wide spread and have significant financial impacts in both the costs of prevention and the costs of fraud when prevention fails. In addition, there are emotional and psychological impacts on victims. While businesses and governments have significant roles to play in minimizing the occurrence and consequences of identity theft and fraud, a critical role remains for consumers. A better understanding of the factors that influence their defensive behaviours is key to controlling the greatest threat to consumers today.

REFERENCES:

1. J. Gilbert and N. Archer, "Consumer identity theft prevention and identity fraud detection behaviours," *J. Financ. Crime*, vol. 19, no. 1, pp. 20–36, 2011, doi: 10.1108/13590791211190704.

2. A. D. Smith, "Identity theft as a threat to CRM and e-commerce," *Electron. Gov.*, vol. 2, no. 2, pp. 219–246, 2005, doi: 10.1504/EG.2005.007096.

3. E. McNulty, "Boss, i think someone stole our customer data," *Harvard Business Review*, vol. 85, no. 9. 2007.

4. S. Romanosky, R. Sharp, and A. Acquisti, "Data Breaches and Identity Theft: When is Mandatory Disclosure Optimal?," in *Workshop on the Economics of Information Security (WEIS)*, 2010, pp. 1–34.

5. I. Sakharova, "Payment card fraud: Challenges and solutions," in *ISI 2012 - 2012 IEEE International Conference on Intelligence and Security Informatics: Cyberspace, Border, and Immigration Securities*, 2012, pp. 227–234, doi: 10.1109/ISI.2012.6284315.

6. P. Gibler, "Phishing, Pharming, Spimming, and Spoofing.," *Credit Union Exec. Newsl.*, vol. 31, no. 7, pp. 7–8, 2005.

7. G. Ashenmacher, "INDIGNITY: REDEFINING THE HARM CAUSED BY DATA BREACHES.," *Wake Forest Law Rev.*, vol. 51, no. 1, pp. 1–56, 2016.

8. P. Hille, G. Walsh, and S. Brach, "Understanding Online and Offline Consumer Behavior: Conceptualizing Fear of Online Identity Theft: a Qualitative Study and Model Development," *AMA Summer Educ. Conf. Proc.*, vol. 22, pp. 214–215, 2011.

9. R. Bose, "Intelligent technologies for managing fraud and identity theft," in *Proceedings - Third International Conference onInformation Technology: New Generations, ITNG 2006*, 2006, vol. 2006, pp. 446–451, doi: 10.1109/ITNG.2006.78.

10. N. Tariq, "Impact of Cyberattacks on Financial Institutions," *J. Internet Bank. Commer.*, 2018.