Identity Fraud Management: A Qualitative Study into the Managerial Practices in E-tail Sector

By

Zahoor Ahmed Soomro

A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy at the University of Central Lancashire.

December, 2018

uclan
University of Central Lancashire

STUDENT DECLARATION FORM

Concurrent registration for two or more academic awards

I declare that while registered as a candidate for the research degree, I have not been a registered candidate or enrolled student for another award of the University or other academic or professional institution

---

Material submitted for another award

I declare that no material contained in the thesis has been used in any other submission for an academic award and is solely my own work

---

Collaboration

Where a candidate's research programme is part of a collaborative project, the thesis must indicate in addition clearly the candidate's individual contribution and the extent of the collaboration. Please state below:

The whole work has been carried out by the undersigned, without any collaboration.

Signature of Candidate

Type of Award Doctor of Philosophy

School Lancashire School of Business and Enterprise

Abstract

E-commerce has offered many opportunities to business firms to minimise their operational costs, enhance the customer base and develop better customer relationships. These opportunities have also created some challenges, especially those related to identity frauds. Therefore, this study aims at understanding identity fraud management and analyses existing managerial practices at large e-tailers to suggest improvements.

To attain the objectives of this study, the qualitative approach of data collection was adopted. The interview method of data collection helped to get in-depth information about the context under study. The case study research approach was chosen to investigate the what, how and why of the issues and practices of identity fraud management. The data were collected at three large e-tailers based in the UK, in the course of 33 semi-structured interviews. For the analysis, thematic approach was adopted and the results were processed using single and cross-case analysis.

The findings revealed that identity fraud was one of the biggest challenges for e-tailers, as they are losing a significant amount of their revenues. Various types and methods of identity frauds have been explored. The results show that the case firms have the process of managing identity frauds, and the stages of fraud management suggested by Wilhelm (2004) were present. It was also found that e-tailers prioritised the technological aspects of fraud management, while the developing the skills and awareness of their staff was not given required focus, which may be one of the possible reasons for the existing deficiencies in fraud management. In fact, this study has found that human factor is a critical aspect of fraud management. It has also been established that customer education is not carried out effectively, despite the fact that identity theft mostly occurs at the customer side. A more active and explicit stance against identity fraud is recommended. However, because the e-tailers operate in a highly competitive environment, there is a trade-off between putting up extra security layers and the ease for customers for making a purchase, making identity fraud management ever more challenging for them.

Present study contributes to the body of literature by understanding identity fraud management and analysing current managerial practices at large e-tailers. Reflecting on the theoretical and empirical data, e-tailers are forwarded some novel practices for better management of identity frauds. Additionally, e-tailers are also suggested improvements in existing managerial practices**.** This study may help e-tailers to effectively manage identity frauds, which will result in reduced fraud losses, better firm image and favourable customer relations and offering the society a secure environment for online shopping.

Finally, a conceptual framework has been suggested for effective management of identity frauds in e-tail context. Managerial practices are suggested and guidelines are given at each stage of the framework for effective management of identity frauds.

Table of Contents

List of Tables

List of Figures

ACKNOWLEDGEMENTS

Thanks to Almighty Allah for bestowing upon men his blessing that encouraged and helped me throughout such a long and challenging process of completion of my PhD project. He also made me consistent, passionate and hardworking and kept me in a good health, which was the pre-requisite to complete this long journey.

Next, I am very grateful to my parents for their prayers and encouragement that enabled me with continued confidence towards the achievement of this goal. The role of my beloved wife is also admirable here as she always concealed the sufferings and supported me to towards my goal. Throughout the process, my children also suffered but understood my position and were a source of motivation for me.

During the journey there were also many other peoples contributing to my success. First and foremost, I would like to extend my gratitude to the supervision team: Dr: Mahmood Hussain Shah, Dr: Matthias Meckel, Prof: Andrei Kuznetsov and Dr Mitchell Jonathan Larson, whose presence was like a candle in the dark. Their continued guidance and support not only broadened my horizons but also helped to make the project accomplished. I am highly indebted to these dignitaries. Many thanks to Professor Waqar Ahmed, whose guidance and motivation made me focus on the research goal. I am also indebted to the management and staff of the case firms, especially, Mr: Gary Summersgill for his continued efforts to get access on the empirical data.

Finally, I cannot forget the big support from my sponsoring institute; Shah Abdul Latif University, Khairpur Mirs' Sindh, for the financial support to achieve this degree.

List of Abbreviations

App	Application
CEO	Chief Executive Officer
CIFAS	Credit Industry Fraud Avoidance System
COO	Chief Operating Officer
CV	Curriculum Vitae
E-tail	Electronic Retail (Online Retail**)**
E-tailer	Electronic Retailer (Online Retailer)
HRM	Human Resources Management
HM	Her Majesty
ID	Identity
IDF	Identity Fraud
IDFM	Identity Fraud Management
IDT	Identity Theft
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
IT	Information Technology
MAC	Media Access Control
RBF	Role Based Framework
UK	United Kingdom
USA	United States of America
USD	United States Dollar

CHAPTER 1
INTRODUCTION

1.1 Background of the Study

The advancements in technologies have changed the way of life; especially shopping habits have been changing quickly. Online shopping is taking the place of high street shopping. It saves time and offers a better comparison of products and prices. As a result, an increasing number of business organisations is getting involved in e-tailing. The nature and methods of frauds are also changing with the changes in selling practices. Identity fraud has become a challenging type of fraud for e-tailers, especially in developed countries like the USA, the UK and others.

In the USA, 15.1 million customers suffered identity fraud in 2016 (Javelin Strategy, 2018). Every two seconds, an American becomes a victim of identity fraud. The number of victims increases each year (see Table 2.3). Identity fraud accounts for billions of dollars in losses: in 2016 alone they amounted to US$ 16 billion (Javelin Strategy, 2018). Such losses, on the one hand, increase the cost of doing online business, on the other hand, discourage customers from online shopping; hence identity fraud is a significant challenge to e-tailers.

In the UK, the situation is similar to the USA. Table 2.4 presents the picture of online fraud from 2013 to the mid of 2017. In 2013, 177,476 cases of identity-related fraud were reported by CIFAS member organisations, which grew to 227,003 in 2015 (CIFAS, 2018b). The actual number of instances of identity fraud would be higher, as not all online business firms are members of CIFAS[1].

The increasing number of IDFs is ever expanding the challenges for e-tailers not only in the UK but for throughout the globe. Usually, when calculating the identity fraud losses, only direct losses are accounted for. The indirect losses such as reduction in sales, a decrease in market share, share price drop, and other legal costs have a significant adverse impact on business firms.

[1] Credit Industry Fraud Avoidance System (CIFAS) is a non-profit membership organisation, based in the UK. Established in 1988, CIFAS is a leading fraud prevention service. It offer fraud database and networking opportunities for its member organisations and supports the fraud victims. Currently it has more than 350 member organisations.

Identity fraud in e-tailing has attracted the attention of academics. The extent literature covers different aspects of the problem. Bai and Chen (2013), Guitton (2012), Leasure and Zhang (2017) and Shamsi *et al*. (2016) deal with the behavioural aspect of fraud management. The focus of these studies is limited to the deterrence of fraud. In turn, studies by Alrashed (2016), Baz, *et al*. (2017), Prakash *et al*. (2015), Teh *et al*. (2016) and others investigate the technical aspects of fraud prevention. Research by Al-Jumeily *et al*. (2015), Carneiro *et al*. (2017) and Dorfleitner and Jahnes (2014) has its emphasis on the detection mechanism of IDFs.

In addition, there have been some studies on comprehensive management of identity frauds, such as Jamieson *et al.* (2007) and Kumar *et al.* (2007) but they have focused on internal fraud from an audit perspective and on developing collaboration in fraud management respectively. So far, no significant study has sought to suggest better managerial practices in IDFM in e-tail sector. This study aims to bridge this gap.

1.2 Aim and Objectives of the Study

This study provides an understanding of identity fraud management and analyses the managerial practices in e-tailing, through a qualitative approach and suggest improvements. Therefore the objectives of the study are:

- To explore types of identity fraud facing the e-tail sector in the UK.
- To investigate the existing managerial practices of IDFM in e-tail sector.
- To extend the fraud management lifecycle framework (Wilhelm, 2004) for improving managerial practices in IDFM in e-tail sector.

A case study research design was selected for its merits and advantages to achieve the above objectives. This approach allowed the researcher to study the real life events and managerial practices and to examine phenomena under examination in greater depth (Yin, 2014). The case study design was also helpful to know the elements behind management actions, revealed organisational culture and human resources management activities (Metwally, 2013) and provided information about activities, culture and norms of the organisation (Stake, 2013). The case study approach with interviews as the data collection method, also helped to interact with the practitioners who dealt with the real world IDFM issues to get first-hand information in the problem under investigation (Gibbert *et al.*, 2008).

As a research method, case study incorporates a variety of means of data collection. As this study was aimed at analysing managerial practices, an in-depth investigation of existing practices was employed to establish “how” and “why” of IDFM issues, for which qualitative data collection method was a better choice (Yin, 2014). Data was collected through a series of semi-structured interviews held at three large e-tailers in the UK.

Organisations for this study were selected on the basis of replication logic, reflecting the fact that in multiple case study research cases are not selected to be the representatives of the whole but for similar (literal) or contrary (theoretical) results (Yin, 2014). For this study, the cases were selected for similarities; with only three cases, these are to be selected for predicted similar results (Yin, 2014). Although, the selection of the case firms was not tactical as the most of these large e-tailers have shared characteristics in relation to identity fraud issues and management. However, the selection criteria was set as; a) the firm must be among the top 25 businesses engaged in online retailing, b) must be based in the UK and c) must be an independent organisation and not a market place.

Questions for the interviews were designed to reflect the findings obtained during the analysis of the extant literature on the fraud management lifecycle framework proposed by Wilhelm (2004). A pilot case study was conducted to test the interview questions, data collection techniques, time management and data analysis methods. All in all, 33 interviews were conducted at three firms.

This study used the thematic analysis approach, which offers flexibility in developing themes by thoroughly reading and re-reading the data set. The managerial practices could also be extracted through in-depth study of the data; such approach helped in exploring and analysing the managerial practices.

1.3 Significance of this Study

This study helps to identify and understand the weaknesses and limitations of managerial practices that exist at each stage of IDFM. Based on the analysis process and reflections from the literature, guidelines are suggested to improve IDFM in large e-tailers in the UK.

The analysis of the fraud management framework undertaken in this thesis will help large e-tailers to improve the existing managerial practices and adopt better ones to enhance the effectiveness of IDFM. In accordance with the stages of fraud management, e-tailers are offered a number of recommendations to help business managers adopt a holistic appraoch for better control on losses associated with identity frauds.

Better managerial practices will also help the e-tailers to establish favourable customer relations and provide safe online shopping environment, providing these e-tailers with a competitive advantage. Unlike some other studies, this research anchors its recommendation in the analysis of a comprehensive set of activities at each stage of the framework, covering human, technological and procedural aspects of IDFM. This study also provides insights in the development, communication and awareness of and compliance with IDFM policies, which may help managers to ensure strategic actions towards the achievement of business objectives.

This study offers suggestions for a balanced and appropriate management focus on managerial practices at each stage of IDFM. The findings reveal that generally, the e-tailers are not giving proper attention to some of the stages of fraud management, which undermines its effectiveness. Importantly, this research provides evidence that calls for putting more emphasis on human aspects of IDFM. In particular, maintaining staff awareness and professional training are identified as the means of increasing the efficiency of fraud management.

The role of customer education is also highlighted. Finally, tactical practices are advised to show the firms' attitude to safeguard their customers and taking legal actions against fraudsters. E-tailers are also advised to publicise their measures against the fraudsters and send messages to the society that can reinforce customers' confidence in the safety of online shopping and the potency of threat for fraudsters, which simultaneously may enhance fraud deterrence and develop customer trust.

With the help of the recommended framework, e-tailers should be able to design and modify the managerial practices to improve the methods, procedures and policies, strategies and tools of IDFM. It will also help the e-tailers to enhance the human abilities to manage identity frauds, through feedback, training, knowledge and skill development.

Like other studies, this research has some limitations. Firstly, the present study relies on data collected from a limited number of large e-tail firms, so the results of this study may not be generalizable to the whole population of e-tailers. Therefore, research based on survey would help in generalising the outcomes of this research. Secondly, the present research used qualitative method of data collection, with limited number of respondents, although, the qualitative data give more detail and in-depth insight into the problem under study but it does not offer testing hypothesis or propositions, so in future qualitative studies are suggested to cover this limitation of present study.

Another limitation, which may have significant impact on outcomes of future research, is the size of case firms and the economies these operate in. Present study focused on large firms operating in a developed economy, whereas small and medium e-tailers and those operating in developing economies may have variant practices for managing identity frauds, because of financial, cultural different managerial and economic conditions. Therefore, more studies are suggested encompassing different economic conditions and various sizes.

1.4 Structure of the Thesis

The thesis consists of six chapters and is structured as follows.

Chapter 2: This chapter provides an in-depth insight into the identity fraud types and existing body of knowledge on its management. Various frameworks are explored and analysed, and the managerial practices at each stage of IDFM are presented. A critical analysis of the extant research is given, and a research gap is identified.

Chapter 3: In this chapter, the research philosophies and methods are presented. The research design is explained and justified.

Chapter 4: The data collected from the case firms are presented and analysed in the context of the extant literature. For each company guidelines are developed to improve their practices of IDFM.

Chapter 5: The chapter presents a cross-case analysis of the collected results. It also discusses the managerial practices at each firm. The extended framework is explained and improvements are suggested at each stage of the framework. The novelty of this research is explicated in this chapter.

Chapter 6: This chapter summarises the research outcomes and offers a brief on the accomplishment of this study. The key finds are highlighted and the extended framework is described. Finally, the research limitations are specified and avenues for future research are suggested.

The rest of this thesis explains these chapters in detail.

CHAPTER 2
LITERATURE REVIEW

2.1 Introduction

Literature review is a critical part of an academic research. It syndicates outcomes of many studies producing a holistic conceptual frame for a study. It helps to categorise, and investigate the structure and dynamics of change within a body of literature (Nairn *et al.*, 2007). The literature review process starts with articles focusing on the significant facts on fraud and managerial practices in broader contexts.

In the next phase, articles focusing on the analytical approaches to managerial practices specific to fraud are included. For theoretical reflections, articles on theories of fraud management are also reviewed. These highlight mostly the behavioural aspects of fraud management and help to understand its broader aspects. At the final stage, articles related to managerial practices and frameworks in fraud management are reviewed. This allows to get a comprehensive picture of identity fraud management covering all aspects of identity fraud management.

This chapter discusses various concepts regarding fraud management. The types and the impact of identity fraud are examined as well as the role of managerial practices in fraud management. The concept of the fraud management is established, and stages of fraud management are explained. This chapter also scrutinises various frameworks suggested for effective fraud management. Finally, the framework selection process is described, and a research gap is identified.

2.2 Understanding Identity Fraud in E-tail Sector

The shopping preferences are changed with the introduction of internet as 82% of internet users in the UK prefer online shopping (Xiao, 2017). Due to this shift in shopping, traditional businesses have entered into online business and many new online businesses are also set up. The online business offers many advantages to the entrepreneurs especially related to investment and low cast of business operations. On the other hand online shopping provide many opportunities to the buyers, which a traditional market cannot offer. Due to these reasons, online business is fast growing especially in the UK. These opportunities of e-tail business do come with a cost of online frauds. Identity frauds make more than half of these crimes (CIFAS, 2018b). Identity fraud (referred as IDF in the remaining document) is the fraud committed by using the stolen or fabricated identity information to make an online purchase or to skip financial charges. It is the most common type of fraud in online retail organisations (CIFAS, 2015) and sometimes termed as identity theft.

2.2.1 Identity Fraud

The term identity in this study refers to any information specific to an individual or an organisation such as the name and date of birth, as well as information contained in personal documents such as the driving licence, passport, identity card and others. It also includes bank details, credit and debit card numbers, passcodes, passwords, any account information with organisations, tax returns, health card numbers, or any specific data that make it possible to identify an individual or organisation. IDF is a type of fraud attempted by using stolen or fictitious identity information. IDFs are committed to gain money, purchase goods and services and avoid payment obligation through stolen or fabricated identity.

2.2.2 Methods of Stealing Identity Information

The methods of identity theft can be divided into two broad sections, online and traditional methods. Online or cyber-identity theft occurs with the help of information and communication technologies; these methods are highly organised and need technological expertise (Roberts *et al.*, 2013). Some common methods of cyber-identity theft are phishing, key logging, malware and social engineering[2]. These are the technology-based methods, so countermeasures need technological solutions; management here can support IT professionals to counter such fraud attempts.

The traditional methods of identity theft are mostly non-technical. These include theft of mail (which may contain personal or credit card information), lost purse, shoulder surfacing (when someone tries to peak over the victim's shoulders to get identity

[2] Phishing is a cybercrime involving contacting the targeted individuals through emails, phone calls or text messages for the purpose of extracting sensitive personal data. A key logger is a software which records every key stroke of a computer, mobile phone or such other devices. The key logger is installed into the target device through different methods and the hacker than knows every key stroke; thus identity information is stolen to commit frauds. Malware (in short for malicious software) is a software, designed to damage or gain authorised access to a computer system, to get identity information with a view to committing IDFs. In turn, social engineering refers to identity theft through social media.

information) and friendly frauds. The latter occurs when a fraudster gets personal information from a friend or a family member by abusing the existing relations of trust. Mostly traditional attempts of identity theft occur with customers, but effective customer education can help to prevent such information theft. IDFs are also committed using fabricated information, in which the fraudsters make fictitious identity and try to use it for personal gain.

2.3 Impact of Identity Frauds on E-Tailers

Identity fraud losses are a growing concern, especially for online business organisations. In the USA, 15.4 million customers suffered identity fraud in 2016 (Javelin Strategy, 2018). Every two seconds, an American becomes a victim of identity fraud. The number of victims increases each year (see Table 2.1). Identity fraud accounts for billions of dollars in loss.

Table 2.1 shows that USA business firms are suffering significant losses on account of IDFs. The table also presents the amount of losses in IDFs from 2014-2016. Such amount of losses, on the one hand, discourages customers from online shopping while, on the other hand, increases the cost of doing online business.

Table 2. 1 The impact of identity fraud on US business

Number of Identity fraud victims			Amount lost to identity fraud (Billion USD)		
2014	2015	2016	2014	2015	2016
12.7	13.1	15.4	16.2	15.3	16.0

Source: Javelin Strategy (2018)

In the UK, the situation is similar to the USA. Table 2.2 presents the picture of online fraud in 2013-2016. The table shows that identity related frauds are the leading type of frauds, and increasing year by year. The data on IDFs from CIFAS member organisations is shown in the following table.

Table 2. 2 The nature and scale of frauds reported by CIFAS member organisations

Fraud Type	Number of frauds			
	2013	2014	2015	2016
Asset Conversion Fraud	301	323	258	381
Application Fraud	38,573	37,960	41,186	31,559
False Insurance Claims	342	324	366	496
Facility/Account Takeover Fraud	30,349	18,771	15,497	22,525
Identity Fraud	108,554	113,838	169,592	172,919
Misuse of Facility Fraud	42,956	105,779	94,001	96,803
Total	221,075	276,993	320,900	324,683

Source: (CIFAS, 2018a; CIFAS, 2018b; CIFAS, 2018c)

Identity-related fraud makes a major contribution to overall business frauds in the UK. Table 2.2 contains data on the share of identity-related fraud over the last five years. The Table shows that the number of IDF is continuously increasing. Such a large number of identity frauds is a severe concern to online business firms in the UK, as business firms bear most of these losses (Brody *et al.*, 2007). Furthermore, the data on identity related frauds trends and it share in total frauds is presented in the following table.

Table 2. 3 Identity-related frauds 2013-2017

Fraud type	2013 % of total frauds	2014 % of total frauds	2015 % of total frauds	2016 % of total frauds	2017 % of total frauds (Jan-Jul)
Identity fraud	108,554 (49.1%)	113,838 (41%)	169,592 (52.9%)	172,919 (53.3%)	89000 (56%)
Account/ Facility takeover fraud	30,349 (13.7%)	18,771 (6.8%)	15,497 (4.9%)	22,525 (6.9%)	N/A
Application fraud	38,573 (17.4%)	37,960 (13.7%)	41,186 (12.9%)	31,559 (9.7%)	N/A
Total Identity related frauds	177,476 (80.3%)	170,569 (61.6%)	226,275 (70.5%)	227,003 (69.9%)	N/A

Source: (CIFAS, 2018a; CIFAS, 2018b; CIFAS, 2018c)

Table 2.3 represents the identity related frauds and their trends. The firms calculate application and account takeover frauds separately from other identity frauds so for the purpose of this study these are added to give a comprehensive picture of IDFs. The table shows that IDFs are continuously at inclining trend. It also reveals that the number of IDFs has significantly increased in last four years except 2014. The CIFAS reports show that fraud in e-tail sector is growing at higher rate as compared to other sectors; it increased by 28% from 2013 to 2016 (CIFAS, 2018a; CIFAS, 2018b).

According to CIFAS (2018c), IDFs (excluding the account takeover and application fraud) for first six months of 2017 increased by 5%, from the corresponding period the year before, accounting for 56% of the total number of frauds reported by its member organisations. CIFAS also reports a sharp rise in IDF in e-tail sector. These figures confirm that IDF is a growing challenge for e-tailers. The figures presented in the above tables are limited to the CIFAS member organisations, so the actual number of IDFs may be higher than these. Additionally, the CIFAS report only covers large organisations, whilst medium and small organisations are not included. IDFs suffered by these e-tailers are mostly not reported at all.

E-tail business is one of the sectors most affected by online frauds. According to the public / private sector partnership Get Safe Online (getsafeonline, 2017), the UK businesses have lost over one billion pound for the period 03/2015 to 03/2016 to online frauds. It has also been confirmed that IDFs constitute more than half of the total online frauds. Mostly, when calculating the identity fraud losses, only direct losses are accounted for. The indirect losses such as: reduction in sales, a decrease in market share, share price drop, and other legal costs have significant adverse impact on business firms.

Online identity fraud trend is changing and the e-tail sector is getting more attention of fraudsters as the number of IDFs in the UK e-tail sector has grown by 49% from 2016 to 2017 (CIFAS, 2018b). Such trend shows that IDF in e-tailing is getting more significance as it has negative implications for them. These frauds result in a significant business losses thus lead to reduction of the market value and net profits. In the given scenario, management of IDFs is also getting more attention from the stakeholders of e-tailers.

Identity fraud is also attracting the focus of academics, as no significant work has been undertaken (Amasiatu and Shah, 2018). The literature on IDFM especially on e-tail sector is at the infancy, thus, leaving a significant gap in the literature on how to effectively manage these frauds in e-tail sector (Amasiatu and Shah, 2018). There have been some studies (Alrashed, 2016; Baz et al., 2017; Boss et al., 2015; Teh et al., 2016) on technological aspects of preventing and detecting identity frauds but the author could not find a significant literature on holistic management of identity frauds in e-tail sector, encompassing every aspect of fraud management. Thus, this study would help to bridge this gap by understanding IDFM, analysing managerial practices and suggest e-tailers improvements to enhance their understanding on IDFs, controlling fraud losses, maintaining better customer relationships and maintain the growth of online shopping.

The data shows that online organisations are suffering from significant financial and non-financial losses because of identity frauds. The identity frauds are also a serious obstacle to the development of online business markets, as lack of customers' trust in online purchasing hinders growth in online business activities. The extant literature has multiple studies on fraud management, but these are not focused on managerial practices in e-tail sector. Therefore, there is a need to focus on managerial practices to effectively manage the IDFs.

2.4 Significance of Management in Dealing with Identity Frauds

Identity fraud is one of the biggest challenges to e-tail organisations, so the sole responsibility of managing the fraud lies with the management of business organisations. Hannagan and Bennet (2008 p.05), define management as "*the process of achieving organisational goals and objectives effectively and efficiently through planning, organising, leading and controlling the human, material and financial resources available to it".* Management deals with the day-to-day and strategic business issues by utilising the organisational resources.

The role of management is critical to the success of any organisation, which is reflected in the market position of the organisation. An efficient management system is pivotal to the success of organisations. In the age of close competition, only organisations with excellent and sustainable management system can perform better. Therefore, each organisation should seek to develop a specialised management system for sustainability and excellence (Latham, 2012). A good management system entails better managerial practices, which have significance for superior firm performance (Bloom and Van Reenen, 2007). Despite the recognised importance of management systems, the author could not find any study analysing the managerial practices in IDF management in the UK e-tail sector, which is the aim of this study.

2.5 Managerial Practices in Fraud Management

Effective identity fraud management would be a competitive advantage because if an organisation is better at managing IDFs, the fraud tends to move to the competitors

(Becker *et al.*, 2010). Identity fraud management consists of peoples, processes and technology. Managerial practices have a significant impact on these three elements of fraud management. In an organisational context, peoples are a critical resource for online organisations. HRM practices such as recruitment and selection, training and performance review have a significant impact on the management of identity frauds in online organisations.

Organisational processes and internal control systems are developed by the management of organisations to ensure a required outcome of the employees' activities. Thus, the processes involved in the management of identity frauds are also designed by managers, but literature is mute on how managers establish such processes and internal control system to manage IDFs effectively. Managerial practices related to the management of identity fraud are critical for its effectiveness, which can determine the organisational standing on such a challenging issue, but no study is focused on analysing these practices to suggest improvements.

Online business is based on technology and the decisions related to the acquisition, deployment, functioning and evaluation of the technology are at the disposal of the management of organisations. These decisions are extremely important. Therefore, managerial practices on decisions regarding investments, technology acquisition, deployment, policies on their use and training to the end users, need to be analysed.

Before moving to the analysis of managerial practices in identity fraud management, it is necessary to know what constitutes fraud management, as without knowing its boundary it is not possible to set managerial practices in the current domain.

2.6 Understanding Fraud Management

As already mentioned, there has been no research on the management of identity frauds in online business organisations, especially in the management context. However, fraud is an old activity, so the literature is rich in fraud management activities, but the contexts are deviating from the current study. Therefore, to attain the aim of this study, it is necessary to study the existing practices for fraud management in related contexts.

Regarding the behavioural aspects of fraud management, it is a well-established argument that the potential fraudsters can be deterred from fraud by the fear of being caught and punished (Alanezi and Brooks, 2014), as the first stage of fraud management. The concept of changing the behaviour of potential fraudsters comes from the deterrence theory. It has been widely 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 (Tannenbaum *et al.*, 2015). So far, the significance of this deterrence has been confirmed in various contexts mainly in relation to accounting and audit (Dorminey *et al.*, 2012) and employee theft (Hollinger and Clark, 1983). In the identity theft domain Kumar *et al*. (2007) suggest that fear appeal do deter identity fraudsters, as it hinders the IDF to move from a threat to an attempt. So far, the literature shows that the significance of deterrence has been investigated and found to be an active element of fraud management. Although, deterrence has an impact on the fraudsters' behaviour, still frauds are attempted. The literature is missing on how e-tail organisations deter the identity frauds and what practices they have adopted in this sphere, how these practices work and what are their limitations. So far, research is needed to analyse managerial practices for IDF deterrence in e-tail organisations to suggest improvements

Although, deterrence has a significant impact on fraud attempts, in spite of this the frauds are still attempted. One of the major reasons, as suggested by Cressey (1950) in Fraud Triangle Theory, is the existing of an opportunity of committing a fraud, which refers to the system's weaknesses to prevent and detect frauds. Because of this, fraudsters can escape from being caught and punished. What follows is that in addition to deterrence, organisations should also have systems to prevent and detect attempted frauds.

To safeguard from fraud attempts an effective prevention is a significant tool, which is based on information security systems and the organisational arrangements (Devos and Pipan, 2009). For effective prevention, there should be IT-based solutions (Devos and Pipan, 2009), preventive technologies to fail any attempt of information theft and IDF (Boyer, 2007). A sound prevention system is an effective anti-fraud action (Prabowo, 2011). So far, it may be deducted that prevention is a critical element of fraud management.

For online transactions, customers use credentials to access their accounts, to prevent unauthorised access, e-tail organisation needs an effective authentication system to validate such information (Usman and Shah, 2013). Such credential information are stored on the business database. These databases are the hot target for fraudsters to steal the customers' information, so information security is critical to prevent identity information theft (Sanchez, 2012).

On the other hand, these systems are also the interacting point for the customers/ fraudster and the organisations, so there is a need to have an effective system to prevent unauthorised access to the customer account. Additionally, for the security of organisational databases and communication systems from any identity theft or data breach, an effective prevention system is inevitable (Alonso-Paulí and Pérez-Castrillo, 2012; Bishop, 2004; Koskosas, 2013). Thus, prevention is a critical stage in fraud management.

Although, measures are there to prevent identity fraud attacks, however, the literature findings reveal that fraudsters may use genuine customers' information. As a result, some fraudulent transactions still pass through the security net. These transactions are usually based on genuine but stolen information, so organisations need to implement systems to detect these suspicious transactions as the next stage after prevention, in fraud management (Chang and Chang, 2011). Detection is a critical stage to fight online fraud (Devos and Pipan, 2009) as without an effective detection system it is impossible to control the online frauds (Kundu *et al.*, 2009).

The literature suggests that a fraud attempt is merely a result of an assumption of the lack of detection, Therefore, organisations should have an effective detection system, which helps to create the fear of being caught and punished (Cressey, 1950). Dorminey *et al.* (2012) in a meta-analysis of white-collar frauds conclude that detection is an anti-fraud response to fraudsters. Thus, the extant literature suggests organisations to have an effective detection system to manage identity frauds if deterrence and prevention fail.

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 (Jamieson *et al.*, 2007; Kumar *et al.*, 2007). Sometimes, prevention and mitigation terms are used interchangeably, but in fraud management, mitigation is a distinct concept and applies to the practices in minimising the effects of fraud (Wilhelm, 2004). The purpose is to adopt the managerial practices, which can help to minimise the extent of fraud losses or to discontinue it. Mitigation is a significant stage of fraud management that allows to keep 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 (Jamieson *et al.*, 2007; Kumar *et al.*, 2007; Wilhelm, 2004).

Once fraud has been detected and mitigated, it is necessary to identify its type, methods and means, and the reasons why it passed through the prevention system. In fraud management, this set of practices is called fraud analysis. It helps the organisations to assess fraud risks and to estimate the effectiveness of prevention and detection systems to counter the frauds attempts (Brody *et al.*, 2007). Such analysis help enhancing efficiency at each stage of fraud management and develops guidelines for its effectiveness. These guidelines are forwarded as fraud management policies and technological evaluations. Thus, the analysis stage works, once a fraud has been attempted, whether successful or not and suggest measures to improve fraud management process.

At each stage of fraud management, anti-fraud policies create layers of protection for the organisation and its employees and to have no policy on fraud is a bad strategy (Verdon, 2006). Development of an anti-fraud policy would help to protect the personal information that may be used in identity frauds (Calvasina *et al.*, 2007) and such policies are meant to improve the effectiveness of identity theft management (Kumar et al., 2007). In addition to the development of anti-fraud policies, there should be an efficient communication of policies and guidelines on how to comply with (Prabowo, 2012). Therefore, it may be deduced that anti-fraud policies and their communication and compliance are a significant stage of fraud management.

The above-mentioned fraud management stages focus on actions before and during the fraud attempt, but successful frauds require further investigations and prosecution to recover the fraud losses and to get the fraudsters punished. Although, fraud investigations is a function of law enforcing agencies, businesses have a part to play. For example, they may help by collecting and preserving evidence in close partnership with the law enforcement agencies (Gogolin and Jones, 2010). Business organisations should investigate fraud occurrences and collect as much evidence as possible for a successful prosecution of the fraudsters.

Investigation and prosecution are critical in fraud management. Successful prosecutions help organisations to recover fraud losses. Secondly, an effective prosecution will disperse the warning message to potential fraudsters (deterrence) of being caught and punished. Thirdly, it helps organisations to uphold their image against fraudsters, and finally, a better customer relationship is maintained. The success of prosecutions depends on investigations, so organisations should be involved in investigations to develop and effective coordination with law enforcing agencies.

So far, the discussion has highlighted the stages of fraud management - deterrence, detection, prevention, mitigation, analysis, policy, prevention and prosecution of frauds. These stages have also been confirmed to be significant for managing fraud in banking, insurance, and credit card issuing companies (Wilhelm, 2004), in internal fraud and audit (Jamieson *et al.*, 2007), in collaborating for combating identity theft (Kumar et al., 2007) and in first-party fraud (Amasiatu, 2016). By contrast, Ijeoma and Aronu (2013) argue that a holistic fraud management, consisting of these stages is not effective in internal fraud management in small and medium conventional business organisations in Nigeria. Based on the literature, this study assumes that these eight stages are significant in IDFM in e-tail sector. Therefore, this study analyses managerial practices at each stage of IDFM and suggests improvements at each stage, which will confirm the significance of these stages in IDFM in e-tail sector.

These eight stages are not single actions but sets of various practices. A stage is “one of a series of positions or stations one above the other” or “a period or step in a process” (Merriam Webster, 2018). Both definitions are applicable in the context of this study, as the stages of fraud management follow one-an-other. Such as deterrence comes before any fraud attempt, and prevention works when a fraud is attempted. If prevention fails, the next stage is to detect the fraud, and next is mitigation to verify the customer identities and reduce the fraud impact. Analysis stage diagnoses frauds to know its methods and trends and to evaluate the other stages, which failed to stop the fraud and report to senior managers to develop and update fraud policies. Finally, investigations take place to collect evidence and fix responsibilities of frauds, which is followed by prosecution.

For superior anti-fraud performance, a coherent strategy should be adopted rather than focusing on one or more activities (Amasiatu, 2016). So far, the literature suggests adopting a more holistic approach to fraud management (Button, 2011; Wilhelm, 2004). Thus, it may be deduced from the above discussion that a comprehensive fraud management consists of eight stages. Therefore, the next step is to review the extant literature for any fraud management framework comprising these stages. This is necessary to understand the relation and role of each stage in fraud management and establish a balance of focus among these stages. An appropriate framework would also suggest the best composition of these stages, and a balance between these stages. The literature review on fraud management frameworks also helps the selection of an appropriate one to extend in this study.

A systematic review approach was adopted to explore frameworks of fraud management consisting of these stages. At the exploration stage, the database Business Sources Complete and the search engine Google Scholar were used to identify such frameworks. Furthermore, to make the search more specific, name of each stage was also used in parallel to the key words framework, fraud and management. The search engine returned 153 items and the database 1862 items. Next each item was carefully checked for the presence of any of these stages, and any study with these stages was selected for further investigation.

Most studies were focused on one, two or three stages. Even some frameworks included three or four stages, but these were not appropriate enough to meet the objectives of a comprehensive fraud management. In the end, the sorting process produced only four studies suggesting the frameworks based on already mentioned fraud management stages. It is also an objective of this study to extend a framework, so selection criteria are mentioned, and the appropriateness of the selected framework is also explained. These frameworks are detailed in next section.

2.7 Fraud Management Frameworks and the Selection Process

A framework is an arrangement of parts that gives something its basic form (Merriam Webster, 2018). Because fraud management is a proces, its parts are madeup of stages, which are deterrence, prevention, detection, mitigation, analysis, policy, investigation and prosecution. The term framework has been used to describe any combination of these eight stages. The literature search has identified four such frameworks which differ in how stages are organised and managed.

These are Role Based Framework (Shah and Okeke, 2011), Action-Event Identity Theft Management Framework (Kumar et al., 2007), Identity Fraud Enterprise Management Framework (Jamieson *et al.*, 2007), and Fraud Management Lifecycle Framework

(Wilhelm, 2004). Although, all these frameworks have been developed for fraud management, none was designed specifically for e-tail activities. The next task, therefore, is to establish which one would best fulfil the objective of this study to extend it to IDFM in the e-tail sector. The selection criteria are discussed in the next section.

2.7.1 Framework Selection Criteria

Selection of an appropriate IDFM framework is critical. Surprisingly, the literature has nothing to offer in this regard except for a study on first party frauds by Amasiatu (2016). The selection criteria proposed by Amasiatu (2016) are adopted in this study. The selected framework should be functional, adoptable and comprehensive to cover all the necessary stages of fraud management, provide support for ongoing improvement, be empirically derived, each stage/step should have a clear focus and the stages should be interconnected. Finally, the selected framework should be based on fraud management or related context. The purpose of such exercise is to select an appropriate framework for extension in IDFM. The extended framework will provide the e-tail organisations, a coherent strategy with a comprehensive approach for IDFM.

a) ***Functionality:*** It is the capability of or suitability for being functional (Merriam Webster, 2018). Being functional is to be capable of fulfilling its objectives.

b) ***Adoptability:*** It refers to taking up and using something (Merriam Webster, 2018). It relates to the flexibility of a framework, which allows it to modify for the given purpose without losing its effectiveness.

c) ***Comprehensiveness:*** This relates to covering something entirely or broadly (Merriam Webster, 2018). The holistic nature of the framework is necessary to address each aspect of fraud management. Therefore, the comprehensive framework should contain all the stages of fraud management as mentioned above, as a holistic framework should involve all necessary activities to address the problem (Furlan and Bajec, 2008)

d) ***Support for Ongoing Improvements***: Performance monitoring and evaluation are critical to the success of any framework that helps to improve its performance (Pergola and Sprung, 2005). Such continuous monitoring ensures that the aim of fraud management is achieved (Furlan and Bajec, 2008).

e) ***Empirically Derived:*** Such frameworks are based on primary data, so their validity is less doubtful (Amasiatu, 2016).

f) ***Focused Stages:*** It relates to the quality of actions and practices at each stage of the framework. They should be distinguishable, as the ambiguity in actions would lead to the confusion between various actors in fraud management (Wilhelm, 2004).

g) ***Interconnectedness*****:** The stages of the selected framework should be interconnected, as some practices need close connection and frequent communication for the effective performance of the framework.

h) ***Context Relatedness:*** The context of the framework is important, as a framework in the related context would better fulfil the aim of its extension.

Potential frameworks for this study are discussed below in relation to the selection criteria.

2.7.2 Role Based Framework (RBF) (Shah and Okeke, 2011)

The Role Based Framework (Shah and Okeke, 2011) focuses on the prevention of the internal identity theft. The framework synthesises the existing preventive measures against identity theft within organisations. It is suggests the responsibility of management at each level of authority and that of the law enforcing agencies. The fraud management practices are divided into three categories according to the management levels, and each is suggested a set of practices to perform.

The strategic practices such as; identity theft risk management and policy related issues are linked to the top management of organisations. The framework suggests that the top management should develop the prevention and deterrence policies that would drive the behaviour of the employees towards the achievement of organisational goals and take disciplinary actions to correct the deviant behaviour.

The middle management is engaged in developing training programmes to minimise the chances of human errors and help them to comply with the policies. Managers at this level should directly involve in the identity theft incident management and analyse the loopholes in the systems, causes of incidents and fix the responsibilities. Such practices would help to enhance the performance of technological systems and redress the shortcomings of the control systems.

The contribution of operation managers is critical for effective identity theft prevention. They are directly involved in day-to-day business activities. The framework suggests that the front-line managers have a direct influence on and frequent interaction with the employees so that they can play a vital role in identity theft detection and investigation. The operation level management also has a significant role in the free flow of communication between the management and the employees, which helps to flow the objectives, directions and policies right at the target.

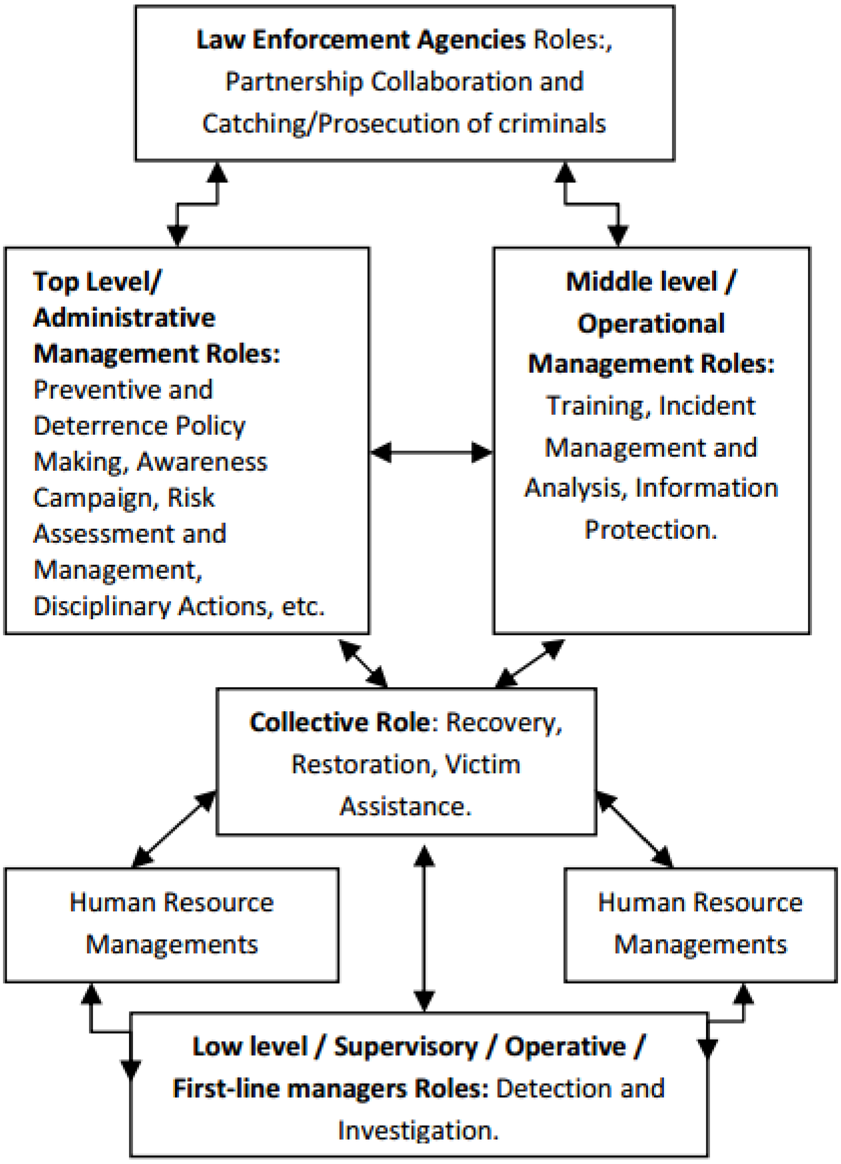
Law Enforcement Agencies Roles:, Partnership Collaboration and Catching/Prosecution of criminals
Top Level/ Administrative Management Roles: Preventive and Deterrence Policy Making, Awareness Campaign, Risk Assessment and Management, Disciplinary Actions, etc.
Middle level / Operational Management Roles: Training, Incident Management and Analysis, Information Protection.
Collective Role: Recovery, Restoration, Victim Assistance.
Human Resource Managements
Human Resource Managements
Low level / Supervisory / Operative / First-line managers Roles: Detection and Investigation.

Figure 2. 1 Role-Based Framework (Shah and Okeke, 2011)

The Role-Based Framework is meant to prevent the internal identity theft in online organisations. The role-based framework has not been tested in any empirical study. So its functionality is not proven. Its adoptability is also not validated by any study, as it has not be used in any empirical research. Managerial practices at each stage of fraud management are fixed with any level of the management, such as policy is set top-level management practice, while literature suggests the involvement of the operational staff. Thus, the Role Based Framework is rigid with managerial practices fixed at each level. Furthermore, it is not a comprehensive one as two important stages, i.e. mitigation and prosecution are missing, and without these stages, effective fraud management may not be ensured.

The framework suggests for ongoing improvements, which make it matching with one of the criteria. The framework does not focus on the fraud management stages, but the role of each management level is highlighted, which makes the stages secondary. The stages of the fraud management also lack the interconnection that would negatively affect the performance of fraud management. Finally, the framework is focused on internal identity theft prevention only, which limits its context, while identity fraud management needs broader context for its effectiveness. Therefore, the Role Based Framework is not considered to be used as underpinning framework for an extension.

2.7.3 Action-Event Identity Theft Management Framework (Kumar et al., 2007).

Although, Kumar *et al.*, (2007) use the term identity theft, they actually analyse the activities and stages of identity fraud management. Their research is focused on the collaboration of organisations to combat the identity theft and touches the activities in identity fraud management. The framework is designed to respond to four events (challenges) of identity frauds, which are threat, attempt, occurrence and loss.

The threat represents the possibilities of fraud attempts from various internal and external sources. For that, deterrent activities are suggested to control the behaviour of potential fraudsters through fear appeal. The attempt refers to an attack on information systems or personal devices to get personal information and account credentials with a motive to use that for identity frauds. The prevention activities are recommended, and some preventive measures are suggested to fail any information theft attempt.

Identity theft occurs when an attack breaks the security measures, and the fraudulent transaction is successful. The detection and mitigation activities are suggested to coup with a successful identity theft attempt. In the case of failure in protecting the identity information, anything that happens because of the use of stolen information, either financial or non-financial is termed as a loss. To cope with these challenges, the framework proposes the analysis, policy and prosecution stages.

The action-event identity theft management framework offers practices to manage the identity theft irrespective of any specific context. Although, the framework offers some actions at each stage of the identity theft management yet, it lacks a detail of practices at each step of the framework. The identity theft management stages are also borrowed from the Wilhelm (2004).

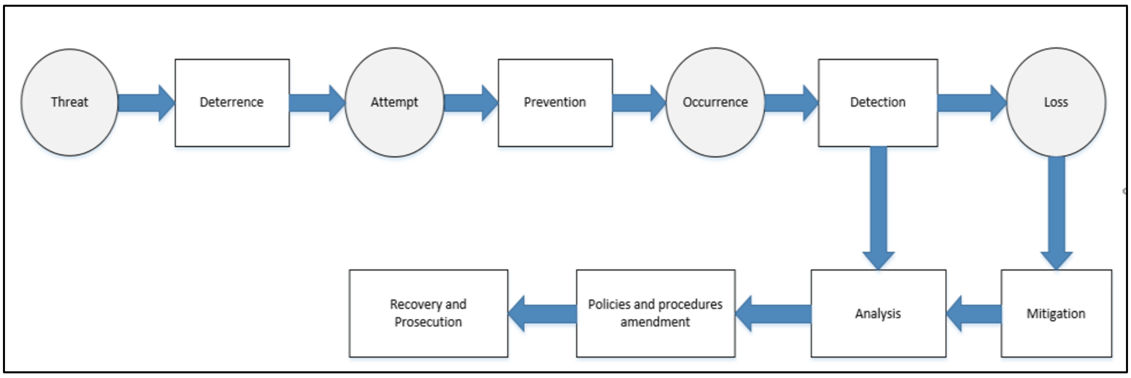

Figure 2. 2 Action-Event Identity Theft Management Framework (Kumar et al., 2007).

Nevertheless, it may be a workable framework, but it has some limitations to be the appropriate one based on the selection criteria. The framework may be functional and adoptable, as it is already developed for identity fraud management. On the comprehensiveness, it lacks the investigation stage. The absence of an investigation stage would negatively affect the other stages such as prosecution and deterrence. First, without investigations, there will be no evidence to prove the fraudsters guilty of identity frauds, the arrest of fraudsters would not be possible, which is necessary for prosecution and creating the fear of being caught and punished. Finally, the framework does not support the communication of analysis results, which results in lack of ongoing improvements in identity fraud management.

The framework is developed for collaboration among the stakeholders of identity information security. It is a set of suggestions not based on any empirical data or empirically tested. Although, the stages of the framework are focused, for developing colloboration among the organisaitons however, these stages are also working in a sequence without any interaction, which hinders the way for back and forth information flow to improve the efficiency of these stages, so it fails on the interconnectedness. Finally, although it is context related, however, missing of a significant stage, lack of empirical validity and absence of the support for ongoing improvements, make it inappropriate to extend it in the current context.

2.7.4 Identity Fraud Enterprise Management Framework (Jamieson *et al.,* 2007)

The framework incorporates three phases: anticipatory, reactionary and remediation. The anticipatory phase is a precaution to identity frauds, which includes stages of the policy, risk assessment, deterrence and prevention. The second phase comes into action once the fraud occurs. This phase consists of fraud detection, mitigation, analysis, incident management and review of the incident. The detection activities help the organisation to uncover any fraud attempt and take actions to minimise the effects of the frauds under mitigation stage. The fraud incidents are then analysed to know the fraud methods and techniques used to learn about how to prevent these in future. The next steps are incident management and the review of the incident that led the organisation to manage the effects of the incidents and to prepare to prevent such frauds in future.

The remedial phase includes the investigation, prosecution, recovery and restoration stages. In this phase, the organisations have to investigate the nature of fraud, its methods and patterns, and collect the evidence and devices necessary to make the fraud prosecutable. Once the organisation collects enough evidence and is in a position to fix the responsibility the litigation process is initiated to prosecute the fraudsters. The recovery becomes possible after successful prosecution and restoration are achieved once the matter is fully resolved.

The framework also suggests learning steps at three levels of the framework. The purpose of these steps is to gain an insight into the performance of the three phases. The first learning step includes the test and train as sub-activities. At this step, the authors suggest the testing of employees’ abilities to manage the frauds and necessary training to equip them with capabilities to deal with the frauds. A continued learning through a supervised and unsupervised training on the fraud system operations and effectiveness is suggested in the framework. Based on the learning steps, the framework suggests procedure adjustment steps for all three phases to improve the performance of these steps.

The framework is functional as it has a potential to be used in this study. It is also adoptable as it is developed for the identity fraud management. Although, it is comprehensive and covers all the stages necessary for fraud management, some of the stages are fragmented, or actions of one stage are divided into more stages, which makes it more complex. For example, the stages mentioned as incident management and review are the part of fraud mitigation and analysis.

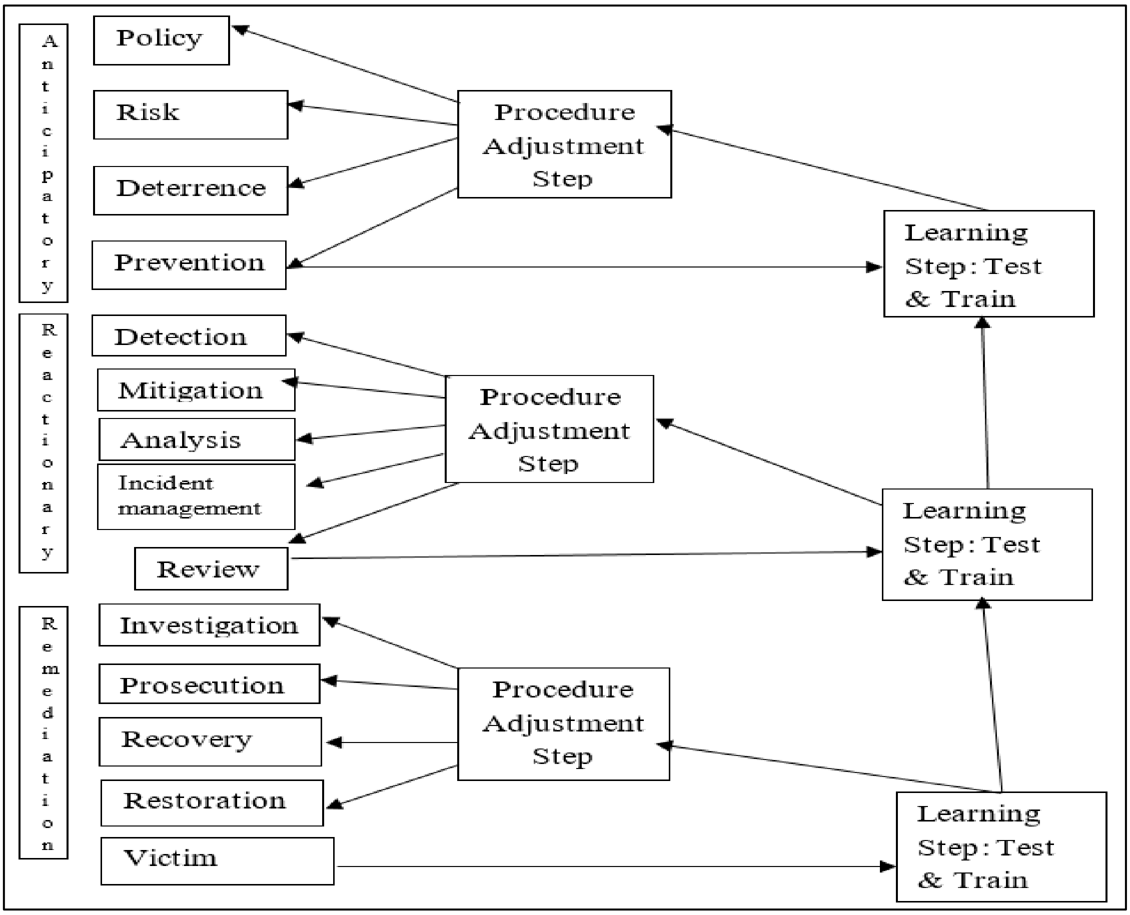

Figure 2. 3 Identity Fraud Enterprise Management Framework (Jamieson et al., 2007).

Under incident management, they refer to is the implementation of activities related to fraud occurrence, i.e. identity verification, and data matching, which are already discussed as part of mitigation. The review they refer to is a feedback to other stages, which already exists at the analysis stage. Thus, recovery and restoration are also set as a part of prosecution stage in other frameworks.

Additionally, internal audit is also suggested to review the process at each stage of fraud management which is already a part of analysis stage. So, such unnecessary fragmentation increases the number of stages and duplication of practices at various stages makes it complex. The analysis stage and internal audit support for the continuous improvement in fraud management. The framework is based on data from banking and public-sector organisations, which shows it is empirically derived. Nevertheless, the stages of fraud management are focused but lack direct interconnections of these stages, which may negatively affect the performance of fraud management.

Although, the context of the framework is related to this study, the separation of learning practices and adjustment process adds to its complexity. Furthermore, all the stages of the framework rigidly flow in a series, which hinders the free flow of communication between each stage. The separation of these stages also limits the implementation of the framework in micro level organisations (Jamieson *et al.*, 2007). Based on the limitations mentioned above this framework may not be suitable to be extended to achieve one of the objectives of this study.

2.7.5 Fraud Management Lifecycle Framework (Wilhelm, 2004)

The framework is based on an empirical study of a variety of industries, i.e., retail financial institution, mortgage providers, telecommunication and insurance. A broader concept of fraud is adopted to include online and offline identity frauds. The framework proposes eight stages of fraud management life-cycle: deterrence, prevention, detection, mitigation, analysis, policy, investigation and prosecution. The framework is virtual because; its stages are not rigidly sequential, where without completing activities of one stage one cannot move to another stage. On the other hand, the stages in the framework are networked to work either sequentially (see figure 2.6) or simultaneously if needed.

The first stage, deterrence, is characterised as actions and activities to deter fraud attempts through fear appeal. The second stage, prevention, involves actions to prevent the occurrence of attempted frauds through technological measures. At this stage, sophisticated technology and effective information security measures are advised. Activities at the third stage, detection, are aimed at identifying and locating fraud before, during and after the completion of the fraudulent activity.

For detection of any suspicious transaction in the system, automated detection systems based on data mining and fraud rules are suggested. Activities to minimise fraud losses, stopping frauds continuity and blocking the sources of frauds are part of the fourth stage, called mitigation. Stage five consists of activities to analyse frauds that deterrence, prevention, detection and mitigations stages failed to control. It is a critical stage that analyses fraud methods, its channels and patterns, and reasons for the failure to stop it. Such analysis is useful to update the systems and developing policies and strategies to manage fraud. The stage of analysis also includes risk assessment and evaluation of the technologies, processes and organisation of fraud management.

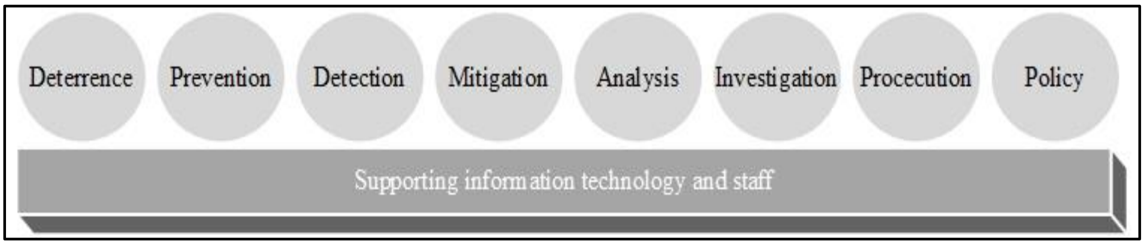

Figure 2.4 The linear representation of the Fraud Management Lifecycle Framework (Wilhelm, 2004).

The development and compliance of policy to reduce incidences of fraud are the activities performed at the sixth stage, named as policy. This stage is helpful to control human activities and resource constraints to reduce chances of fraudulent occurrences. The next stage investigation; consists of undertakings to obtain enough evidence and information on fraud occurrence and to support the prosecution process, which is the final stage of the framework. At prosecution, stage organisations work with law enforcing agencies to recover losses, get compensation and conviction of the fraudsters.

The framework is functional, it has been used in various contexts. For example, Amasitu (2016) applied it to first-party fraud and Ijeoma and Aronu (2013) to internal frauds. For this study, as the stages are clear and managerial practices at each stage can easily be analysed for improvements. Its stages are not rigidly sequential, so it is flexible that can adjust changes without scarifying its purpose, which confirms its adoptability. As already mentioned that it consists of the eight stages, which are necessary for fraud management. Therefore, it is a comprehensive one. Furthermore, the framework itself suggests some managerial practices, which is an added benefit. Its analysis stage is focused on the facts about the fraud incidents and performance measurement of the other stage. Thus, it supports ongoing improvements in the fraud management.

As already mentioned, it is based on the primary data from the retail financial institution, mortgage, telecommunication and insurance industries, which confirm it as being an empirically derived. Each stage is given a boundary, so practices at each stage are distinguishable and every stage is given focus and are set equally important, which shows that the stages of the framework are individually focused. One of the best characteristics that no other framework offers is the interconnectedness of the stages. The networked representation of the framework (see figure 2.5) expresses fifty-six connections of the framework, which proves the interconnectedness of the stages. Finally, the framework has already been used for fraud management in various industries, which confirms the context relation of the framework with this study.

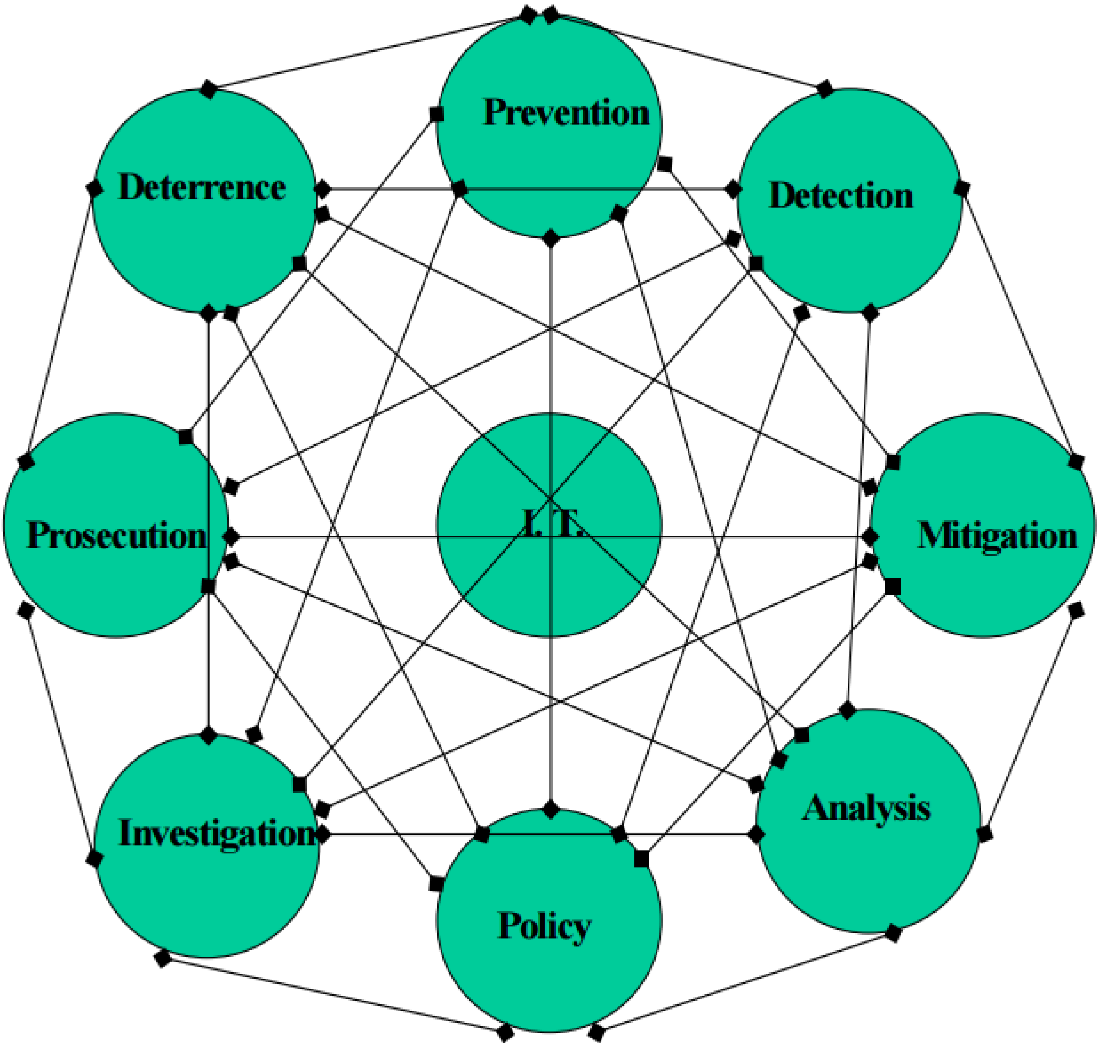

Figure 2. 5 The network representation of the Fraud Management Lifecycle Framework (Wilhelm, 2004).++++++nn

The framework has been developed to investigate the fraud management and activities are divided distributed in its stages, which makes it a holistic framework. The framework has merits but does not explore in detail managerial practices at each stage of fraud management. Therefore, the literature on these eight stages have been reviewed individually. These practices were linked to the related stages of the framework. Finally, these practices are analysed in IDFM in e-tail sector. Based on empirical data and literature, the framework is extended for its effective use in IDFM in e-tail sector. Managerial practices reported at each stage of the framework are discussed in the following section.

2.7.6 Summary of the Evaluation of the Frameworks

In previous sections the potential frameworks have been explained and evaluated. The summary of the evaluation in given in the following table.

Table 2. 4 Showing the summary of evaluation of the frameworks based on the selection criteria

Criteria / framework	**Functional**	**Adoptable**	**Comprehensive**	**Support ongoing improvements**	**Empirically derived**	**Focused steps/stages**	**Interconnectedness**	**Context relatedness**
(Shah and Okeke, 2011)	Y	Y	N	N	N	Y	Y	N
(Kumar *et al.*, 2007)	Y	Y	Y	Y	N	Y	N	N
(Jamieson *et al.*, 2007)	Y	N	Y	Y	Y	Y	N	N
(Wilhelm, 2004)	Y	Y	Y	Y	Y	Y	Y	N

Table 2.4 shows the appropriateness of the discussed frameworks and presents the potential of each framework. The evaluation criteria as already mentioned was adopted from Amasiatu (2016). It offers eight steps for the evaluation of frameworks, which are already mentioned. This research applied these criteria on the potential frameworks and

analysed their merits to meet each of the eight criteria. The summary of the evaluation of each framework is also given below.

The Role Based Framework proposed by Shah and Okeke, (2011) presents a good insight to prevent the identity theft, but has some limitations. At first, it is not adoptable, as it focuses on the managerial roles, not on the identity fraud management stages. Secondly, it is limited to few stages of the fraud management and has no provision for ongoing improvements. Further, it is based on the literature, so lacks the empirical touch; hence its validity is not proven. Finally, it does not suggest for the interconnections of the fraud management activities, which is significant for its effectiveness. Therefore, this framework may not be suitable for this study.

The Action-Event Identity Theft Management Framework suggested by Kumar, et al., (2007) although has some potential but it lacks the important stage of the investigation. Without investigation, it is not possible to collect the evidence and fix the responsibility, which also diminishes the role of prosecution. The framework also lacks the empirical grounds for its validity. The stages of the framework are also linear and sequentially interconnected, which make it unsuitable to be used in this study.

The Identity Fraud Enterprise Eanagement Framework, proposed by Jamieson, et al., (2007) has much potential to be used here, but there are two significant limitations. At first, the stages of the framework are linear, sequential and rigid, which makes it non-adoptable. Secondly, the stages of fraud management lack the interconnectivity that may lead to a lack of coordination and communication. Such lacking may negatively affect the performance of the framework in given context. Additionally, the framework has a complex structure with duplication of some steps. For example, the activities of review and risk assessment steps are already mentioned in the analysis stage, and restoration and recovery are the part of the prosecution stage. Furthermore, the rigidity of the stages makes it complex, as policy cannot be developed before risk assessment and the fraud analysis. Therefore, this framework may not be an appropriate for this study.

Unlike all other frameworks, fraud management lifecycle theory, developed by Wilhelm (2004) meets the required criteria. It is functional and adoptable on account of its flexibility. It contains all the stages, necessary for effective fraud management. The analysis stage helps to evaluate its performance. Thus, operational improvement is possible in this framework. Further, the framework is empirically tested in industries like banking, credit/debit card issuers, insurance, telecommunications and mortgage providers. Moreover, the stages of the framework are not rigidly linear like other frameworks, but also networked, which allows coordination and closer communication between each stage of the framework. The networked nature of the framework will allow grouping of various stages, thus, small and medium size organisations can have the advantage of the framework. Additionally, the practices at each stage are focused and specific to related stage, so a better fraud management organisation is possible. Finally, the framework is specially designed for fraud management in online and offline organisations. Therefore, it may be helpful to attain the objectives of this study.

The eight stages - deterrence, prevention, detection, mitigation, analysis, policy, investigation and prosecution - of IDFM and the managerial activities at each stage given in extant literature are presented in the next section. According to Wilhelm, (2004) each stage is the set of activities or practices performed to attain the objective of the stage. Therefore the managerial practices at each stage of fraud management are given below.

2.8 Existing Managerial Practices at Each Stage of Fraud Management

The extant literature has various studies investigating managerial practices in fraud management. Most of the studies focus on one or two stages of fraud management. Only a few studies researched fraud management comprehensively, yet no significant work has been identified during this research that investigates the managerial practices in the e-tail context. This section examines the state of the art in the fraud management literature covering various operations contexts such as internal fraud management, insurance frauds, information security, banking, service sector, financial sector and telecommunications and how it discusses managerial practices at each stage of fraud management are discussed in the following sections.

2.8.1 Deterrence

Deterrence should discourage fraudsters from committing a fraud. In fraud domain, the fear of being caught and punished and customer education and awareness are considered as fundamental deterrence practices (Jamieson *et al.*, 2007; Wilhelm, 2004). Deterrence is a set of precautionary measures to implement before any fraud attempt takes place (Jamieson *et al.*, 2007). Precautionary measures include customer education and sending a clear message to potential fraudsters to create fear of being caught and punished by the law (Jamieson *et al.*, 2007; Wilhelm, 2004). Thus, the deterrence of identity fraud is based on the customer education and fear of being caught and punished.

Customer education, awareness and knowledge also have a significant impact on fraud deterrence (Sperdea *et al.*, 2011). Customer education enhances the knowledge and awareness of customers that help them to avoid the risk of identity theft (Arachchilage and Love, 2014; Seda, 2014). Thus, customers may be educated to regularly monitor their bank account transactions, online business accounts and their credit files, and not to share any personal information on social media (Alrashed, 2016; Amori, 2008; He *et al.*, 2014; McGee and Byington, 2015). Customer education also increases their efficacy when using technological systems, which has a positive impact on identity fraud deterrence (Arachchilage and Love, 2014; Holt and Turner, 2012).

Additionally, organisations should also educate their customers concerning the growing risk of identity theft methods and practices to minimise that risk (Bourgeon *et al.*, 2008; Wang *et al.*, 2006). Frequent communication and interaction between customer and business regarding the education are required to enhance customer knowledge, awareness and efficacy, which directly affect their behaviour and encourage them to deter the online fraud (Wang *et al.*, 2006).

In addition to general awareness and education, online organisations could send specifically designed messages to a particular group of customers and victims to educate them on specific issues (Copes *et al.*, 2010). Furthermore, the organisations should check the contents and context of messages that they communicate to the customer for their education and awareness on identity theft (Hille *et al.*, 2015). Although, the discussion shows that customer education and awareness has a significant impact as an identity fraud deterrence, excessive warnings can undermine customers' confidence. Therefore, e-tail organisations should adopt those managerial practice to educate customers that have the least impact on their reputation.

As already mentioned, the fear of being caught and punished has a significant impact on fraudster's behaviour, towards not attempting a fraud (Workman and Gathegi, 2007). Importantly, the certainty of punishment is more effective to discourage the fraudsters to commit fraud than its severity (Leasure and Zhang, 2017). The fraudulent behaviour can be averted by creating the fear of being caught and punished according to law (Dorminey *et al.,* 2012; Sperdea *et al.,* 2011). Furthermore, the literature shows that the law enforcing agencies are less interested in catching fraudsters involved in small business frauds (Lewis *et al.*, 2014). However, managerial practices for creating fear of being caught and punished in e-tail organisations have not been analysed.

Sending a clear message to potential fraudsters about the certainty of being caught and punished has a positive impact on fraud deterrence (Akers, 2013; Leasure and Zhang, 2017). Regarding sending such messages, mass media plays an effective role and increases the effectiveness of deterrence by creating the fear of being punished (Zadig and Tejay, 2010). However, managerial practices have not been analysed for disseminating the information that creates fear among the potential fraudsters. Therefore, this study analyses managerial practices to investigate how the e-tail organisations are creating fear of being caught and punished to change the behaviour of identity fraudsters. Managerial practices discussed above are presented in the following table.

Table 2. 5 List of the practices suggested for fraud deterrence

Source	**Practices**	**Interpretations**
(Akers, 2013)	- Identity fraud deterrence should be increased by creating the fear of being caught and punished in according to law. - The certainty of punishment has a real impact on deterrence of frauds, so it should be promoted.	- The fear of being caught and punished averts the behaviour of fraudsters. - Certainity of punishment changes the intention of fraudsters towards not attempting any fraud.
(DeAngelo and Charness, 2012)		
(Leasure and Zhang, 2017)		
(Shamsi *et al.*, 2016)	- Publicise the attribution of attack by mentioning the cyber weapon, the origin of the attack and the identification of the attacker.	- Such practice creates the fear of being caught and punished, thus help in deterrence.
(Alrashed, 2016)	- Customers should be advised to check their bank transactions, online accounts and credit files frequently. - They should also be suggested for not sharing personal information on social media.	- It creates vigilance and help earlier detection of IDFs. - Such practice minimise the chances of IDT.
(Amori, 2008)		
(McGee and Byington, 2015)		
(He *et al.*, 2014)		
(Hille *et al.*, 2015)	- The organisations should check the contents and context of messages that they communicate to the customer for their education and awareness on identity theft.	- Messages should not have any negative impact on customers, but help them minimising the possibilities of IDT.
(Arachchilage and Love, 2014)	- Customers should be educated about identity theft risk, its methods	

(Seda, 2014)	and guidance to avoid any identity theft occurrence.	- Such education motivates customers in securing their credentials.
(Bai and Chen, 2013)	- Try the full employment of mass media for deterrence communication.	- Mass media has wider access to the community, so it may help warning potential fraudsters.
(Guitton, (2012)	- Publicise the information on detection, arrest or punishment of cyber security attackers.	- Such information creates fear, which leads to fraud deterrence.
(Dorminey *et al.*, 2012)	- Organisations need to take two significant actions for effective fraud deterrence: - Educate their customers - Send fear messages to the society for fraudsters being caught and punished.	- Customer education helps in minimising the number of IDT occurrences. - Fear appeals lead to avert negative behaviour of fraudsters.
(Sperdea *et al.*, 2011)		
(Copes *et al.*, 2010)	- Specific messages should be directed to the targeted customers and victims of identity theft.	- Customised messages help in different situations to deal accordingly.
(Zadig and Tejay , (2010)	- Establish a sense of security. - Establish the visibility of active policing. - Prosecute the fraudsters. - Make aware the potential fraudsters of the organisational efforts and actions on information system attacks.	- Sense of security develops customer trust. - Policing helps in reducing the number of IDF attempts - It enhances the IDF deterrence. - Such arrangements increase fraud deterrence.
(D'Arcy *et al.*, 2009)	- Develop the user awareness of security policies. - Develop security education and training programs. - Monitor computers for any violation. - Establish the threat of punishment for potential fraudsters.	- It is to ensure effective compliance. - It motivates staff for the secure use of IT. - Earlier detection may reduce the impact of attack. - The threat of punishment results in fraud deterrence.
(Workman and Gathegi, 2007)		
(Baer, 2008)	- Deterrence depends on the fraudsters' evaluation of risk, so societies should increase the expected penalties for effective deterrence	- Severity of punished has direct impact on behaviour of fraudsters.

Table 2.5 shows various managerial practices for effective deterrence of frauds. These practices are suggested for other contexts, such as; online banking, health services and m-commerce, for information security, bio-matric authentication system, internet frauds and identity theft. However, these practices have not been analysed in identity fraud

deterrence in e-tail organisations. Thus, the extant literature has no significant studies on managerial practices about how e-tail organisations are deterring identity fraudsters? Therefore, this study analyses the managerial practices for identity fraud management in e-tail organisations to answer the question and will help the e-tail organisations to improve these practices for effective identity fraud deterrence.

2.8.2 Prevention

In fraud management domain, prevention practices are designed to prevent the frauds or to secure the information through technical systems and creating hindrances to commit identity theft. Prevention is important in failing any fraud attempt, while deterrence is limited to discouraging the fraudsters through fear using conventional methods, which are already discussed in the previous section. Prevention is a process of developing arrangements against predicted risks which is based on IT solutions and managerial practices (Devos and Pipan, 2009). In literature and academia, prevention, deterrence and detection of frauds are sometimes interchangeably used (Wilhelm, 2004). However, the use of a framework helps to clarify the differences among these concepts with a set of practices at each stage.

In online business, prevention refers to the deployment of protective systems, procedures, processes and practices, which help to protect online identity information and data breaches from fraudsters. Such stolen identity information is then used for identity frauds (Lee and Yu, 2012; Whitman and Mattord, 2011). Prevention also helps to validate the credentials of customers to access their account for online shopping.

Online business organisations are responsible for protecting customers' information and to prevent any identity theft attack (Cordell, 2013). For this purpose, mostly technological arrangements are made along with some organisational arrangements (Devos and Pipan, 2009). These include a strong encryption technology, anti-virus, anti-malware, anti-phishing technologies, firewalls, intrusion detection and digital signatures and certificate systems (Devos and Pipan, 2009; Geeta, 2011; Goyal *et al.*, 2012).

Online organisations are also suggested to implement strong encryption on the personal information on organisational and personal devices; as in case of any theft, emergency or error, it will prevent the identity theft, even after the devices are accessed (Alrashed, 2016). Although, these measures have been suggested for the security of information systems, but no research has been carried out on e-tail organisations that what practices these organisations have adopted to secure their customer information.

An authentication system is critical to validate and verify the identity of the customers before allowing them access to their accounts (Usman and Shah, 2013). Weaknesses or limitations of an authentication system can lead to identity frauds, so online organisations should have a strong system to validate and verify the identity of customers before allowing them access to their accounts (Prakash *et al.*, 2015; Sharma *et al.*, 2015). For effective authentication, apart from traditional ID and password, online organisations are recommended to use bio-matric authentication, such as; finger printing, retina and face recognition and voice recognition (Mansfield-Devine, 2013; Usman and Shah, 2013; Teh *et al.*, 2016).

Although, bio-matric authentication systems have significant merits to verify the identities of customers, a significant limitation is suggested by Wang, *et al*., (2006): once bio-matric information is compromised, it is not possible to change it. To address the challenges of authentication, one-time password is suggested by Bang *et al*. (2012). These one-time passwords can be sent as text messages on the customers' registered mobile numbers (Ates *et al.*, 2013; Creswell and Poth, 2017), additionally customers can also be informed about account login, through such messages to timely prevent any identity fraud (Wang *et al.*, 2015). The literature suggests various authentication systems and their effectiveness, but managerial practices on how e-tail organisations select and evaluate the effectiveness of their authentication system to prevent unauthorised access to customers' accounts are not analysed.

The practice of ensuring the validity of customer identities before accessing any account will prevent identity frauds. Furthermore, organisations may adopt the practice of sending a one-time password for account access to prevent any unauthorised access (Bang *et al.*, 2012). Such password will be sent to the registered contact of the customer, which will ensure the identity of the customer. Also, the practice of sending account login alerts also helps to detect any unauthorised access to a customer account, which can prevent any activity on the account (Kumar and Goyal, 2016; Wang *et al.*, 2015). However, the practices for sending login alerts are effective in preventing unauthorised access in real time, but these have not been analysed in e-tail context. Furthermore, practices on how e-tail organisations detect unauthorised access and what channels they use to inform the customers for identity fraud prevention are not analysed.

For effective prevention of information theft, organisations are encouraged to make arrangements to secure customer data at each step. Prosch (2009) emphasises that organisations should have a secure encryption system, protect data from internal and external theft through controlled access and dual authentication system and data processing should be carefully monitored for any human or system error.

Furthermore, replicated data should be made secure through strong access policies, comprehensive training and periodical scanning of personal computing devices and strictly follow the privacy laws (Prosch, 2009). Although, Prosch (2009) has made good suggestions to prevent identity theft, however, managerial practices on how e-tail organisations are monitoring information security measures to ensure that customers' information are secured and protected are not analysed.

E-tail organisations outsource some of their services, e.g., data storage. Sometimes goods sold through these organisations are despatched by their suppliers. In these cases, e-tail organisations have to share their customers' data with these organisations. These data at third party organisations may be at risk of theft and breach. To ensure the security of their customers' identity information, online organisations are recommended to ensure same protocols of security, (for identity theft prevention) by third parties if any personal information is shared with them (Vahdati and Yasini, 2015; Phan and Vogel, 2010).

The practice of ensuring the effective arrangements for identity theft prevention would help the e-tail organisations to maintain the security of customers' information at every end. Furthermore, online organisations should also ensure strong encryption at suppliers, vendors, and contractors to prevent any identity theft attack (Ahamad *et al.*, 2014; Taitsman *et al.*, 2013). These suggestions are significant to prevent identity information from theft and breach, but research is missing on how e-tail organisations ensure the prevention of their customer information at third party organisations. The functionality of prevention systems depends on the investment in preventive technologies, as a higher investment is linked to the efficiency and effectiveness of the technology (Boyer, 2007). Therefore, it may be deduced that managerial practices related to the investments in sophisticated technologies have a significant impact on the identity theft prevention.

Furthermore, the regular monitoring of prevention systems for their performance, and frequently updating these systems in response to emerging threats are critical to ensuring effective prevention of identity theft (Amori, 2008; Delanty, 2005). These studies emphasise the importance of investing in sophisticated technologies and their performance monitoring and updating. Although, sufficient investments in prevention system would normally ensure its efficiency and effectiveness, however, the nature of e-tail organisations is different. These organisations face intense competition and operate with limited resources, which make their investment decisions challenging.

However, literature is missing on what factors are considered by managers in e-tail organisations before making any investment in preventive technology. Furthermore, the literature is also missing on how managers analyse the effectiveness of existing systems, which subsequently leads towards the decisions on update the existing systems or to require more sophisticated technologies to prevent identity frauds.

At the internal side of the information theft prevention, the extant literature suggests to manage access to information. This helps to limit the data access to the staff members and to monitor who accessed what information (Alrashed, 2016). Keeping the least privilege access policy limits staff access to customers' personal information and authorisation of access to customer data are significant to prevent identity theft from internal staff members (Wang *et al.*, 2006).

Furthermore, for effective internal identity theft prevention, organisations should keep a record of who accessed what type of personal information and the reasons, as such records will help the organisation to fix the responsibility of any mishap, and prevent the staff for any unnecessary access to customer data. (Alrashed, 2016). Nonetheless, data access management and keeping the record of data access may be effective to prevent internal identity theft, but literature is missing on how e-tail organisations are managing the data access and how they keep the record of who access what information.

Having a comprehensive programme for internal and external training and education of employees on information security risk is also necessary to prevent information theft (Meinert, 2016). Also, the creation of the awareness on the severity regarding the risk of identity theft also has a significant impact on prevention of information theft (Boss *et al.*, 2015). Such awareness also changes the staff behaviour towards the safe and secure use of information resources (Boss *et al.*, 2015). Although, awareness of information security risk and training can help the staff to change their behaviour towards a secure use of information resources, while, how awareness is created, what information is helpful to increase the awareness, and how it affects the behaviour of staff members, has not been analysed in e-tail organisations.

Table 2. 6 List of the practices suggested for fraud prevention

Source	Managerial Practices	Interpretations
(Baz *et al.*, 2017).	- Effective internal control system helps in the fraud prevention. - Information sharing is significant practice in the fraud prevention.	- Such practice prevents misuse of IT resourse. - Anti-fraud awareness improves preventive measures.
(Alrashed, 2016)	- Organisations should: - Have a control system for access to personal information. - Recognise the identity of data handlers. - Have a record of staff having access to personal information and their criminal record check. - Organisations should implement strong encryption and firewalls on personal information. - Try to get the minimum required personal information from customers.	- It controlls unauthorised access to personal information. - Such identity may help in fixing responsibility in case of any misuse. - It would help to ensure control the access on personal information and track record of employees. - Encryption helps in preventing any unauthorised access on personal records. - Un-necessary customer information increases the extent of risk.
(Meinert, 2016)	- Having a comprehensive programme for internal and external training of employees on information security is also necessary to prevent information theft.	- Such training help employees in adopting better practices for secure use of IT and avert negative behaviour.
(Mithas and Rust, 2016) (Wilhelm, 2004)	- Regularly evaluate the performance of prevention systems.	- It would ensure the continued effectiveness of the system.
(Kumar and Goyal, 2016)	- Online organisations should send account login alerts to respected customers to prevent any unauthorised access.	- It may help detecting any IDF at an earlier stage.
(Wang *et al.*, 2015)		
(Boss *et al.*, 2015)	- Increasing the severity of the information theft risk for staff and customers and its awareness have a significant impact on identity theft prevention.	- Sense of insecurity results in arrangements for preventing IDT.
(Holt and Turner, 2012)		
(Albrecht *et al.*, 2011)		

(Copes *et al.*, 2010)		
(Prakash *et al.*, 2015)	- Online organisations should have effective authorisation and authentication system to validate the identities before access to customer accounts	- It is necessary to prevent any un-authorised access on customer accounts.
(Sharma *et al.*, 2015)		
(Ahamad *et al.*, 2014)	- Organisations should ensure the strong encryption at suppliers, vendors, and contractors to prevent any identity theft attack.	- Securing in-house resources is not enough, so take steps to secure customer information at every step.
(Taitsman *et al.*, 2013)		
(Seda, 2014)	- Regularly educate IT users on identity theft risk. - Educate IT users on measures to avoid identity theft.	- IT users should know the potential risks to avoid them. - It eases their job to secure identity information.
(Arachchilage and Love, 2014)		
(Teh *et al.*, 2016)	- Online organisations should have a strong authentication system using the biometric identification.	- Biometric authentication is the most effective tool to verify identification.
(Mansfield-Devine, 2013)		
(Usman and Shah, 2013)		
(Vahdati and Yasini, 2015)	- Organisations should ensure the similar arrangements for identity theft prevention at third parties.	- Similar arrangements at information sharing firms ensure IDT prevention at every step.
(Phan and Vogel, 2010)		
(Bang *et al.*, 2012)	- Sending one-time password for account access is a critical practice to prevent any unauthorised access.	- One time password helps to verify the identity of the customers.
(Prosch, 2009),	- Organisations should make arrangements at each step of customer data cycle. - At the transmission, they should have the practice of having strong encryption system. - The stored data should be secured from internal and external theft. - Organisations should have the practice of ensuring same protocols of information security by third parties if any personal information is shared with them.	- Information is processed at different stages, so security measures should be taken at each step. - Strong encryption ensures information theft prevention during transmission. - Database security is critical to prevent any IDT. - Sometime information is stolen from third parties, so firms should ensure similar information security measures with partners.
(Goyal *et al.*, 2012)	- Implement technological solutions such as strong encryption, SSL, anti-virus, firewalls, intrusion detection system, anti-phishing and digital certificates to prevent any information theft. - Invest in technologies such as anti-malware, anti-fishing	- Technological solutions are necessary to prevnet any cyber-security attack. - Sufficient investments in terms of technology, human
(Vijaya Geeta, 2011)		
(Devos and Pipan, 2009)		

	software, security of transaction getaway, monitoring of information communication. - Implement fraud reduction technologies (anti-virus, anti-malware, anti-fishing and other security systems) on customer devices on organisational expenses.	and other resources is necessary for effective measures. - IDT also occurs at customer side, which has impact on firms, so businesses should ensure IDT prevention at customer end.
(Amori, 2008)	- Internal and external prevention systems should be monitored for their performance and updated regularly	- Monitoring of the effectiveness of prevention system ensures its effectiveness.
(Delanty, 2005)		
(Boyer, 2007)	- Make sufficient investment in preventive technologies.	- For acquisition of sophisticated technologies, firms need to allocate sufficient budget.
(Wang *et al.*, 2006)	- Prevent unauthorised data access. - Train staff for secure use of information systems. - Ensure screening of staff members.	- Preventing unauthorised access safeguards sensitive data. - Training help staff to avoid possibilities of data breach. - Staff screening helps to minimise risk of IDT.

Table 2.6 presents the practices for information theft and fraud prevention in various industries as described in the literature. Most of these studies are focused on technological arrangements. Furthermore, these practices are based on examination of financial institutions and public sector organisations and limited to identity theft. Hence, no study has been found to focus on e-tail organisations. Thus, managerial practices regarding how organisations ensure the security of its information sources, how do they ensure the effectiveness of authentication system, how these organisations manage the access on customer information are still missing in the extant literature. Therefore, this study analyses managerial practices for identity fraud and information theft prevention and suggests improvements.

2.8.3 Detection

A fraud detection system consists of practices intended to uncover or locate a fraud before, during and after its occurrence (Wilhelm, 2004). Detection is a critical stage of fraud management; it provides the base for the rest of the stages, as without detection of frauds there will be no mitigation, analysis, policy, investigation and prosecution of the frauds (Jamieson *et al.*, 2007; Wilhelm, 2004). Fraud detection should be given significant consideration in fraud management as no matter how much organisations invest in prevention systems the fraudsters will still find their way to get into the systems (Porter, 2004). In online business, there should be a real-time detection system; as, many transactions take place in a short period, and if detection system fails to process these in real time, it will hang up the whole business process (Jamieson *et al.*, 2007).

For the detection of identity fraud in credit card and loan applications the practice of having an automated screening system built on an organisational database to detect any duplicate or suspicious application is a necessity (Dorfleitner and Jahnes, 2014; Hardouin, 2009; Swathi and Kalpana, 2013). Online transactions are enormous in number, therefore for an effective detection of identity frauds organisations should have a fraud screening system that flag out suspicious frauds for further verifications (Porter, 2004).

Having a fraud screening system based on pre-set cues is significant to spot suspicious frauds (Allan and Zhan, 2010). The fraud screening system is based on fraud cues based on rules and conditions, related to emerging fraud trends to detect identity frauds (Phua *et al.*, 2010). As the fraud trends are ever-changing, so to keep the effectiveness of fraud screening system intact, organisations should regularly update these cues, in accordance with emerging fraud trends (Allan and Zhan, 2010).

After detecting suspicious frauds, these are manually verified at the next stage to confirm whether these are frauds or genuine orders (Carneiro *et al.*, 2017). Having a fraud screening system and updating its cues regularly is helpful in detection of suspicious frauds. The effectiveness of the screening system is based on the proper implementation of fraud parameters, rules and conditions on the dataset (Allan and Zhan, 2010; Bierstaker *et al.*, 2006). However, the effective implementation of fraud parameters, rules and conditions depend on the skills, knowledge and awareness of employees regarding identity fraud in e-tail organisation. In addition, implementation of fraud cues on single organisation dataset is challenging (Allan and Zhan, 2010).

Although, the effectiveness of screening system depends upon its proper implementation, which requires skills, knowledge and awareness of employees but literature is missing on what skills and knowledge are required to analyse the parameters, trends and methods of identity frauds for effective detection in e-tail organisations. Furthermore, how e-tail organisations are enhancing the skills, knowledge and awareness of employees to effectively managing the fraud screening system have not been analysed.

Online customers are connected to the internet with an IP address, which is specific to each customer. This allows organisations to monitor IP address to detect any fraud at an early stage (Cheng *et al.,* 2015; Tan *et al.,* 2016). The practice of monitoring the customers' IP addresses helps organisations to know the location of account users. Thus, an attempt to access the account from an unusual location should trigger the screening system, which would help in detecting any fraud attempt (Tan *et al.,* 2016). Linking customers' devices with their accounts is also significant as a tool to detect identity frauds. Organisations should link customers' device(s) to their accounts so that with the help of device recognition system, identity frauds using suspicious devices can easily be detected (Al-Jumeily *et al.*, 2015; Ghosh, 2010; Peotta *et al.*, 2011).

Although, IP monitoring and linking customers' devices with their accounts and having a device recognition system would help in identity fraud detection, the literature on how e-tail organisations are using device recognition system, and how the practice of linking customers' devices with their accounts helps these organisations to detect identity frauds is missing. Furthermore, the literature on how the identification of customer location, helps e-tail organisations to detect identity frauds is also missing. So, this study tries to analyse these practices to suggest improvements in the effective use of these systems to detect identity frauds.

For early detection of identity frauds, customer education and awareness are also significant. Educating customers to regularly monitoring their bank statement and running transactions would lead to an earlier detection of frauds, which can reduce the chances of further frauds so that additional losses can be avoided (Tajpour *et al.*, 2013). However, how e-tail organisations educate their customers is still not known, and managerial practices, what to communicate the customers, what channels to use for such communication are also missing. Furthermore, setting up of a whistle-blower hotline is useful for detection of frauds (Porter, 2004). However, the anonymity of informers is necessary. Therefore, organisations should provide the customers and staff with a free hotline for fraud reporting with guaranteed anonymity (Njenga and Osiemo, 2013).

Moreover, Porter, (2004) also suggests for manual authorisation of each transaction, but in online business thousands of these take place in a few minutes, so it is not feasible to verify and authorise each transaction manually (Carneiro *et al.*, 2017). Setting up a whistle-blower hotline and manual verification of transactions are significant in detecting frauds, but the literature is missing on how e-tail organisations create such awareness among the whistle-blowers and ensure their anonymity. Above discussed managerial practices for fraud detection are given in Table 2.7.

Table 2. 7 List of the practices suggested for fraud detection

Source	Practices	Interpretations
(Allan and Zhan, 2010) (Carneiro *et al.*, 2017) (Phua *et al.*, 2010)	- Organisations should have an automated screening system, with predetermined cues that flag out the suspicious transactions. - Verify the suspicious transactions manually through fraud analysts. - Organisations should regularly update cues and ensure their accuracy according to identity fraud trends	- Automated screening system works just-in-time to detect any suspicious transaction. - Manual verification helps to identify any fraudulent transaction. - For effective IDFM, it is necessary to cope with emerging fraud trends
(Al-Jumeily *et al.*, 2015) (Ghosh, 2010) (Merriam and Tisdell, 2015) (Peotta *et al.*, 2011)	- Organisations should link customers' devices with their account and use device recognition system to detect IDF. - Device recognition system helps the organisations to detect suspicious transactions for using multiple accounts on one device.	- It helps to verify the identity of customers. - Such system helps to detect a new device accessing any customer account, which may help to detect any fraudulent transaction.
(Dorfleitner and Jahnes, 2014) (Hardouin, 2009)	- Organisations should have an automated screening system based on the characteristics of the applicants. - Organisations should manually review the suspicious applications.	- It helps identifying any suspicious transaction. - Manual reviews help to differentiate between genuine and fraudulent transactions.
(Petraşcu and Tieanu, 2014)	- Top management should ensure the effective internal control systems for fraud detection.	- Internal control system is an effective tools to detect any fraud at an earlier stage.
Swathi and Kalpana, (2013)	- Organisations should have automated detection system built on the organisational database to detect any duplicate or suspicious application.	- Detection system based on database is helpful to identify any fraudulent application.
(Tajpour *et al.*, 2013)	- Educate the customers' for regular monitoring of their bank statements and running	- Earlier fraud detection may help to mitigate the fraud impact.

	transactions for an earlier detection of the frauds.	
(Njenga and Osiemo, 2013)	- Management should provide anonymous telephone line to the staff and public for fraud reporting.	- It would help in detecting fraud at earlier stage, thus would result in less damages.
(Phua *et al.*, 2010)	- Organisations should use data mining techniques for fraud detection.	- Data mining techniques are significant to detect IDFs at earlier stage.
(Jamieson *et al.*, 2007)	- Should have a real-time fraud detection system.	- Fraud detected in real-time may result in no or least loss.
(Porter, 2004)	- Manually authorise each transaction. - Establish whistle-blower hotlines.	- It would help in identifying any fraudelent transaction. - Whistle-blower hotline may result in detection of any fraud well in time.

In Table 2.7 managerial practices suggested for effective detection of identity frauds are mentioned. Mostly these frauds are focused on the banking sector, credit card frauds and information security contexts. This shows that the financial sector is getting more importance in fraud management than e-tail sector. Although, some studies are focused on identity fraud detection, yet managerial practices related to e-tail context are still missing. Thus, not significant study has been found on the managerial practices for identity fraud detection in online retail organisations. Therefore, this study analyses the managerial practices for effective detection of identity frauds in e-tail organisations. It will also try to validate the significance of existing practices in current context and finally, suggestions are forwarded to improve the existing practices of e-tail organisations.

2.8.4 Mitigation

Mitigation starts with the certainty of the existence of a fraud or detecting a reasonable suspicious activity on any account. The purpose of mitigation is to lessen the severity of the fraud or minimising the fraud losses by stopping or discontinuing it. The mitigation practices are focused on controlling the extent of fraud, reducing the amount of the fraud losses and arrangements to recover or correct the implications of fraudulent attempt (Wilhelm, 2004).

Once a fraud or a suspicious transaction is detected, mitigation practices are performed to confirm the geniuses of the identity information, order re-confirmation, trying to contact the genuine customer or victim and recovery of customer account in case of any fraudulent attempt (Jamieson *et al.*, 2007; Wilhelm, 2004). As already mentioned the purpose of mitigation is to try to keep the losses at a minimum and discontinue the fraud, for that a real-time fraud mitigation system is suggested by Jamieson, *et al.* (2007) and Wilhelm (2004).

The notion ‘know your customer’ is also getting importance in effective detection of identity frauds. Albrecht, *et al*. (2011) maintain that organisations should ask their customers for any documentary evidence at the time of account opening to validate their identities, which will help to detect any identity fraud. Online organisations are also recommended to adopt the practices of updating the record of existing customers and devices and other identitical information to detect any fraud (Hardouin, 2009). Updated identity information also helps the organisations when a suspicious fraud is detected (Hardouin, 2009). To detect suspicious fraud, organisations are advised to make phone calls to the customers on their already given contact numbers to verify, whether it is a fraud or not (Cheng *et al.*, 2015; Tan *et al.*, 2016). Thus, through phone calls, organisations can challenge the fraudsters to verify the identity information in company records, which will help to detect a confirm fraud.

At the mitigation stage a third-party involvement in identity verifications such as phone number, address, tax number, and such other information on customer credit history is critically helpful (Jamieson *et al.*, 2007). After having such identity information, a telephonic call can further verify the genuineness of the customer (Cheng *et al.*, 2015; Tan *et al.*, 2016). A telephonic conversation would help to verify and validate the identity, based on the previous collected information.

In addition to the validation of the customer’s identity, the verification of geographic location is also critical as matching it with IP location of the purchase order will determine the genuineness of the transaction (Cross and Blackshaw, 2014). The practice is also significant for vetoing new applications for accounts. Such arrangements before starting a business with a customer would help online organisations to mitigate any fraud well before it occurs.

However, the literature does not reveal whether e-tail organisations implement such practices or not. If e-tail organisations have implemented above-mentioned practices for identity validation, but it has never been evaluated that what other identity information validation practices are implemented and how those are effective in e-tail organisation.

Information sharing on frauds is essential, as it helps to detect any fraud before it occurs (Feledi and Fenz, 2012; Power and Power, 2015). It helps to set the parameters and fraud cues based on such information. Through information sharing, any data used for fraud in one organisation can easily be detected at other organisations before the fraud occurrence. On the contrary, Chohan, *et al*. (2014) argue that organisations are reluctant to share such information due to lack of trust. Information sharing on identity frauds is critical to detect such frauds, but the literature on trust level to share such information among e-tail organisations is missing. Furthermore, managerial practices on what information is shared, and how is it used to detect identity frauds are also missing in the literature.

Real-time mitigation practices are necessary to control the fraud extent. However, the meaning of real-time mitigation differs from industry to industry, yet faster mitigation practices would ensure quick termination of fraud events, with reduced losses and impacts and updating victim's record (Wilhelm, 2004). The mitigation process should also be focused on recovery of customers' credit history in minimal time. Although, a real-time mitigation is suggested for rapid termination of frauds, it is still not known how e-tail organisations ensure the real-time mitigation of identity frauds as no significant work has been done.

Furthermore, what practices do the e-tail organisations have adopted to minimise the fraud losses, and how the customer credit history is recovered is not known. So far, the literature shows that there have been no significant studies on managerial practices for mitigation of identity fraud in e-tail context. Therefore this study analyses managerial practice in mitigation of identity frauds and suggests improvements.

Employees have a critical role in the effective detection of identity frauds. Systems can only point out a suspicious fraud, but experts need to go through the verifications, analysis and make decisions, so the detection systems should not replace the human but complement the experts (Becker *et al.*, 2010). The feedback on these decisions is also significant to evaluate the analysts' performance, so the fraud managers should promptly inform the decision makers about their decisions, and there should be a training programme to enhance their performance (Becker *et al.*, 2010).

The staff related practices in identity fraud detection cannot be undermined, but practices on how e-tail organisations train their staff for effective verifications of identity fraud detection are not analysed. Also, the practices on how e-tail organisations give feedback to fraud analysts to improve their performance in identity fraud detection are still missing in the literature.

For the effective mitigation of frauds, the organisations should develop criteria to prioritise the transactions, such as; the judgemental criteria should be based on the experiences and specialities of the fraud investigators, and high-value transactions should be investigated by the seniors (Wilhelm, 2004). The managerial practices for effective fraud mitigation are listed in the following table.

Table 2. 8 List of the practices suggested for fraud mitigation

Source	Practices	Interpretations
(Cheng *et al.*, 2015)	- For effective mitigation, phone calls help to verify whether it is a real customer or fraudsters, through asking identity related questions to match with records and credit history. - Online organisations should use IP address to check customer's location for effective identity fraud detection.	- Phone calls are more reliable to verify the identity of customers. - IP address location may help to detect any fraudulent transaction.
(Tan *et al.*, 2016)		
(Albrecht *et al.*, 2011)	- Organisations should monitor the customers' identities and ask for documentary proof for earlier detection of identity frauds.	- Documentary proof of identity is significant to verify the genuineness of customers.
(Amori, 2008)		
(Kahn and Liñares-Zegarra, 2016)		
(Cross and Blackshaw, 2014)	- Once a suspicious transaction is detected, organisations should verify the orders, geographic location and identity information to mitigate any chances of fraud.	- These verifications help to detect any identity fraud.
(Power and Power, 2015)	- Organisations should share the data related to frauds, with other organisations and law enforcing agencies, to help and get help to mitigate fraudulent attempts.	- Such information sharing helps in verifying the identity information of customers and stop any fraudulent transaction.
(Chohan *et al.*, 2014)	- Organisations are reluctant to share information on identity fraud management, due to the lack of trust among themselves.	- Due to the competition, firms are not ready to share information about measures taken to manage IDFs.
(Feledi and Fenz, 2012)	- For better mitigation, information sharing on fraud management is a critical practice.	- Information sharing helps to detect any fraud and verification of ID information.

(Becker *et al.*, 2010)	- Detection systems should not replace the human but complement the experts. - Managers should give feedback to fraud analysts on their decisions. - There should be a training programme for fraud analysts to enhance their performance.	- Detection system should include technology and manual process. - Such feedback helps staff to minimise the number of wrong decisions. - Training helps staff to improve their performance for management of IDFs.
(Hardouin, 2009)	- Know your customers. - Update the customers' data. - Monitor the customers' activities.	- Such activities help to verify the genuine customer information and detect any IDF attempt.
(Jamieson *et al.*, 2007)	- Organisations should have fast mitigation process. - Involve third parties for different verifications such as; phone number verification, address check, tax number and other identity-related information.	- It helps to minimise the extent of IDF losses. - Out-sourced verifications are significant to verify the identification through different channels.
(Wilhelm, 2004)	- Organisations should have a real-time mitigation system. - Continuously train the staff: - On emerging trends in identity frauds. - To effectively deal with red-flagged transactions. - The judgemental criteria should be based on the experiences and specialities of the fraud investigators. - The seniors should investigate the high-value transactions.	- In online business, a fast and accurate mitigation system is inevitable. - Staff training on emerging fraud trends and countermeasures helps improving the detection of ID frauds. - Investigators should be specialised in respected fields. - High value transactions need more expertise to deal with.

Table 2.8 mentions the practices in the mitigation of the frauds. These practices are focused on banking, insurance, mortgage and telecommunication organisations and government agencies for application fraud, mobile payment fraud, identity fraud and internal frauds. Furthermore, most of these studies have been investigated in a technological context. Moreover, managerial practice on how e-tail organisations mitigate identity fraud and verify the genuineness of customer identity are missing. Therefore, research will try to answer these questions by analysing the managerial practices that effectively mitigate the identity frauds in e-tail organisations.

2.8.5 Analysis

This stage is critical, as it evaluates the performance of the other stages of fraud management. The importance of this stage lies in its function of reviewing the performance of each stage in fraud management and providing them with the feedback for improvement (Jamieson *et al.*, 2007; Wilhelm, 2004). This stage also works on the analysis of the fraud, its type, nature, methods used to commit it and losses incurred. It also suggests strategies and measures to cope with such frauds in future (Apel and Nagin, 2017; Rose *et al.*, 2015)

The analysis process includes the assessment of fraud risks and suggestions to minimise these risks. These suggestions may relate to allocating more funds, staff availability, training and sophisticated technology, so it is necessary to involve senior management in analysis process (Coulson-Thomas, 2017; Yelland, 2013). Additionally, organisations are suggested to evaluate the performance of employees, their strength and weakness and quality of work in fraud management, which will help the management to improve the human aspects of fraud management (Vahdati and Yasini, 2015). This shows that the senior managers should regularly evaluate the performance of employees who are involved in fraud management, which can increase the effectiveness of its process in e-tail organisations. However, the managerial practices regarding the evaluation of employee's performance and their factors for identity fraud management have not been analysed in e-tail organisations.

The fraud vulnerability review helps organisations to improve prevention and detection strategies (Seda, 2014). Such reviews analyse the organisational exposure to the fraud attempts and help predict possible ways of fraud attempts, based on that review; organisations can establish effective prevention and detection strategies (Bierstaker *et al.*, 2006). Organisations should also analyse the performance of detection system through statistical and false positive ratio analysis, to locate the weaknesses of the technology. Furthermore, evaluation of prevention system is also suggested, for which penetration test and vulnerability assessment are recommended (Rogers, 1975; Seda, 2014).

For the effectiveness of overall fraud management, organisations should analyse the performance of the tools, techniques and processes used in identity fraud management, as it would help to enhance their performance (Dorminey *et al.*, 2012; Phan and Vogel, 2010). Additionally, Fraud analysis may also include risk assessment, knowing fraud trends, diagnosing patterns and methods of frauds and calculating the fraud losses (Apel and Nagin, 2017; Rose *et al.*, 2015; Yelland, 2013). The fraud risks and emerging trends should continuously be monitored as with the technological advancements, online fraud and its trends are rapidly changing Weisman and Brodsky (2011). The literature findings on fraud analysis are given in the following table.

Table 2. 9 List of the practices suggested for fraud analysis

Source	Practices	Interpretations
(Coulson-Thomas, 2017)	- Involve the top-level management in the analysis of frauds, to seek their input into fraud management.	- Involvement of top-level management will ensure input from all areas of business.
(Apel and Nagin, 2017) (Rose *et al.*, 2015) (Yelland, 2013)	- Fraud analysis should include risk assessment, knowing fraud trends, diagnosing patterns and methods of frauds, calculating fraud losses and evaluating the system.	- Fraud analysis should be comprehensive enough to cover all areas of IDFM.
(Dorminey *et al.*, 2012) (Vahdati and Yasini, 2015)	- For the effectiveness of identity fraud management, organisations should analyse the performance of tools, techniques and process involved in it.	- Such practice would help in improving the performance of tools and techniques used for IDFM.
(Vidalis and Angelopoulou, 2014) (Yelland, 2013)	- Analysis process should help to improve the management of identity theft.	- Suggestions for improvement should be the outcome of IDF analysis process.
(Vahdati and Yasini, 2015)	- Organisations should analyse the performance of employees, their strength and weakness and quality of work in fraud management.	- Such analysis would help to improve the staff performance in IDFM.
(Seda, 2014)	- The performance of prevention tools should be analysed by penetration testing and vulnerability assessment.	- These tests can identify limitations of the system and may help improving them.
(Weisman and Brodsky, 2011)	- Organisations should continuously monitor the frauds risks, and its management practices as the fraud are dynamic and evolving.	- Continuous monitoring of fraud risks and management would help to cope with emerging fraud trends and their management.
(Jamieson *et al.*, 2007)	- Review the performance of stages of identity fraud management and suggest improvements. - Organisations should analyse the past and suggest improvements in future practices in IDFM.	- Performance review of each stage of fraud management would help to identity and redress their limitations. - Base on previous arrangements and countermeasures, analysis

		stage should suggest improvements.
(Bierstaker *et al.*, 2006)	- Analyse the vulnerability of organisation for fraud risks. - Analyse the performance of detection system through statistical and false positive ratio analysis.	- It would help to develop countermeasures to manage IDFs. - Performance analysis of detection system may lead to its performance improvement.
(Wilhelm, 2004)	- Review the performance of each fraud management stage and provide feedback and measures to improve it.	- Such review practice would help improving overall management of IDFs.

The practices at the analysis stage (see Table 2.9) are related to fraud risk management, review of the performance of tools, techniques and process and that of the staff members in fraud management. Accordingly, an analysis stage helps to improve management of identity frauds.

Although, these suggestions are significant to improve identity fraud management, however managerial practices on how e-tail organisations analyse their systems and staff performance, are missing. Therefore, this study tries to analyse managerial practices in identity fraud analyses in e-tail sector and forwards some improvements for an effective analysis.

2.8.6 Policy

The managerial practices under the policy may include the creation, evaluation, communication and compliance with the policies to manage the frauds effectively (Wilhelm, 2004). Creating and maintaining an anti-fraud policy is necessary to guide the employees and to maintain the organisational performance. So while making an anti-fraud policy, the organisations should consider all the stages in fraud management and ensure its compliance to safeguard against identity frauds (Njenga and Osiemo, 2013).

Fraud management policies are the matter of survival for business organisations, therefore these should be dealt at the higher ranks and should be included in boardroom agenda (Coulson-Thomas, 2017) as they can consider all the fields in the area and the overall business needs. In addition, employees' participation is also necessary because it has a two-fold advantage (Chen *et al.*, 2015). First, they input their initial information gained through their personal experiences and second, their involvement in the policy development can be a motivating factor to its compliance (Chen *et al.*, 2015).

Furthermore, fraud policies should include the technical, organisational and human aspects of fraud management, as an absence of any aspect would limit its effectiveness (Ji *et al.*, 2007; Rhee *et al.*, 2012). In addition, organisations that share their information with other parties and contractors should also ensure same information security protocols and anti-fraud policies for them (Liu *et al.*, 2010).

After devising fraud management policies, the organisation should regularly evaluate and update those (Bechtsoudis and Sklavos, 2012). This helps to ensure that the policies are helping to achieve their purpose. Updating policies in response to emerging threats are critical for ensuring that the objectives of the policies are being achieved, but how e-tail organisations update identity fraud policies, and frequency of their review is not known in the literature.

Without proper compliance the developed policies will not yield desired results. For effective compliance, policy awareness is the first step. To this end, organisations should communicate the policies to each related staff member and ensure that the recipient read and understood the policies (Bierstaker *et al.*, 2006; Siponen *et al.*, 2014; Soomro *et al.*, 2016).

Additionally, awareness training is also suggested by Singh, *et al.*, (2013). The suggestions for policy communication and creating awareness through training are pre-requisite for any policy compliance, but what channels are effective for policy communication and how to ensure that staff read and understood identity fraud policies in e-tail organisations had not been analysed.

In addition to policy communication and awareness, organisations should have a mechanism to monitor and audit policy compliance (Chen *et al.*, 2015; Parsons *et al.*, 2014; Singh *et al.*, 2013). Monitoring is a continuous process implemented by the immediate supervisors to ensure that the staff is complying with fraud policies effectively. For this it is necessary that the senior staff should be aware of related policies (Njenga and Osiemo, 2013; Wright, 2007).

In addition, the organisations should provide training and awareness to their staff on policy compliance methods and processes (Chen *et al.*, 2015; Singh *et al.*, 2013; Soomro *et al.,* 2016). Such training and awareness influence the employees' perceptions and assumptions on identity frauds, which result in compliance behaviour of fraud policies. The literature findings on the managerial practices regarding IDFM policies and related issues are summarised in the following table.

Table 2. 10 List of the practices suggested for fraud policy

Source	**Practices**	**Interpretations**
(Coulson-Thomas, 2017)	- Fraud management policies should be dealt at highest ranks in organisations	- Involvement of top level management may ensure comprehensive policies on IDFM.
(Soomro *et al.*, 2016)	- Organisations should have comprehensive policies on information security. - Organizations should create policy awareness. - Train the employees on policy compliance methods.	- It would cover a wider aspects of IDFM. - Policy awareness is a key to compliance. - It would help them to comply with IDFM policies.
(Chen *et al.*, 2015)	- Encourage employees' participation in the design and development of information security policies. - Ensure policy compliance through close monitoring.	- It's a motivational technique for effective policy compliance. - Immediate supervisors should ensure policy compliance.
(Parsons *et al.*, 2014)	- Make the employees aware of the information security policies. - Train the staff to develop their positive attitude towards the policy compliance. - Organisations should have policy compliance mechanism.	- Policy awareness is first step toward policy compliance. - It enhances staff motivation toward the compliance. - It would help ensuring effective compliance.
(Siponen *et al.*, 2014)	- Create awareness, as it is a useful mechanism for policy compliance.	- Unless staff know the policies, compliance is not possible.
(Njenga and Osiemo, 2013)	- Create and maintain an anti-fraud policy to guide the employees. - While making an anti-fraud policy, consider all stages of fraud management and overall business objectives. - Anti-fraud policies should apply to all members of staff including the senior managers.	- Management should create policies for all to comply with. - IDFM policies should be comprehensive to cover every aspect of fraud management. - Every staff member should comply with the IDFM policies regardless of their designation.

(Singh *et al.*, 2013)	- Organisations should have comprehensive policies on information security. - For the compliance of policies, awareness and training programs should be implemented. - There should be an effective mechanism for policy compliance.	- Firms should have a set of policies on information security. - Policy awareness and training are necessary for compliance. - Staff should know the mechanism on how to comply with policies.
(Bechtsoudis and Sklavos, 2012)	- Update the policies regularly. - The policies should be evaluated to ensure their effectiveness for the purpose.	- It helps to counter emerging challenges. - Such evaluation would result in the effectiveness of the policies.
(Ji *et al.*, 2007)	- The policies should focus on technical, organisational and human aspects of fraud management.	- Such policies would be comprehensive to encompass every aspect of fraud management.
(Rhee *et al.*, 2012)		
(Liu *et al.*, 2010)	- Regularly update the policies for their effectiveness. - Organisations should ensure the same policy for third party contractors regarding the IS and fraud management.	- With the emerging fraud trends, policies become obsolete. - Shared customer data has similar risks at other firms, so businesses should ensure similar policies with partners.
(Albrechtsen and Hovden, 2010)	- Involve the employees in policy development. - Enhance the employees' knowledge of policy and compliance methods.	- It helps to develop effective policies and is a motivational technique for compliance. - Having knowledge on compliance methods would create a complying culture.
(Wright, 2007)	- Anti-fraud policies should also apply to the senior management. - Anti-fraud policies should establish the organisation's commitment to combating frauds and communicate organisational stance against frauds.	- Every staff member should comply with anti-fraud policies. - Anti-fraud polices should reflect firms standing against frauds.
(Bierstaker *et al.*, 2006)	- Organisations should develop and maintain anti-fraud policies. - Anti-fraud policies should be stand-alone and distinct from firm's code of conduct. - A written acknowledgement should be ensured that all the staff have received a copy and understood it.	- Having policies is the first step towards IDFM. - Anti-fraud policies should have a separate recognition. - It helps to ensure policy compliance.

Anti-fraud policies have a significant impact on the management of information security and frauds. Table 2.10 presents the managerial practices suggested by various authors in information security, internal, banking and accounting frauds. The extant literature suggests various managerial practices on policy development, updating, communication and awareness and compliance, but the literature on managerial practices in e-tail sector is missing. Therefore this study tries to analyse managerial practices in e-tail sector to give an insight into the sector and suggest some improvements in identity fraud related policies and related issues.

2.8.7 Investigation

In the fraud management domain, investigation refers to practices related to inquiries into the facts about the fraud, collecting physical and digital evidence to identify the fraudsters (Jamieson *et al.*, 2007). So far, the fraud investigations should be focused on collecting sufficient evidence for effective prosecution and means for the recovery of losses (Furlan and Bajec, 2008; Rose *et al.*, 2015).

Wilhelm (2004) suggests three sets of practices, i.e., internal investigations, external investigations and coordination with law enforcing agencies. The internal investigation practices refer to investigations of employees, contractors and vendors. Investigation of customers for fraudulent claims and practices to find facts on committed frauds are the part of external investigations. The coordination with law enforcing agencies refers to providing information, evidence and sources of the frauds, and to maintain a partnership with every level of the law enforcing entities. Such practice of coordinating with law enforcing agencies is also recommended as inevitable for online fraud investigation by Cross and Blackshaw (2014).

Law enforcement agencies face problems when gathering and preserving evidence from live systems, electronic devices, search and seize the devices and other technological issues (Cross and Blackshaw, 2014). Business organisations should help them in technological areas and build a close partnership for effective investigation (Gogolin and Jones, 2010). The law enforcing agencies may lack interest in small financial frauds as they have some other important responsibilities (Cross and Blackshaw, 2014). However, the collaboration and effectiveness of investigation can be enhanced by employing a team of specialist investigators (Amori, 2008). These specialist investigators should have a background in fraud investigations and knowledge on technological systems to extract evidence and build a case for prosecution (Lewis *et al.*, 2014). These suggestions are based on studies on the ability of law enforcing agencies in dealing with digital crime. Despite the fact that these studies show the significance of employing private investigators, literature is missing on what should be their specialities, their working background and how to enable them working with e-tail organisation-specific technological systems in identity fraud investigations domain.

With a team of specialist investigators, business organisations should conduct the investigations at their end and be involved in a further investigation conducted by law enforcement agencies (Brooks and Button, 2011; Lewis et al., 2014). Only financial aspect is involved in identity frauds in e-tail sector, and with a small amount involved, the law enforcing agencies are reluctant to take the cases and investigate (Cross and Blackshaw, 2014). Sometimes the local police are not interested in online frauds, because of lacking technical expertise in digital investigations, so identity fraud investigations at the business end are inevitable (Lewis *et al.*, 2014). Investigations of identity frauds at the organisational end is significant, but no study presents a clearer picture of how e-tail organisations investigate identity frauds.

The collection of evidence is a critical part of investigations; organisations are advised to collect evidence from internal and external sources and field investigations (Cross and Blackshaw, 2014). The internal investigations refer to extracting evidence from live information systems, databases and other sources. The use of internal and external sources is significant to collect evidence. The external sources may include telephone directories, financial databases, credit history and any other data bases available through external organisations.

The investigation should include a complete set of documents, description of the activities, contact information, and physical and digital evidence (Wilhelm, 2004). After collecting the evidence, it is necessary to preserve it. Online organisations should have an authentic electronic evidence preservation system to preserve the evidence for the courts of law (Gogolin and Jones, 2010). The collection and preservation of digital evidence need technical expertise and forensic resources. The availability of these resources requires sufficient funds, so organisations should invest in human resources and technology to make its investigations more effective (Wang *et al.*, 2006). Collecting and preserving digital evidence and documentation of frauds is critical in investigations, but how e-tail organisations document, collect and preserve digital evidence is missing in the literature. Furthermore, it has not been analysed that what evidences are required to justify and prosecute the fraudsters. Therefore, this study analyses these managerial practices to verify their significance in identity fraud investigations in e-tail sector and suggest improvements.

Table 2. 11 List of the practices suggested for fraud investigation

Source	Practices	Interpretations
(Cross and Blackshaw, 2014)	- For effective investigations, close coordination with police should be established. - Law enforcing agencies may not investigate all frauds, so business organisations should come forward to investigate privately. - Collect evidence from internal and external sources for field investigation and prosecution.	- It helps to take legal action against fraudsters. - E-tailers should assume the responsibilities of IDF investigations. - Evidence collection should be the core function of fraud investigations.
(Amori, 2008)	- For better investigations and prosecution, organisations should consider private agencies or appoint expert team.	- Government agencies are less interested in small scale business frauds, so firms should take such responsibility.
(Brooks and Button, 2011)	- Conduct investigations at the business end.	- E-tailers should assume the responsibility of fraud investigations and coordinate with law enforcing agencies for further actions.
(Lewis *et al.*, 2014)	- Be involved in further investigations conducted by law enforcement agencies.	
(Furlan and Bajec, 2008)	- Fruad investigations should be aimed at collecting evidence, which supports for effective prosecution. - Fraud investigations should also focus on recovery of losses.	- Evidence collection during fraud investigations should be supporing for prosecution. - It would help businesses to controll fraud losses.
(Rose *et al.*, 2015)		
(Gogolin and Jones, 2010)	- Develop strong coordination with law enforcing organisations by helping them in technological areas. - Build a close partnership with law enforcing organisations for effective investigation. - Authentic electronic evidence preservation system should be adopted.	- Law enforcing agencies may lack required technologies to collect digital evidence, so firms should come a step ahead. - Help law enforcing agencies in fraud investigations. - Firms should have a system to preserve electronic evidences.
(Jamieson *et al.*, 2007)	- Police lack interest in online frauds because of lack of resources and IT skills.	- E-tailers should assume the responsibility of fraud investigations.

(Lewis *et al.*, 2014)	- For investigations, organisations should have skilled and experienced investigators and forensic experts. - Organisations should have knowledge of state laws on investigation and prosecution. - Organisations should have an expert system on preserving and presenting the evidence.	- Business firms are expected to have specialist fraud investigators. - Knowledge on state law regarding on fraud is pivotal for effective investigations. - E-tailers should assume responsibility to preserve and present digital evidence.
(Wang *et al.*, 2006)	- Invest in resources for effective investigations of frauds.	- Sufficient investment is necessary for fraud investigations,
(Wilhelm, 2004).	- Investigations should include a complete set of documents, description of the activities, contact information, any physical and digital evidence. - Investigation practices should include the coordination with law enforcing agencies.	- Investigation reports should be comprehensive, to include all the information required for prosecution. - Without coordination with law enforcing agencies, fraud may not give required outcome.

Table 2.11 presents the managerial practices for effective investigations of digital crime, business and identity frauds. Most of these practices are focused on information security attacks and other technological aspects. A few of these are focused on police role and organisations arrangements, but the practices on how online retail organisations investigate identity fraud are still missing. Further, the practices on how online retail organisations cooperate with police and other law enforcing agencies are also missing. Therefore, this research analyses the managerial practices on how these organisations investigate identity frauds and cooperate with law enforcing agencies. This research also suggests some improvements in fraud investigations to e-tail organisations.

2.8.8 Prosecution

The prosecution stage refers to the litigation with the fraudsters in the courts of law to get the fraudsters punished and request the court for appropriate compensation (Wilhelm, 2004). Successful prosecutions send explicit messages to potential fraudsters, which enhance the deterrence and business reputation against fraudsters (Dorminey, 2012). The fraudsters are sanctioned and punished according to the state laws, which vary from country to country (Brook and button 2012). As this study is based in the UK, so the fraudsters are prosecuted according to the laws of this country. Related to the identity frauds, UK has Fraud act 2006 to prosecute the fraudsters.

According to the Fraud Act, 2006 section 1*, "A person is guilty of fraud if he is in breach of any of the sections listed in subsection (2) (which provide for different ways of committing the offence".* Regarding the Identity fraud sub-section 2 (a) mentions that any false representation is a fraud, and its result would be a fine or an imprisonment or both (Savirimuthu and Savirimuthu, 2007).

The business organisations should involve in prosecution process as the law enforcing agencies have less expertise in collecting, preserving and presenting the digital evidence (Gogolin and Jones, 2010). In the absence of state intervention frauds are growing. Therefore, private organisations should involve in investigation and prosecution (Lewis *et al.*, 2014). Although, the successful prosecution has a direct impact on deterrence through creating fear of punishment which helps to reduce the frauds. However, it depends upon the role of e-tail organisations how aggressively they involve in prosecution to get fraudsters punished. Moreover, the prosecution is the process in which various external organisations and law enforcement agencies are involved, such as police and private investigation and recovery firms. Nevertheless, managerial practices for information sharing with outside organisations have not been analysed. In addition, it has also not been analysed what and how they present the information based on evidence with the court and other entities to prosecute the fraudsters. Therefore, this study analyses the managerial practices for the prosecution of identity fraudsters in e-tail organisation.

2.9 Finding a Research Gap

Identity frauds have a critical impact on online business organisations. They constitutes more than half of total frauds faced by the business industry. Every year a significant amount of revenues is lost through fraud. This has a negative impact on the customers' buying behaviour and a significant obstacle towards the growth of the online business industry.

The extant literature has many studies on identity fraud, but only a few studies present a comprehensive approach to identity fraud management. However, the few practices discussed in identity fraud management literature do not have a direct focus on e-tail organisations. For a comprehensive approach to identity fraud management, previously mentioned stages are commonly suggested. The literature at each stage of fraud management has been reviewed, and some related frameworks were also discussed giving a meaningful insight into the state of the literature.

Deterrence has been focused on as the first line of defence. The extant literature (see Table 2.4) has many studies on the importance of deterrence in fraud management. Various studies have focused on the significance of deterrence and suggested actions to make the deterrence more effective (see Table 2.4). At the same time, investigation of managerial practice in identity fraud deterrence in e-tail organisations is still missing. This indicates a research gap that needs to be bridged to promote improvements in fraud deterrence in e-tail firms.

Similarly, there are numerous studies that are focused on customer education and awareness as measures of information theft prevention and fraud deterrence (Amori, 2008; McGee and Byington, 2015; Arachchilage and Love, 2014; Dorminey *et al.*, 2012; He *et al.*, 2014; Seda, 2014), but there are no studies investigating these issues in realtion to the e-tail industry. To rectify this situation, the present study investigates managerial practices in customer education for effective identity fraud deterrence, and forwards some suggestions to improve these practices in e-tailing.

Prevention is a critical stage in IDFM. At this stage measures are taken to prevent any IDT and securing customers' account from unauthorised access. For preventing the IDT various studies have been carried out (Albrecht *et al.*, 2011; Alrashed, 2016; Baz *et al.*, 2017; Copes *et al.*, 2010; Devos and Pipan, 2009; Holt and Turner, 2012; Meinert, 2016; Prosch, 2009; Seda, 2014; Usman and Shah, 2013; Vijaya Geeta, 2011), but no significant research has been carried to investigate IDT prevention issues in the e-tail sector. Additionally, there have been some studies on preventing unauthoirsed access on customers' accounts (Mansfield-Devine, 2013; Prakash *et al.*, 2015; Teh *et al.*, 2016), however, no study has been found on the prevention of unauthorised access on e-tail customers' account. Thus, the managerial practices on identity fraud prevention are still missing in e-tail sector. To help bridging this gap, the present study analyses managerial practices in preventing IDT and unauthorised access on customers' account for effective IDF prevention and suggests improvements in these practices in e-tailing.

Table 2.6 presents the managerial practices for detection as suggested by various authors. The practices of having automated detection system and verification of suspicious transactions are recommended by various reserchers (Al-Jumeily *et al.*, 2015; Allan and Zhan, 2010; Becker *et al.*, 2010; Carneiro *et al.*, 2017; Dorfleitner and Jahnes, 2014; Ghosh, 2010; Hardouin, 2009; Njenga and Osiemo, 2013; Peotta *et al.*, 2011; Swathi and

Kalpana, 2013) in different contexts. Additionally, some studies (Phua *et al.*, 2010; Tan *et al.*, 2016) on fraud detection are focused on technological aspects only. So far, no study has been found focusing on the detection of IDFs in the e-tail industry. To rectify this situation, the present research analyses managerial practices and forwards suggestions to improve these practices for an effective IDF detection in e-tail sector.

Similarly, no substantial work covering the mitigation of identity frauds in online retail organisations has been found. None of the studies on IDF mitigation (Jamieson *et al.*, 2007; Power and Power, 2015; Wilhelm, 2004) has investigated managerial practice in IDF mitigation in e-tailing. This study responds to the challenge by understanding IDFM, analysing the managerial practices in IDF mitigation and forwards suggestion to improve these practices in e-tail industry.

Analysis of IDFs is a critical stage that helps to develop policies and strategies for effective IDFM. The extant literature has some studies on fraud analysis (Bierstaker *et al.*, 2006; Coulson-Thomas, 2017; Rose *et al.*, 2015; Seda, 2014; Vahdati and Yasini, 2015; Vidalis and Angelopoulou, 2014) but none of these studies have focused on IDF analysis in e-tail sector. In the absence of any research, the e-tailers have no significant practices to control IDF through effective fraud analysis. To correct that situation, this research investigates the managerial practices in IDF analysis in e-tail industry. The present study suggests some improvements in existing managerial practices, which will help e-tailers to improve IDF analysis process leading to adopt better anti-fraud strategies.

Policies have critical role in driving the behaviour of staff towards the achievement of organisational objectives. In IDFM, policies have significant role to adopt anti-fraud practices. The extant literature has some studies (Chen *et al.*, 2015; Coulson-Thomas, 2017; Njenga and Osiemo, 2013; Parsons *et al.*, 2014; Singh *et al.*, 2013; Soomro *et al.*, 2016) but none of these have investigated managerial practices related to policy issues in e-tail sector. To help bridging this gap, the present research analyses the managerial practices in IDFM policies and related issues. This study suggests improvements in existing managerial practices and adds some more practices for the development, communication, awareness and compliance of IDFM policies in e-tail sectorIn the same vein, studies on investigation and prosecution (see table 2.10) are not focused on the identity fraud management in e-tail sector. The absence of such practices in e-tail industry results in lack of proper investigation and prosecution of IDFs. To rectify this situation, the present study analyses the managerial practices in investigation and prosecution of IDFs in e-tail sector.

This study helps to understand the management of identity fraud, analyses the managerial practices in e-tailing and suggest improvements. The issue of identity fraud relates to online sales of e-tailers, so better managerial practices may help in effective management of identity frauds (Jamieson *et al.*, 2007; Wilhelm, 2004). Researching the firms at grassroots level may be effective to help improving their core functions. However, effective management of identity frauds needs a comprehensive set of managerial practices at each stage of fraud management. The grassroots level study may help better in incorporating the basic functions related to production, human resources management, financial and operational management, whereas IDFM is more focused on managerial practices limited to combat online frauds based on stolen or fictitious identities. Such study may not be helpful in management of identity frauds as it requires a set of advanced managerial practices with support from IT and information sharing with outside industry. Therefore, this study is limited to understand IDFM, analyse managerial practices and suggest improvements for e-tail sector.

To summarise, there have been some studies on comprehensive fraud management. The extant literature also has some studies focusing on one or more stages of fraud management. These studies have suggested various managerial practices at each stage of fraud management in various contexts. Although, there are numerous managerial practices at each stage of fraud management, however, these have not been analysed in identity fraud management in e-tail context. These are some questions awaiting resolution: What managerial practices are there to manage each stage of identity fraud management? Are the practices of fraud management existing outside e-tailing going to be effective in the e-tail context? Moreover, how can these practices be improved to make identity fraud management effective in e-tail sector? To investigate these issues, this study aims at understanding IDFM, analysing the managerial practices at each stage of the fraud management and suggest improvements, through an empirical study. Thus, the objectives of this research are: a) to explore identity fraud types facing the e-tail sector in the UK, b) to investigate the existing managerial practices of IDFM in e-tail sector and c) to extend the fraud management lifecycle framework (Wilhelm, 2004) for improving managerial practices in IDFM in e-tail sector. The Fraud management lifecycle framework has also been extended in the current context, the proposed framework is presented below.

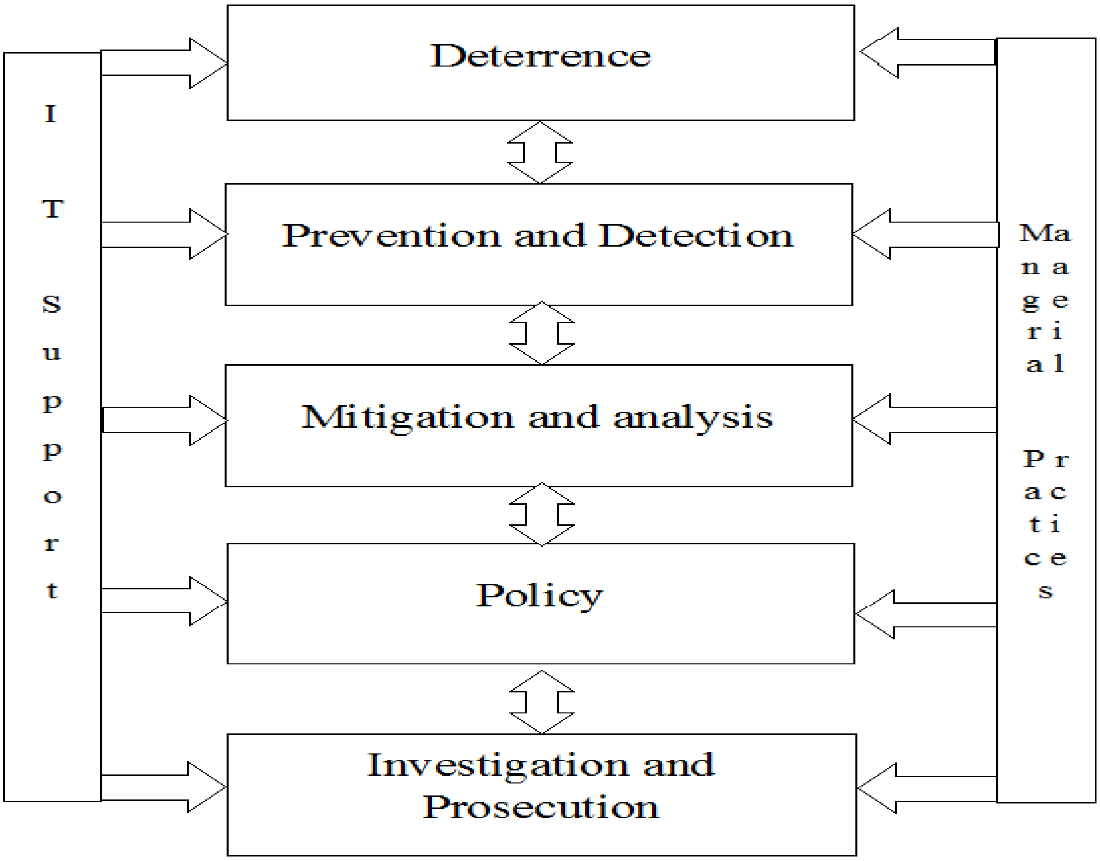

Figure 2. 6 A Conceptual Framework for Management of Identity Fraud.

2.10 Summary of the Chapter

This chapter presented an overall view of the existing state of the art in fraud management. At the beginning, literature was reviewed and significance of managerial practices was explored in business management. The types and the impact of identity frauds on UK's economy were presented. The picture of identity fraud types and its trends were also conceptualised to understand the frauds, trends and implications. The literature on the management of fraud was reviewed to understand what constitutes an effective fraud management. Thus, the eight stages were found to be critical for fraud management. Based on the understandings on a holistic approach for fraud management, the literature was reviewed to explore frameworks. After exploring fraud management frameworks, these were reviewed to evaluate their appropriateness for extension in identity fraud management. Thus, selection of an appropriate framework would help to explore managerial practices in fraud management at each stage and analysis of empirical results from e-tail organisations.

Managerial practices at each of the eight stages were explored in fraud management. Reviewing literature on these managerial practices helped to understand the current state of the art in fraud management and their limitations. During the review process, it was found that no study has been focused on IDFM in e-tail sector. Although, no research was found in IDFM in e-tail context, yet the literature on managerial practices in different contexts would help to analyse empirical data, to know their significance and limitations. In the absence of IDFM practices in e-tail sector, the process of integrating the literature and empirical data would result in suggesting effective managerial practices.

The extant literature helped to understand the weaknesses in IDFM system, not only in relation to having or not having any system but the issues related to how these systems are implemented in the current domain, and what makes these systems work effectively, are more critical. So far, how and what about the technology, people and process directed this study towards an in-depth enquiry into the issues of IDFM. Therefore, the qualitative method has been adopted, and semi-structured interviews were conducted to know how what and why about IDFM practices. Furthermore, the review process also helped to understand that separate management of the stages is not possible in small and medium organisations, therefore, large organisations were selected for data collection. The methodology of this study is presented in the next chapter.

CHAPTER 3
METHODOLOGY

3.1 Introduction

The purpose of this chapter is to discuss the philosophy adopted in this research as well as to explain and justify the choice of specific research methods used for data collection. Methodology is a critical part of any research as it helps to attain the research objective. Selection of appropriate methods and approaches is a critical decision, which can affect the reliability and validity of the research. Therefore, each selected approach or method has to be justified with the aims and objectives of this research in mind.

This research is aimed at understanding IDFM, analysing the managerial practices in e-tail organisations based in the UK and suggesting improvements by extending the fraud management lifecycle framework proposed by Wilhelm (2004). To achieve the research objectives the qualitative approach of data collection is used. In the previous chapter, a comprehensive review of the literature was carried out, which allowed to identify a research gap.

In this chapter, relevant research philosophies are discussed and the most appropriate one is selected. Furthermore, the two main research methodologies, quantitative and qualitative, are analysed from the point of view of their potential use in this study. The quantitative methodology is associated with the positivist philosophy and is preoccupied with quantification, replicability, objectivity and causality (Bryman, 2015). On the other hand, qualitative research helps to understand the real world in actions. As a result, qualitative methods help the researcher to understand the problem under investigation by collecting the data in a natural setting (Creswell and Poth, 2017). Within a qualitative dataset, ethnography, grounded theory and case study are the most common research designs. In this chapter I examine these research designs in terms of their appropriateness for this study and conclude in favour of a case study design. A detailed presentation of the implemented case study design that follows ensures the replicability of my research.

This research uses the identity fraud management lifecycle framework proposed by Wilhelm (2004) as an underpinning theory. This requires the adoption of a deductive approach to extracting themes from primary sources. The findings are prodiced through thematic analysis based on coding, categorising and extracting themes from a qualitative dataset. This research uses three real-life case studies for data collection, and predefined criteria were setup for the selection of the cases. A pilot study was conducted to test the research instrument for validity. Figure 3.1 presents approaches adopted for this study, and each section is detailed in this chapter.

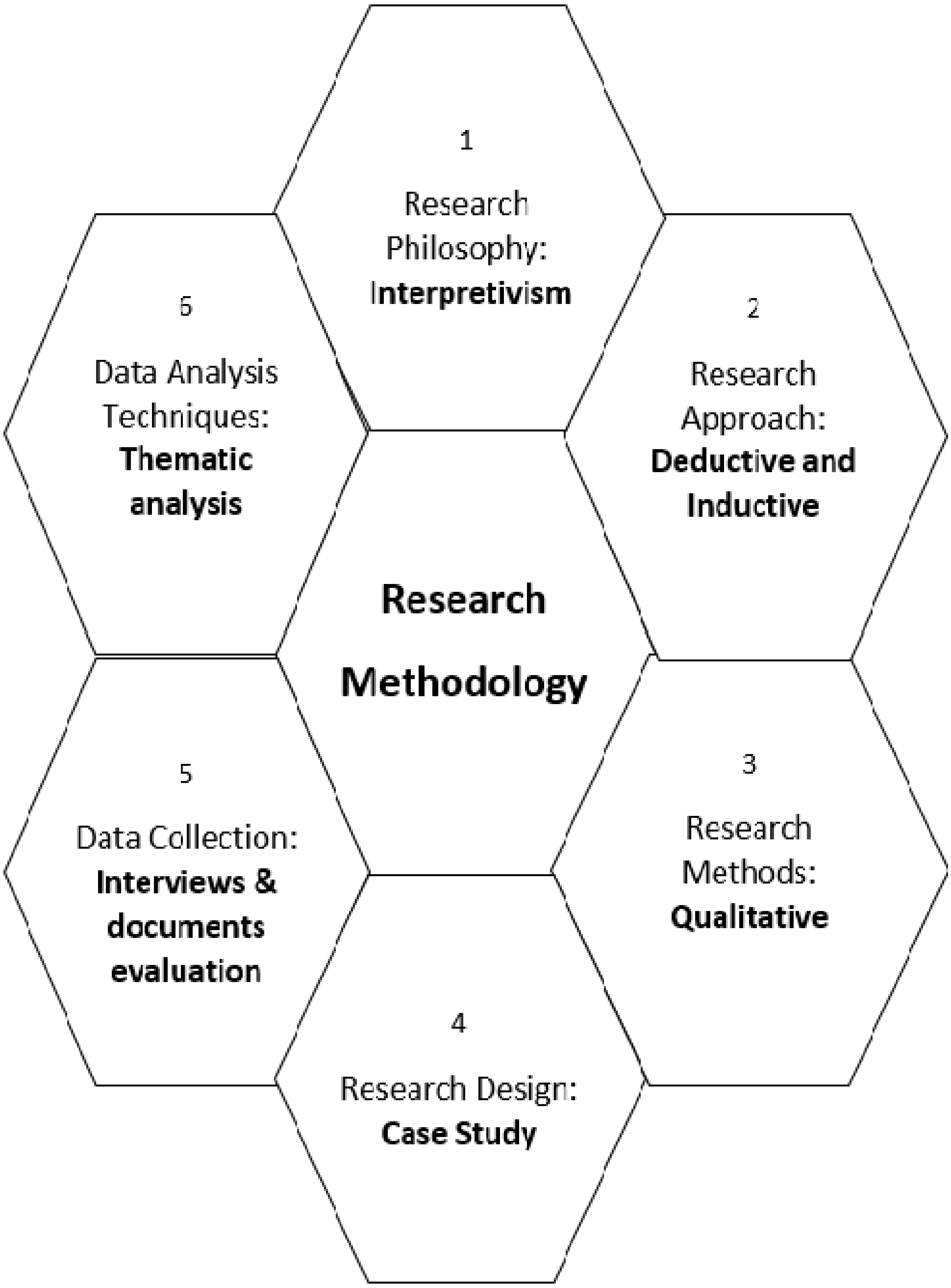
1
Research Philosophy: Interpretivism
2
Research Approach: Deductive and Inductive
3
Research Methods: Qualitative
4
Research Design: Case Study
5
Data Collection: Interviews & documents evaluation
6
Data Analysis Techniques: Thematic analysis
Research Methodology

Figure 3. 1 The Honey Comb of the Research Methodology (Wilson, 2014)

3.2 Research Philosophy

According to Easterby-Smith *et al*. (2013), research philosophy is important because it helps to choose the research design, the types of evidence required for research and the method of their collection. It also assists the researcher to recognise the subject constraints. Every academic research is guided by a set of beliefs, or paradigm, which is based on ontological and epistemological assumptions (Wilson, 2014).

3.2.1 Ontology

Ontology is concerned with the assumptions, researchers make about reality and the theoretical perspective they employ in their research. It is concerned with the research ideas about the relationships between people, society and the world (Eriksson and Kovalainen, 2015).

There are different ontological schools. According to the subjective school, the reality is based on perceptions and experiences, which differ from person to person and may vary over a period of time. From this perspective, the reality is multiple because it is observed through many individual points of views (Creswell and Poth, 2017). By contrast, objectivism assumes that the social world has an independent existence and is not affected by people and their actions. The present research is focused on the managerial practices implemented by peoples. These practices are based on the actions and experiences of individuals, which are grounded in transmission of information. Therefore, this study assumes reality as a contextual field of information, whereby individuals share and process information, related to certain contexts. Furthermore, the present study assumes that managerial practices are the reflections of the information process in IDFM context, so this research tries to analyse these practices.

3.2.2 Epistemology

Epistemology is related to the investigations of the nature of knowledge and customs of inquiring into the social and physical worlds (Easterby-Smith *et al.*, 2015). Epistemological assumptions within research relate to the understanding of the knowledge, the ways it is created and the methods to learn it (Ritchie *et al.*, 2014).

Epistemological assumptions within research relate to the understanding of the knowledge and the ways it is created. Much scholarly debate has surrounded the issue of whether social science can be studied in the same manner as the natural science is studied. Within business research, those who agree with applying scientific methods to business research tend to follow the positivist position, which "advocates the application of the methods of the natural sciences to the study of social reality" ((Bryman and Bell, 2015). Others oppose the replication of such methods to social processes because they believe that society cannot be investigated in the same way as nature. They advocate an interpretivist approach**.** Both approaches are discussed below.

a) Positivism

Positivism uses the scientific approach for investigations, which assumes reality as an objective construct and may not be affected by human actions ((Orlikowski and Baroudi, 1991). This paradigm is also used to investigate phenomena of a fixed relationship through a structured instrument. Additionally, positivism is more related to understand the process and actions without knowing the subjective information behind these processes and actions.

Positivism may not be an appropriate paradigm for this research as it would create a problem if respondents are considered as autonomous, which overlooks their capability to reflect on the problem and their reaction to it (Robinson, 2002). Further, under the positivism, principal data collection methods are the experiments and sample surveys, which are carried out while the researcher being remote (Christie *et al.*, 2000). Contrary to it, the aim of this research is to understand IDFM, analyse the managerial practices and suggest improvements, so scientific methods of inequity may not be workable to achieve the objectives of this study.

b) Interpretivism

Interpretivism refers that reality is determined by human actions and perceptions. It is also termed as 'social construction' or 'constructionism'. The concept of interpretivism is rooted in Hermeneutics and Phenomenology (Blaikie, 2007). Hermeneutics relates to the interpretation of the text and linking a meaning to that text (Delanty, 2005). The Phenomenology refers to the perceptions of the individuals for making sense of the world they live in, so it assumes reality as subjective, constructed by people (Bryman, 2015).

Interpretivism believes that access to reality is through social constructions such as language, consciousness, and shared meaning (Myers and Avison, 1997). Social constructionism believes that reality is determined by peoples, rather than objectives or external factors (Easterby-Smith *et al.*, 2015). Thus, the bases for determining the reality are the acquired information and experiences gained in the related contexts.

The interpretivism significantly differentiates between the research objectives of social and natural sciences. In natural sciences, the researcher develops some hypothesis and theories and tries to fix any of these with the phenomena under investigations. Contrarily, a social science researcher investigates phenomena to understand the social world, developed by the individuals through their perceptions and actions. This view of interpretivism rejects the objective reality and assumes reality as subjective and socially constructed by human actors.

The subject matter of this study is managerial practices within e-tail organisations in reaction to a new and developing contextual challenges. These managerial practices are based on the perceptions, knowledge and experiences of individuals within certain contexts. Peoples have different perceptions based on their experiences and various other factors. After all, this research is to understand IDFM and analyse managerial practices, which are based on the perceptions, knowledge and experiences of individuals in e-tail industry, so the scientific principles of knowing the reality might not help to attain the objectives of this research. Therefore, the philosophy of epistemology with interpretivism paradigm was the best choice to analyse the managerial practices in real world setting.

3.3 Selection of research methods

This research investigates reality as an ever-changing activity based on the transmission of information. In this reality human beings are constantly involved in interaction with their contexts on the basis of receiving, interpreting and acting on information they obtain through this interaction. Following this ontological outlook, this study investigates the informed opinions of managers regarding identity fraud management as an operational challenge, managerial response and reasons behind their actions and practices. Qualitative research suits these objectives best because it gives details of events and reasons of happenings (Bryman, 2013; Gray, 2013; Myers, 2013). Qualitative research explores answers to “how”, “why” and “what” aspects of problems and issues (Yin, 2014). This study seeks to highlight on what managerial practices are effective and why by investigating such practices in relation to real life settings. The qualitative strategy of data collection is the most appropriate for the purpose (Gray, 2013).

This project is undertaken in the area of study, which is new and under-researched. Thus, it is not limited to understand IDFM and existing managerial practices but also explore new ones at each stage of identity fraud management. The extant literature suggests that qualitative research is a good choice for an exploratory study like this (Myers, 2013).

Qualitative research methods are highly flexible; they allow a variety of research strategies and data collection methods (Gray, 2013). These strategies and data collection methods are detailed in next section.

3.4 Research strategy

The extant literature offers various research strategies including ethnography, grounded theory and case study (Boss *et al.*, 2015; Gonzalez and Tacorante, 2004; Mithas and Rust, 2016; Subramony, 2006). These research strategies and their relevance to the present study are discussed below.

3.4.1 Ethnography

Ethnography is a qualitative strategy of data collection in which the researcher tries to understand the shared values and patterns of a group (Creswell and Poth, 2017). It is based on extended time spent in the field, frequent interactions with community under study, building relationships with them and participating in community life, such observations and experiences are then transformed into a meaningful study (Cunliffe, 2010). Thus, the ethnographic method requires the researcher to become part of the group under study and collects data through direct experiences. Consequently, it is instrumental in investigating complex interactions and patterns within groups and societies. The key role of ethnography is to highlight visible working patterns of social behaviour of the groups under study.

Ethnographic studies avoid the early use of theories and concepts that may poorly fit with the participants' perceptions (Silverman, 2016). The primary source of data collection is the researcher's observation; therefore, it is also called as participant observation. It also includes interviews, symbols and some other sources (Atkinson, 2015). In ethnography, the researchers are is directly involved and become active observers, they should have knowledge on the shared culture and the values of the group under study.

Therefore, Ethnographic approach is appropriate for research on the shared cultures, values, and behaviour of the individuals. This research is not aimed at investigating the cultures or values of groups of individuals, rather it's focused to understand and analyse the managerial practices and management actions, so ethnography is not an appropriate strategy. Furthermore, direct observation is not possible because of limited access, privacy issues, and time constraints. Thus, it will not help to attain the objectives of the study. Finally, the results of an ethnographic study sometimes cannot be generalised from a few cases (Silverman, 2016) whereas, this study uses only three cases.

3.4.2 Grounded Theory

Grounded theory was suggested by two American philosophers, Barney Glaser and Anselm Strauss, in 1976. Grounded theory challenged the dominance of positivism using quantitative methods in social sciences. Since the qualitative methods were challenged to be an unsystematic and narrative, rather than theory generating (Denzin and Lincoln, 2011).The grounded theory rejects it and provides a comprehensive and systematic approach using qualitative data collection and analysis for theory development (Strauss and Corbin, 1990).

Grounded theory supports an inductive approach and suggests a theoretical explanation of the aspects of the research. These explanations should be grounded in the data and observation in a real world setting (Strauss and Corbin, 1990). Concepts are developed solely from primary data by systematically driving codes and themes. Grounded theory requires researchers to collect data in multiple steps using a zigzag approach to compare constantly the collected data with emerging themes for similarities and variations (Creswell and Poth, 2017).

Grounded theory may be the best option for a qualitative research when no previous theories exist explaining the phenomena, or very little is known about it (Creswell and Poth, 2017). Furthermore, it is limited to inductive approach for qualitative data analysis. However, this study extends the existing framework suggested by Wilhelm (2004). Additionally, the data was collected and analysed using the framework. Finally, grounded theory requires multiple data collection stages, so researcher needs to return continuously to the natural setting until data saturation stage is achieved, which is not possible, due to the limited access to the company, time constraints, and privacy issues. Hence, grounded theory may not be appropriate for this research.

3.4.3 Case Study

Case study is a practical inquiry to examine a contemporary phenomenon, (a case) in its real life setting (Yin, 2014). It is a widely used investigative strategy in business and information management. It is a comprehensive process for research, which offers customised case design, a variety of data collection methods, data analysis approaches and presentation of results in an appropriate way (Yin, 2011). The case study strategy has wide applicability in various disciplines such as psychology, sociology, economics, business, management, information management, information security, knowledge sharing, and many other fields.

Investigation based on the scrutiny of cases gives the researcher the advantage of examining phenomena in a real life situation. Research may involve a single case or multiple cases. In a single case situation, the data are collected from a set of respondents from one unit or organisation, while in multiple cases designs data are collected from sets belonging to two or more units or organisations. This characteristic of a multiple case design makes it particularly appropriate for the purpose of this research.

Online retail companies have adopted various managerial practices for identity fraud management. To analyse these practices with a view to improve them, a multiple case study research is the most appropriate method. The case study method also offers both deductive and inductive approaches as the foundation for data analysis, whereas, grounded theory supports the inductive approach only. Additionally, grounded theory supports theory building, while this research test existing fraud management practices in given context and extends the framework which is only possible through case study.

Adopting a case study approach also helps to carry out a close interaction with real world practitioners, which helps to create knowledge relevant to managerial aspects of the practices involved in IDFM. This provides an in depth understanding of organisational problems, culture and its psychology and clarifies management decisions by explaining why they were taken, how these decisions were carried out and what their outcomes were? (Stake, 2005).

Furthermore, case study offers a flexible and multifaceted strategy that provides the option to adopt the inductive or deductive approach, using qualitative or quantitative data collection method, interpretive and positive analytical approach and use of single or multiple cases at a time (Cavaye, 1996). Data triangulation is also possible in case study, because it relies on more than one source of data collection.

Additionally, prior theories and theoretical propositions can also be adopted in case study method to develop the research questionnaire and to get guidance on data collection and analysis (Yin, 2014). Benbasat and Zmud, (1999) has pointed out some advantages of doing case study research. Such as; it helps to analyse the phenomena in real world setting, use of multiple sources of data collection, option of a single and multiple cases, it supports the pre-adoption of a theory of propositions and also helps to develop a new theory.

Moreover, Cavaye, (1996) also advocates the case study method and affirms that it allows refining the existing theories, helps the researcher for in-depth understanding of the phenomena under study, and allows the researchers to understand the already discovered and newly discovered facets of the phenomena and multiple case study helps the researcher to relate the differences in various settings. Finally, the case study was a better option and the reasons for applying it are explained below.

a) It helps to investigate the phenomena in real world setting The case study method helped to investigate IDFM practices in real world setting. It also made possible to personally visit the staff involved in IDFM process, and investigate issues and problems in real setting. During the process staff was inquired of practical steps taken to manage IDFs in their respective organisations.

b) ***Multiple sources of data collection can be used*****:** Under the case study approach it was possible to collect data through multiple sources. In this study, in addition to the interviews, some documents were also collected in relation to IDFM. The case study approach also helped to collect some policy documents and see wall posters for communication of policies and promotion of IS culture.

c) ***Data triangulation is possible with multiple data sources:*** Data triangulation helps to verify the data collected through various sources, which is supported in case study method. Thus, it helped to verify some interview information with documents collected from the source person.

d) ***Case study offers option of a single and multiple cases:*** The single case study approach offers depth of the data, while multiple case study method offers in-depth and broader aspects of data to encompass maximum possible themes. Both the options were used as single case analysis for each firm were made to get deeper insight into the issue under investigation. The data collected through multiple case option were also compared to get meaningful insights into the variations among the case companies.. Such option is only offered by case study approach.

e) ***It supports the adoption of theories or theoretical assumptions for data collection:*** Adoption of a theory or theoretical assumption is significant to set the boundaries and focus on the issues under study. In the present research, fraud management framework was used as underpinning for data collection. It helped to cover comprehensive area of information for an effective IDFM.

f) ***It supports the exploratory, explanatory and descriptive types of research***. In this research new managerial practices were explored, the effectiveness of existing practices were explained with their impact of fraud management. The significance and impact of managerial practices were also described in detail. Thus, the case study approach helped to attain the objectives of this study.

g) ***A Case study helps in refining a theory or evolving it for further studies***. In this study, the framework was applied into a new context and further studies are also suggested. Thus, case study method supported to adopt an underpinning framework, extending in a new context and opening a new avenue for future research.

Although, case study is a comprehensive research approach (Merriam and Tisdell, 2015; Yin, 2014) with a number of advantages, it has two weaknesses in current context: lack of generalisability and lack of rigour.

The major concern is the methodological rigour, as often researchers fail to follow a systematic procedure (Yin, 2014). One of the possible reasons for such failure may be the availability of fewer research studies, covering the similar fashion (Yin, 2014). The lack of rigour is presumably less of an issue with other methods of research because of rich literature providing step-by-step guidance to researchers. Therefore, to ensure the methodological rigour for this research, the case study was fully designed, and methods of data collection, interview protocols, and analysis approaches and patterns are strictly followed and documented.

With regard to generalisability, the results of a single or a few cases are unlikely to be sufficiently comprehensive. However, similar to experimental outcomes, such results have value because they may expand and generalise theories (analytical generalisation), rather than infer probabilities (statistical generalisation) (Yin, 2014). Therefore, the present research tried to generalise the underpin framework in e-tail sector.

This research aims at understanding IDFM and analysing the managerial practices in e-tail organisations. That is only possible by investigating the phenomena in real world setting. A multiple case study approach helped to compare and contrast the data, which ultimately enabled the researcher to relate these variations in managerial practices. Therefore, case study was the best fit for attaining the objectives of this study.

3.5 Case Study Design

Yin (2014) describes the case study design as a logical system that connects empirical data to research's preliminary questions and finally to its conclusions. There are some critical components of a case research design, which include a case study's questions, propositions if any, units of analysis, the logic for linking the data to the propositions and criteria for interpreting the findings. Such component pertained to my research are discussed below.

3.5.1 Purpose of the Case Study

Case studies may be exploratory, explanatory and descriptive (Yin, (2014) depending on the objectives pursued by the investigator. This research is exploratory in nature. On the one hand, this study explores new insights into managerial practices in identity fraud management, thus analysing these practices for their effectiveness in current domain, which is not done yet. On the other hand, this study describes the real-world phenomenon of UK's e-tail sector in relation to IDFM. This study also provides insights on what managerial practices are adopted by the case organisations to manage IDFs.

3.5.2 Unit of Analysis

The unit of analysis (case) may be a person, a process, a program, a decision a group, organisation or anything to study. Following the aim and objectives of this study, online retail organisations have been selected as cases for this study. With multiple case study approach, three cases have been selected. A large number of research projects use 2-3 cases to study a business practice in depth (for example, (Palmberg, 2010; Schafermeyer *et al.*, 2010), while this research used three cases of UK e-tailors. Unlike the survey, organisations for study were selected for analytical generalisation, because, in multiple case study research, cases are not selected to be the representative of the whole but for the literal or theoretical replication (Yin, 2014).

For this study, cases were selected for similarities (literal replication) because with a few number of cases; these are to be selected for predicted similar results (Yin, 2014). The selection criteria for case organisation were: a) the organisation must be engaged in online retailing, b) must be based in UK and c) must be an independent organisation not a market place.

3.5.3 Validity and Reliability of the Research Design

Trustworthiness, credibility, conformability and data dependability of any study depends upon its research design. To judge the quality of a social research design, Yin (2014) and Wilson (2014) suggest four logical tests, construct validity, internal validity, external validity and reliability.

a) Validity

Validity in this research is limited to the generalizability of research findings beyond the immediate study. The generalizability is an important aspect of positivist approach that uses sampling, while case study research designs are not intended to generalise the findings (Wilson, 2014). On the other hand, Yin (2014) explains that unlike the survey, case study results cannot be statistically generalised. In this study, analytical generalisation is done, that is to generalise the application of the framework, and with three cases, replication logic is achieved by exploring the similarities in managerial practices for IDFM.

b) ***Reliability***

The reliability of a case study depends upon consistency and repeatability of research procedures used. The purpose of reliability is to make certain that, later if a researcher follows the same method as described by earlier researcher and conduct the same case study again, later researchers should achieve same findings and conclude same ideas. Yin (2014) suggests that for reliability, a researcher should document whole procedure of case study, by using case study protocol and developing case study database.

A case study protocol as suggested by Yin, (2014) has four important sections; first an overview of the case study, which relates to objectives of research, issues of case study and readings on topic under study. To attain first section objective, the overview of cases is given, and literature review chapter is evident for readings on topic under study. Second, data collection procedures, which include process for protecting human subjects, identification of data sources, and sources of data other than interviews. In this regards, identities of human subjects are kept undisclosed, selection criteria were developed for cases as data sources and documents are mentioned as other source of data. The third section is about data collection questions and sources of evidence, for which a questionnaire was developed and transcription of interviews are presented as evidence of data. Finally, for case study report, it is important to mention that the university's guidance for, thesis format, outlines, bibliography and other aspects are well incorporated in final thesis. Thus, reliability of this research is attained.

3.5.4 Sources of Data Collection

Yin (2014) discusses six sources of data in the case study: documentation, archival records, interviews, direct observation, participant-observation and physical artefacts. This research is aimed at understanding IDFM and analysing the managerial practices to suggest improvements, therefore the data were collected through interviews and documents (where possible).

The semi-structured interviews were helpful to enquire in-depth on what, why and how about real life situation and documents helped to know in detail about the policies and procedures on the issue under study. Such in depth inquiry on how and why about the adopted managerial practices is best offered by the semi-structured interviews. The interviews also helped in probing further on any matter either explored during the interview or already focused. Thus, interviews were more appropriate way to collect in depth data on managerial practices in IDFM. To some extent the documents also helped in data triangulation but these were offered by only one firm.

3.5.5 Development of the Questionnaire

Research questionnaire has a critical role in the collection of data appropriate to achieve the aim and objectives of this study. As already mentioned, IDFM consists of eight stages, so the questionnaire has the same parts.

The formation of questions is based on the stages of the framework. The framework has eight stages, so the questionnaire was also divided accordingly (see annexure 1). As already mentioned, semi-structured interviews were conducted, only basic questions were formulated according to the stages. These basic questions were to enquire what and how of each stage, while following questions were about the existing practices in the literature and developed from their responses. The questions related to the each stage were kept separate. At first, primary questions on what and how on the each stage of fraud management were designed. Mostly, these questions were based on the literature findings. Making the most of semi-structured interviews further in-depth questions were asked based on the answers of the respondents.

The verification and the validation of a research questionnaire is critical to justify its outcomes. For the verification of the questionnaire, it was dually checked by the supervisory team and also peer review was sought from senior PhD scholars in the related field to confirm the pre-construct and pre-content validity. The pre-construct and pre-content validities relate to the research questionnaire before seeking its validity through a pilot study (Colton and Covert, 2007). Furthermore, a pilot study was also conducted to confirm its content and construct validity. The questionnaire was refined as per the feedback from the supervisory team, peers and the pilot study.

Content validity refers to the logical link between the questions and the objectives of the study or the topic under study (Kumar, 2014). To ensure the content validity of the questionnaire, the related literature was thoroughly reviewed to include the factors leading to the management of IDFs. Additionally, the questionnaire was also reviewed by the supervisory team to ensure its validity as suggested by Colton and covert (2007).

To demonstrate the content validity of the research questionnaire, it has been divided into eight sections representing the each stage of IDFM.

Construct validity is related to the quality of research questionnaire to measure what it is supposed to (Kumar, 2014). Such validity is determined by confirming that each construct of the questionnaire contributes to the whole of variance in the phenomenon. The validity of the questionnaire was confirmed by including the questions related to all the stages of IDFM. For this purpose the questionnaire was divided into eight parts according to the number of stages in IDFM. Hence each part (construct) of the questionnaire contributes to the whole of IDFM (total variance). Thus, the construct validity was sought.

3.6 Pilot Study and Changes in Research Questionnaire

Before interviews in the case firms were arranged, a pilot was conducted to test the interview questions, data collection techniques, time management and data analysis methods. The research instrument (interview guide) was designed and developed on the basis of research objectives, stages of the selected framework and the literature findings. Potential respondents were purposely selected to have some knowledge on information security, online business and management.

Overall, for the pilot nine participants were contacted through email and personally. One of the participants did not responded the email, two other participants did not agree for an interview. Therefore, interviews were conducted with six participants. Five of them were postgraduate research students and one was taught course student. During the pilot study all protocols suggested by (Von Glinow *et al.*, 2002) were strictly followed, which included persuasion of participants, consent for the study and their selection based on their knowledge and experience in the relevant field. The study took six weeks to complete due to Christmas holidays.

The participants were fully informed about the project and the purpose of the interview. They were informed that such participations were voluntary and they were also informed about their right to quit the interview at any time. The time and venue was fixed with each respondent and then study studios in the university's central library were booked. All the interviews were conducted face-to-face. The participants were also asked to look at the research instrument for grammatical accuracy, repetition, clarity and sequence of the questions. The logic or the reasons of the questions were also discussed with the participants to confirm the required outcome of each question.

The feedback regarding repeated questions, grammatical mistakes, and complexity of questions was welcomed. The comments and feedback of participants were considered and suggestions were incorporated accordingly. In the light of their suggestions a few questions were removed and some were rephrased for clarity and grammatical accuracy. Furthermore, as all the interviews were conducted in semi-structured style, so some additional questions were also asked on the responses of the participants which were also added in final version of the questionnaire.

Moreover, various things were also noted which helped in real world case studies such as; interview timing and performance of recording tool in different circumstances. The minimum time of interview was 20 minutes and maximum time was 55 minutes. This will help to schedule interviews in real environment. The recording tool was tested through face-to-face interviews for the clarity of sound. The pilot study process also proved to be a training for better interview conduct. Listening of the interviews was helpful to realise unnecessary interception, and to learn tact to get more information through additional questions, which will make future interviews more effective.

Finally, two sample interviews were also transcribed with a view to improve the interviewer role, tone, speed and style of asking questions. This process enabled to improve the interviewer’s role, speed, tone, undue interception and additional questions development.

Although, the pilot study took some time but it helped to develop the final questionnaire and provided information about the utility and trustworthiness of the information produced. The pilot study was also helpful to confirm the construct and content validity of the questionnaire (Colton and Covert, 2007). As already mentioned, the respondents were students from the related field, their feedback on the interview questions was determinant for the acquisition of desired information.

3.7 Data Collection Methods

As mentioned earlier, a case study approach offers a variety of sources for data collection. Yin, (2014) mentions documentations, archival records, interviews, direct observations, participant observation and physical artefacts as major sources of data in case study method. This study used interviews and documentation (where possible) as sources of collecting data from cases. Detailed review of literature was also done for developing instrument and refining methodology of this research. The next section discusses in detail about sources of data collection for this study.

3.7.1 Interviews

As a method of data collection, the interview offers some unique characteristics, which other sources may fail to offer. To begin with, only the interview makes further probing possible, allowing to get deeper insights into the issues in fraud management and related managerial practices. Secondly, it provides a chance for the respondents to make their response rich with details. Finally, face-to-face communication also helps the respondents to understand the research objectives and remain focused on the issue. Face-to-face interviews also make it easier for the researcher to control the situation and keep the focus of respondents towards the asked questions. The semi-structured interviews have been proved to be a flexible tool delivering in-depth information without losing a consistent line of enquiry. The semi-structured interviews have helped the respondents to discuss important issues related to the context, and to show their personal attitude and views about the situation or context under study.

The interviewees were selected on the basis of their job description and position in the organisational hierarchy. Managers of different levels and employees involved with information technology, information security, human resources management, finance management and fraud management were selected for interviews. Direct, face-to-face interviews were conducted and recorded in a device for transcription to ensure validity and reliability of the study. Time and venue for interview was set at the convenience of interviewee. Duration for each interview remained between 40-60 minutes. The interviews remained open-ended and conversational manner yet case study protocol was followed closely. Total number of interviews were 33, which is a good number for a PhD thesis (Mason, 2010).

3.7.2 Documents

Documents contain a significant amount of information necessary to clarify the organisational process and managerial practices in identity fraud management. With this in mind, this researcher also collected some documents from a case organisation. Under the process, the key contact person was formally asked to provide the documents related to this study.

Only a small number of documents was received because of privacy and confidentiality issues. Most of the documents received were related to security policies and guidelines on some day-to-day business activities related to this research. These documents were helpful for in-depth and comparative analysis of the organisational practices in identity fraud management and related contexts. Some information was also taken from the organisational websites.

3.8 Selection of Case Firms and Participants

As already mentioned, the data was collected from three online retail organisations. It was observed that mostly the large firms have similar type of business process and online sales, which made it easy to select any large firm. All large e-tail firms in the UK have websites and mobile applications for online sales. It was also known that nearly all of the large e-tail firms offer their customer credit purchase without interest for a certain period of time. The customers are asked to open an account with these firms and some personal information is collected. Considering various situations, these firms offer varying credit limits to their customers. Similarities in business processes in large firms made the selection process easier.

The criteria for selection were set as follows: a) the organisation must be engaged in online retailing, b) must be based in UK and c) must be an independent organisation and not a market place, d) information security and identity frauds must be managed in house. These criteria helped to ensure that the chosen organisations would have an identity fraud management system**.** Three organisations were chosen for data collection. At the initial stage, these organisations were sent letters explaining the nature of the study, an interview questionnaire and a list of potential interviewees.

The organisations were also assured of the confidentiality of the respondents and the organisation. The organisations responded with the list of potential interviewees and their contact detail to arrange interviews with them. Afterwards, each individual respondent was contacted and interview schedule was fixed. All the interviews were conducted at the respondents’ offices at an agreed time. Table 3.1 presents the source of data collection and number of respondents.

Table 3. 1 List of the case organisations with the nature of their business and data collection sources

Code of the organisation	**Nature of the organisation**	**Sources of Data**	**Number of respondents**
Organisation1	Online retailer selling multi-brands with some physical stores	Interviews and internal documents	11
Organisation2	Online retailer with a chain of stores, selling many brands.	Interviews	16
Organisation3	Online retailer with a chain of stores, selling own brand.	Interviews	6

Table above presents the nature of the case organisation, sources used for data collection and the number of respondents. The detailed introduction of each case organisation and the results are presented in the following chapter.

3.8.1 Data Access

The potential respondents were approached through key people within the case organisations. The target respondents were fraud managers, fraud analysts, fraud advisors, fraud investigators, information security and data compliance managers, loss prevention and recovery managers, and managers from human resources and finance departments. The respondents belonged to various managerial levels.

Face-to-face interviews were conducted on a one to one basis at agreed time and venue. The consent forms, interviewer's CV, short summary of the project and list of job titles of the potential respondents were sent to the case organisations. An agreement on data privacy and protection was duly signed by the researcher and the representatives of the case organisations. Data protection act 1998 and the university's guidelines regarding privacy and data protection were also well understood to comply with.

3.8.2 Participant Selection and Theoretical Saturation

In the process of selection of the participants, the key person from each case firm was briefed about the project in order to get access on the appropriate participants. During that process the researcher was informed about the staff and their responsibilities working in the IDFM related area. Such information helped to obtain the appropriate participants.

Furthermore, the potential participants were finally selected on the bases of their role in relation to the project under study.

The number of participants does have a significant role to obtain sufficient data required for a research study. Bryman (2015), suggests that sample size in qualitative research should be appropriate to achieve theoretical saturation, which is not possible in a small sample, while a large sample size will make it difficult to undertake a deep case oriented analysis. Theoretical saturation is a point where additional data do not lead to emergent theme (Saunders *et al.*, 2018). In this study, the interviews were conducted with intervals, which provided the researcher sufficient time to transcribe and process the already collected data. Such practice helped to understand the level of the collected data and selection of further participants. So the practice of reading and processing the already collected data, helped to obtain further necessary data. Once theoretical saturation point was achieved (the data related to each of the stage of IDFM was obtained and further interviews were not adding a new information) the data collection process was assumed completed, so no further interviews were conducted. The variation in the number of participants at each case study is due to the achievement of theoretical saturation point at different levels (Kumar, 2014).

3.9 Qualitative Data Analysis Approach

The qualitative data analysis methods available to this research were content analysis and thematic analysis (Corbin and Strauss, 2008). Content analysis is a systematic approach for coding and categorising the data, it helps to determine the trends and patterns of words used in data set and to know the frequency of words, their relationships, structures and discourses of communication (Grbich, 2013; Pope et al., 2006). This approach is used mostly to describe the characteristics of the contents of documents and themes are developed based on the frequency of their occurrences (Bloor and Wood, 2006). Content analysis is a simple method for reporting common issues and problems mentioned in data. It offers possibility of quantifying the data along with qualitative analysis (Grbich, 2013).

Although, content analysis has some potential for being used in this study, there are some limitations to be considered. Firstly, the codes are developed on the bases of their frequency in the dataset, which may left some important but less mentioned codes. Secondly, the use of frequency technique is objective and concerned with surface meaning of the document, rather than hidden agenda or contextual meaning (Bloor and

Wood, 2006). Furthermore, content analysis is more suitable for the analysis of communications and the characteristics of the contents, whereas this study seeks to extract the managerial practices. Thus, the content analysis approach was deemed not flexible enough for the purpose of this study and restricted in its application.

By contrast, thematic analysis was found to be more appropriate for this study. Thematic analysis has a distinction from content analysis. As already mentioned, content analysis is based on the frequency of words, which limits its usability for this research. However, the thematic analysis provides for an in-depth data analysis for each theme. Thus, thematic analysis explores each theme irrespective of its frequency. It is an independent approach for identifying, analysing and reporting the patterns and themes within the qualitative data set. It is a flexible analytical tool, which provides a detailed and in-depth account of qualitative data (Braun and Clarke, 2006). Therefore, Vaismoradi*, et al*. (2013) suggest that qualitative researchers should be more familiar with this approach.

The aim of this study is to understand IDFM and analyse the managerial practice, which needs both manifest and latent content analysis in order to explore and describe the significance of the managerial practices. The analysis of manifest and latent contents of the qualitative data set is only possible in thematic analysis approach (Braun and Clarke, 2006). Therefore, this study used thematic analysis approach, which offered flexibility in developing themes by thoroughly reading and re-reading of the data set. The managerial practices could also be extracted through in-depth study of the data; such approach helps in exploring and analysing the managerial practices. Therefore, thematic analysis approach was a better choice for this study.

3.9.1 Data Analysis Process

As already mentioned, a thematic approach has been adopted to analyse the data set. This approach is based on the decisions regarding the identification of themes and richness of the data to support these themes. For identification of the themes in data set, inductive and deductive approaches were used, which are also termed as bottom-up or top-down.

There are no pre-determined rules for the identification of themes in the thematic approach, so such flexibility allows the researcher to identify the themes based on their significance in relation to the aim and objectives of the research. The flexibility in identifying the themes made it possible to set themes based on the theoretical framework using deductive (top-down) approach, and some themes were also developed from the empirical data through inductive (bottom-up) approach.

Under the deductive process of themes identification, this research relied on the fraud management lifecycle framework proposed by Wilhelm (2004). Nevertheless, the deductive approach helped in identifying themes from the data sate but it is limited to already existing themes. To overcome such limitation, the inductive approach was also used to identify those themes, which were not cropped in literature. Thus, both the approaches were used not to miss the important themes.

The data set of this study include 33 semi-structured interviews and some documents, from three online retailers based in the UK. At first, the codes were identified based on the themes mentioned in selected framework and literature discussed in chapter two. These codes reflect the first objective of this research, which is to explore existing managerial practices in fraud management at various business contexts. However, the novel managerial practices and emerging trends from the data set were also deduced. It reflects the second objective of this study, which is to analyse the managerial practices in case organisations. Use of the both approaches confirms that the data set is comprehensively covered to explore and analyse each managerial practice either already known or the novel ones.

Social research involves ideas and experiences with shared meaning within the context under study (Myers and Avison, 1997). Therefore, being a social researcher, the answers of the respondents were interpreted on the reflections of the aim and objectives of this research. The respondents were well informed about the aim and objectives of this research, before the interviews, so each answer was interpreted in the context under study, which reflects the shared meaning of the terms and practices. The quotations taken form the responses of the interviews are interpreted in accordance with the shared meaning of the terms and managerial practices reflecting the aim and objectives of this study.

The computer aided qualitative data analysis system (NVivo 10.0) was employed to assist with coding and developing themes from the dataset. The software helped to highlight and assign the managerial practices related to the each stage of the framework. At first, the primary nodes were developed in accordance with the underpinning framework stages. In the next phase, further sub-nodes were developed for individual managerial practices under each node. Then after the data was imported from the word files and were read and reread word by word with a view to not missing any theme.

During the readings, managerial practices were extracted and copied into the related nodes and sub-nodes. New sub-nodes were also developed to capture the novel managerial practices emerging from the data-set. Thus, all the managerial practices were extracted and were exported to word file for further analysis. After the initial coding, these were checked for duplication and similar texts in more than one code. Than after the data were segregated to represent every aspect of the data and a rich explanation of data-set (Grbich, 2013). Finally, the nodes, emerged themes and sub-themes were checked for any duplication and relevance with other codes at each stage of the framework. Thus, the managerial practices at each stage of the fraud management were identified.

3.10 Chapter Summary

So far, this chapter discussed the possible research methods and available options to attain the objectives of this study. It started with the introduction of possible research philosophies and the selected philosophy is justified for its significance in this research. In research strategy section, both qualitative and quantitative forms of data collection were discussed and the former was selected to be the promising approach to meet the objectives of this study. Ethnography, grounded theory and case study are the most common research designs. The uses of these research designs were discussed and the case study was selected as an appropriate design to attain the objectives of this study. The case study design section is a detail on the process adopted for the accomplishment of this research. Pilot study and update of the research questionnaire is also mentioned in this chapter. Afterwards, data collection methods and analysis approaches are mentioned and finally, the analysis process of this research is explained in detail. The results and the analysis of the data are mentioned in the next chapter.

CHAPTER 4
ANALYSIS OF THE RESULTS

4.1 Introduction

This chapter presents the analysis of the empirical results collected from the three large UK based e-tailers. First, the list of respondents is detailed with their job titles and area of responsibilities. The introduction of each case firm is presented at the start of the analysis of the results. The results are presented in accordance with the underpinning framework.

4.2 Case Organisations and Respondents

For data collection three large online UK based e-tailers were selected. These firms have significant arrangements in place for identity fraud management, including dedicated teams of employees. First, a list of large UK based online firms was prepared and then invitation letters were sent to the registered contact as stated on their websites. When these data were not available, emails invitations were sent to senior managers. As a result, only five positive responses were received, of which three were eventually selected for investigation. The following selection criteria were applied: a) the organisation must be engaged in online retailing, b) must be based in UK and c) must be an independent organisation and not a market place, d) information security and identity frauds must be managed in house. The characteristics of the selected organisations are presented below in Table 4.1.

Table 4. 1 Case firms staff, business channel, revenue and data sources

Firm	Staff	Methods of data collection	Business channels	Annual sale for 2016/17
C1	Over 5000	Semi structured Interviews, Policy documents and informal discussions	Online and telephonic	Over £1.5 bn.
C2	Over 25000	Semi structured Interviews, and informal discussions	Online, telephone, stores	Over £4 bn.
C3	Over 25000	Semi structured Interviews and informal discussions	Online, telephone and stores	Over £3 bn.

The selected organisations sell their own brands and many other brands. They all confirmed that they practice comprehensive fraud management activities. All three case organisations have separate teams to manage frauds. The list of respondents within each firm is given in Table 4.2.

Table 4. 2 The List of Respondents

Firm	R. No	Professional Field	Participant Role
C1	1	IT Security	Head of IT Security
	2		System Administrator
	3		Senior Security Analyst
	4	Group Security	Loss Prevention Manager
	5		Senior Security Consultant
	6		Investigation Officer
	7		Head of Group Security
	8	Fraud Prevention	Head of Fraud Prevention Team
	9		Fraud Advisor
	10		Fraud Advisor
	11		Fraud prevention manager
C2	12	IT Security	Director IT Security
	13		Operations Manager
	14		System Administrator
	15		Database Administrator
	16		Senior Technician
	17	Group Security	Head of Investigation Team
	18		Fraud Investigator
	19		Liaison Officer
	20		Fraud Investigator
	21	Fraud Prevention	Fraud Analyst
	22		Head of Fraud Prevention
	23		Fraud Analyst
	24		Fraud Risk Manager
	25	Business Operations	Manager E-Business
	26		Senior Manager operations
C3	27	IT Security	Head of IT Team
	28		System Administrator
	29	Fraud Prevention	Fraud Advisor
	30		Fraud Advisor
	31		Fraud Manager
	32	Group Security	Head of Group Security
	33		Fraud Investigator

Because each respondent had an assigned field of responsibility, it was not possible to get answers concerning each stage of the fraud management from every respondent. The case firms are coded as C1, C2 and C3, and respondents are coded as C1-R01……, C2-R02…. and so on. The results from each case study are presented individually below.

4.3 Case Organisation C1

Organisation C1 is one of the largest online retailers in the UK. It came into existence after a merger of two large rival businesses. It has a vast customer network throughout the UK and Ireland. More than 90% of its business is done online, yet it has some stores. It is a multi-brand online retailer. In addition to selling its own brands, it also deals with hundreds of other famous brands. C1 is a credit lending business, which offers its customers some interest free period when purchasing a product. Customers open accounts with the firm by providing personal information and they get login credentials to access their account in the future. The collected customer information is extremely sensitive as it includes the dates of birth, banking details and credit card details. The possession of customers' personal and financial information creates risk of IDT and fraud for the case firm.

4.3.1 Types of IDFs Faced by C1

The results obtained by this investigation reveal that IDF is a significant challenge for C1. It was established that the business was facing various types of IDFs, including application fraud, account takeover fraud, first party fraud and delivery fraud. It was also confirmed that most of these frauds are committed with stolen or fictitious identities, while first party frauds are based on the customer's false statement of not receiving any parcel.

The interviewees at C1 also confirmed that their firm faces the use of stolen identities, but they never knew how such information had been stolen, as they assumed the IDT occurred at the customer side. In spite of arrangements, some respondents mentioned that the firm was still losing significant amount of money to identity frauds. Furthermore, the results confirm that all the stages of fraud management are implemented by the case organisation. The results for managerial practices at C1 at each stage of IDFM are presented below.

4.3.2 Deterrence

Deterrence is related to stopping fraudsters before attempting any fraud (Leasure and Zhang, 2017; Shamsi *et al.*, 2016). The findings confirm that C1 has adopted some managerial practices focused on deterrence because effective deterrence results in saving future costs and other resources. In response to a question on the significance of deterrence, respondent C1-R01 stated:

"*So there is stake on both that if you can't stop it (fraud), the fraudsters try it again and again so more resource is being used all the times so it could get bigger"*.

It reveals that with every successful fraud, the chances of recurrences are multiplied. The statement establishes that the firm is aware of the importance of stopping frauds and one way of doing it is deterrence, so C1 has certain managerial practices to deter identity frauds. Deterrence is an anticipatory stage in identity fraud management that helps the organisation to minimise the potential fraud attempts (Jamieson *et al.*, 2007). For deterrence of identity frauds, C1 has some managerial practices related to the customer education and creating the fear of being caught and punished, which are mentioned below.

a) Customer Education

Educating the customers is an essential aspect of identity fraud deterrence (Sperdea *et al.*, 2011). According to respondent C1-R09:

"*We have advice and guidance, so we also provide customers by saying do not show your credentials, don't show your password, make sure it's a strong password, and ensure your password is changed on a periodic basis. All that kind of advice and guidance is also provided by the e-commerce site".*

This shows that the case organisation has a process in place of educating its customers. For this purpose the case organisation has adopted various practices. These include instructing them not to disclose their account credentials, to use a strong password and to change the passwords periodically. For customer education, the case organisation uses its website, and respondent also mentioned:

"*We do send out regular e-mails and reminders regarding ID theft or ID frauds, that you should change your passwords regularly for security point of view".*

Furthermore, the findings show that the e-tailer informs the customers regarding identity related frauds to enhance their awareness. Although, these practices help customer education, the persistence of these frauds indicates that some additional practices are required such as; advising customers to regularly check their bank account transactions, the credit file and not to share their personal information on social media (Seda, 2014; Arachchilage and Love, 2014). Also, Copes *et al*. (2010) propose that organisations should send specific messages to a targeted group of customers and victims. However, these practices are missing in C1. Adopting these recommendations may help improving customer education on IDFM. Therefore, the firm may be advised to improve its customer education by adopting the suggested practices.

The findings also reveal that C1 is using only a website and emails as instruments of customer education. In doing so they miss many other opportunities. The use of additional communication channels, such as text messages, push messages through a mobile app (McGee and Byington, 2015; Wright, 2007) and mass media (Bai and Chen, 2013) may help them to increase the impact of customer education. These channels have not been tested in e-tailing so far, which may be a deterrent for their use, but they have shown good results in other domains.

This study has also found out that customer education in C1 is limited to the matters of password protection and information sharing. However, the literature advises that customers should be educated on the trends and methods of identity theft and frauds, and measures to avoid such risks (Arachchilage and Love, 2014; Seda, 2014). Therefore, the case organisation may be advised to educate its customers about the emerging trends and methods of identity theft and related frauds to enhance their awareness, which would be more effective in prevention of IDT. In addition, the business may share with its customers, the knowledge about the practices and technological methods that help to minimise the risk of identity theft.

b) Creating Fear Among the Potential Fraudsters

According to the literature, fear has a critical impact on the behaviour of potential fraudsters, so it is a significant practice to create the fear of being caught and punished to deter identity fraudsters (Akers, 2013; Leasure and Zhang, 2017). To this end, C1 has the practice of publicising some information on successful prosecutions, as mentioned by respondent C1-R05:

"We do not name, but what we do in figures, 17 peoples prosecuted, 14 people arrested, this amount recovered".

Another interviewee (C1-R07) commented:

"*The deterrence that we as a group security department can apply is arrest and successful prosecution and highlight in the local papers, from where they were arrested".*

The statements show that the case organisation makes steps to create fear among the potential fraudsters by publicising news on arrests and prosecutions. At the same time, C1 does not publicise information on fraud attacks despite available recommendations, e.g., Shamsi *et al*. (2016), to make the public aware of attacks, the methods used, the origin of attack, including the identification of the fraudsters. As already mentioned, the publication of such information may create fear among the potential fraudsters, which may deter and de-motivate the fraudsters. In response to the question about the benefits of trying to stop potential fraudsters, respondent C1-R09 replied:

"*We know from past experiences, that if we don't stop them, they will come back every time".*

The above statements show that C1 works on fraud deterrence. The results establish that the case organisation only publicises the successful prosecutions and arrests, which is not enough to create fear. For creating fear among the potential fraudsters, Leasure and Zhang (2017) and Sperdea *et al*. (2011) suggest publicising more explicit messages regarding catching and punishing the fraudsters. Furthermore, the online organisations are suggested to make the potential fraudsters aware of the organisational arrangements and efforts on fraud management (Zadig and Tejay, 2010), which can deter the fraudster's behaviour on account of the alertness and countermeasures.

In addition to sending deterrent messages to an outsider, internal staff should also be informed (Workman and Gathegi, 2007). Finally, the channel of communication of the fear appeals by C1 is limited to the local newspaper, which may limit the impact of the arrangements, as the organisation works nationally, the full employment of mass media is suggested by Bai and Chen (2013), to maximise the impact of deterrence communication.

Moreover, the case organisation manages fraudulent deliveries in order to arrest the fraudsters with the help of police. For example, respondent C1-R01 explains:

Once you [the fraudster] *ordered that goods we believe if it is a fraud item what we then do we set up delivery, we know you are a fraudster we will attempt to deliver the goods for you. Once you signed for the goods, with the police help, we arrest the individual.*

The statement shows that the case organisation manages the fraudulent deliveries in order to catch the fraudsters red-handed. Such organisational practice creates fear amongst the fraudsters as told by the informant C1-R06:

"If you capture, if you arrest him [the fraudster] *and you see the trend stops, the volume of fraud in that area disappear very quickly because they know they're being watched"*.

The data shows that with every arrest the number of frauds coming from a particular area comes down very quickly. Arrest creates fear among fraudster and sends a message that the organisation has a watch over the fraudsters. Thus, the practice of catching the fraudsters under controlled delivery system has a significant impact on the creation of fear of being caught and punished, which leads to reduced number of fraud attempts. However, C1 does not publicise that it possesses systems that detect identity frauds in real time and catch the fraudster using managed deliveries, despite available recommendations, e.g. Zadig and Tajay (2010). Therefore, the case organisation should publicise that they are using advanced systems and managed delivery system to arrest the fraudsters with the help of local police. Such practices can increase the fear of being caught and punished among potential fraudsters and enhance deterrence of identity fraud.

4.3.3 Prevention

Prevention is a critical stage in identity fraud management. It helps the organisations to safeguard their information systems and avert any identity theft attempt, which may lead to identity frauds. Responding to a question about their prevention system, interviewee C1-R04 mentioned:

"*Obviously we are concerned as a company, and we've got to put in the right sort of prevention methods to stop identity theft happening to us".*

According to another respondent:

"There's a lot of upfront prevention techniques to stop identity theft attacks". (C1-R07)

The comments above illustrate that the case organisation has some technology to prevent any identity theft, which also confirms that C1 is working on the prevention stage of the fraud management. For prevention, the case organisation has adopted various methods and practices that are discussed below.

a) Sufficient Investments in Prevention Systems

The size of investment in the prevention system has a direct and significant impact on its effectiveness (Boyer, 2007). Regarding investments in fraud prevention systems, respondent C1-R04 informed:

"We do invest heavily into fraud prevention systems".

However, these investments may be limited to acquiring new technologies because findings indicate that the firm is still facing some security challenges resulting in fraud losses. Therefore, it may be deduced that the firm is significantly investing into technology, but more focus in needed on related issues, as suggested by interviewee C1-R05:

"More money and the availability of manpower, the more systems with IT security that are put in place, you find that it does prevent.

Above statement indicates understanding that for better prevention, investments in human resources to have experts in the field is also critical along with the technologies. It refers that for the effectiveness of technological system businesses should also invest into the human resources acquisition and development. Therefore, e-tailers may be advised to ensure the availability of experts in addition to the acquisition of sophisticated technologies, because only related experts can ensure the deployment of technologies in appropriate domain to get desired results.

b) Securing Customers' Information

The security of customers' information, especially their bank details and credit/debit card details, is critical for the business continuity and reputation. A single data breach or an identity theft occurrence may cost organisations millions of pounds and a huge reputational damage (Soomro *et al.*, 2016). Interviewee C1-R09 gave the following answer to the question "How do you secure customers' information?"

"So the internal network is protected all its entry and exit points via a number of managed firewall services".

These arrangements were also confirmed by respondents C1-R10 and C1-R07. The policy document D07 regarding the security of data during communication demands:

"All email and internet traffic must be virus checked, and any malware found should be removed or quarantined on detection".

Furthermore, for the safety of customer information, policy document D03 states:

"Data that requires encryption: Any confidential data that as stated in the data classification policy requires encrypting must adhere to this policy."

These results show that the case organisation has various measures in place to secure the customers' data at every step in communication and storage. Nevertheless, C1 has various arrangements to protect customers' data, it still suffers from IDF losses. One of the possible reasons may be IDT at the customer side, who are assumed as a weakest link in IDT (Da Veiga and Martins, 2015; Tøndel *et al.*, 2014). Therefore, in addition to having measures to secure customers' data at the business end, e-tailers should also educate their customers on methods of IDT and the countermeasures. Such practice of educating the customers on how to take technological measures to prevent identity theft is recommended by Arachchilage and Love (2014) and Seda (2014). Furthermore, customers may be offered free anti-virus software and other security software (Devos and Pipan, 2009). Such practice has already been adopted by banks.

c) Updating the Prevention System Regularly

Information technologies are evolving rapidly, so the prevention systems need to be updated regularly to prevent the identity fraud attempts effectively. According to C1-R10

"There's a business need that identifies sort of a gap or an item of technology which is out of date and obsolete. So we have lifecycle management for all of the systems……everything is patched to maintain its current levels, and full version upgrade happens periodically."

The statement shows that the case organisation identifies the need for technical systems or assess the need for upgrading the existing IT systems. Although, it may help in getting some sophisticated systems and upgrading of the existing ones, but technology is evolving at a pace. To get the benefits of evolving technologies the firm should keep an eye on the IT market for newer developments, as the need for these may not be realised through internal assessment. Additionally, C1 may also be advised to develop close coordination with the related IT industry to get tailored hardware and software, which can meet the firm's specific needs, related to the management of IDFs.

d) Having a Secure Authentication System

The authentication of the credentials is significant to prevent any identity fraud. The authentication system verifies login information with pre-stored data. Upon matching the information, the user is allowed for further processing (Usman and Shah, 2013). Regarding the authentication, respondent C1-R03 reported:

"We have standard authentication system, which is based on account ID and password".

Regarding the failure of the authentication system, participant C1-R06 commented:

"Mostly fraudsters hijack the customer accounts and ask for alternate address or a collection point, which makes fraud easy".

The statement shows that the case organisation has a standard account authentication procedure that requires the customer's account ID and a password. Respondents also confirmed that fraudsters mostly takeover the customer accounts by stealing their credentials and opt for a different delivery address than the one on the account, which makes the identity fraud easier to commit. This shows that standard authentication system may not work effectively, with stolen information and hijacked accounts.

The literature findings show that fraudsters steal login information and hijack the accounts, and alternate delivery or collection options make the frauds easier. The case organisation may be advised for a more robust authentication system (Prakash *et al.*, 2015; Sharma *et al.*, 2015). To make the authentication system more effective Mansfield-Devine (2013), Teh *et al*. (2016) and Usman and Shah, (2013) propose to use a bio-metric authentication system. This, however, may put extra financial burden on the firm. In addition, such a system can reduce the ease of online shopping.

Therefore, management of e-tailers should look for an improved authentication system that should have economic advantages without compromising the customer's comfort of online shopping. Furthermore, Bang *et al*. (2012), suggest sending customers one-time password on their registered contact, Kumar and Goyal (2016) and Wang *et al*. (2015) recommend sending login alerts to make authentication system more secure.

4.3.4 Detection

As already mentioned, detection is a process intended to identify the suspicious and fraudulent activities before, during or after the completion (Jamieson *et al.*, 2007; Wilhelm, 2004). Commenting on the significance of detection, participant R1-04 reported:

"It's more through the detection of frauds that you can gauge, how successful you are".

This indicates that the detection of identity frauds is a significant measure of the success of the organisational efforts against the frauds and confirms that detection is a critical stage in identity fraud management as other stages like mitigation, analysis, investigation and prosecution depend on it. Early detection of identity frauds also results in no loss to the organisations. Therefore, effective fraud detection is treated as a significant stage in identity fraud management.

a) Having a Fraud Screening System

Online business organisations process a large number of orders at one time, for which they need an automated screening system. The automated fraud screening system is based on fraud rules, which highlight any suspicious activity (Carneiro *et al.*, 2017; Dorfleitner and Jahnes, 2014). This view was echoed by participant C1-R04 as:

"So basically, the fraud rules decide whether or not the transaction looks suspicious. It then goes into what are called fraud cues".

Talking about this issue, another interview, C1-R01 said:

"We say that an individual who has been ordering goods say five years, soft goods, and at a sudden, he apply for expensive items, our systems flag it out".

Further to it, respondent C1-R05 told:

"They employ across all accounts, that identifies fraudulent activity or indeed orders which are oversize, over price and non-natural to that account.

These statements show that the case organisation has an automated screening system that identifies any suspicious orders. The system is based on fraud rules, which are pre-installed on the system. Based on these rules, the system flags out suspicious orders as frauds. The findings reveal that these fraud rules are based on the nature of the ordered items and cost of the goods. These rules are the parameters built into the order process system, which flags out every order for which these rules are prescribed. That is an effective system for online orders, as it processes every order in a real-time and detects any suspicious order for further verifications.

Although, the fraud screening system helps to detect suspicious fraudulent order based on parameters related to the online orders but the rules, conditions and parameters regarding identity frauds are missing in screening system. furthermore, the screening system reviews every order and detect suspicious or fraudulent activities, based on the pre-set fraud cues.

Nevertheless, identity fraud trends and methods are continuously changing over the time. In addition, screening system becomes ineffective with stolen identity information, because it depends upon the verification of order information, which is available in pre-exist dataset. For example, interviewee (C1-R05) mentioned that:

"With regard to response and reaction to any compromise on our customer's account, it would be very difficult to mitigate to zero fraud".

The statement shows that the detection system is not effective in detecting IDFs on compromised customers' accounts. Because the information used is accurate so detection system would not work. In this situation the firm may use additional checks on suspecious orders. Additionally, e-tailers may also adopt the practices of linking all the previously used customers' devices with their accounts (Al-Jumeily *et al.*, 2015), which is not being practiced currently.

b) Updating Fraud Rules

Methods and trends in IDFs are ever changing, so to detect emerging frauds, organisations need to update the fraud rules (Carneiro *et al.*, 2017). Talking about this issue, the interviewee C1-R11 said:

"If we then see a pattern, then obviously we can put that pattern in place, then will build a rule into the system that will then reject that type of activity

It confirms that the fraud screening patterns are updated in accordance with new fraud patterns. It also shows that new fraud rules are developed and implemented into the fraud screening system to detect that type of frauds. Thus, the practice of updating the screening system with new fraud rules helps the case organisation to detect fraud with matching patterns.

c) Having a Device Recognition System

The practice of having a device recognition system is significant to detect the recurring frauds. Such a system helps organisations to recognise the devices used by its customers or fraudsters. Regarding it, respondent C1-R02 informed:

"We've got the device recognition that we use, which we brought in a couple of years ago which is really a big deal, device recognition is because we can see who's using what computers and their IP addresses".

This shows that the device recognition system is an effective step towards the recognition of the customers' devices. The system also helps detection of devices previously used in frauds, as told by the interviewee C1-R03:

"Our (Device recognition) system helps to detect multiple applications or transactions using the same device".

The statement reveals that the device recognition system helps the case organisation to detect multiple applications or orders made through one device. Furthermore, on the significance of the device recognition system regarding the detection of recurring identity frauds, participant C1-R07 said:

"Our systems put cookies on the customers' devices, which detect the devices previously used in any fraud".

It suggests that the case organisation is using a device recognition system. First, it detects the use of the same device in more than one account. Second, the system also helps to detect any device, which has previously been used in fraud. Thus, it is significant in detecting identity frauds using the same device.

The results also show that the device recognition system installed by C1 can also identify the IP address of the customer or the fraudster. It is unique and identifiable and may be linked to each individual customer. However, the analysis reveals that C1 does not link customer devices with their accounts because customers may have access to different devices. Although, customers may not be limited to the use of one device, C1 may link all the used devices and IP addresses with customer accounts. Thus, any new devices may be confirmed through varius channels before processing the orders. Therefore, linking customers' devices with their accounts will also help to detect IDFs, which is also advised by Al-Jumeily, *et al*. (2015).

d) Receiving Customer Complaints on Identity Frauds

The interviews reveal that sometimes identity frauds are detected by the customers themselves. In this situation the case organisation receives complaints from the customers:

"Sometimes customers call and inform us that they haven't purchased this item, or I haven't spent that amount or things like that….". (C1-R10)

A similar response was given by some other respondents, indicating that the case organisation is still facing a significant number of identity fraud occurrences. The detection of identity frauds at the customer end may be a result of the customer education enticing to check their bank accounts and credit card transactions regularly. Although, it's a good practice to know on identity frauds, to start mitigation process, however, it also shows that the case organisation's arrangements to detect frauds may be improved.

For effective detection of IDFs, e-tailers may be suggested measures, such as Kumar and Goyal, (2016) and Wang *et al*. (2015) advised to send login alerts to the customers soon after their account is logged in. In case of any identity fraud, the customer will contact back. Thus, the fraud would be detected at the early stage. Therefore, case organisation should adopt the practice of sending login alerts to its customers through their preferred channel of communication.

4.3.5 Mitigation

Mitigation starts once a suspicious activity is detected in a customer's account during the proceeding stage. An effective mitigation system is necessary for a speedy termination of fraud attempts and keeping the fraud losses at a minimum (Jamieson *et al.*, 2007; Wilhelm, 2004).

The findings show that in spite of deterrence, prevention and detection, fraudsters succeed in committing IDFs. In this situation mitigation practices are necessary to keep the fraud losses minimum, as these losses cannot be fully tolerated. The respondent also informed that any fraud detected at an earlier stage would be mitigated to a zero loss. The processes and procedures regarding the mitigation of identity frauds in the case organisation are discussed below.

a) Verifying the Identity Information

The first and foremost practice against any identity fraud is the verification of identity information of the customers. Once an order is labelled as suspicious, the first thing the case organisation does is the verification of the identity information. According to C1-R04:

"We report all of our fraud onto CIFAS. So if you are a member that is another search tool that we use when an account is open, and an order is placed. We will check on CIFAS to see if there is a record on there of misuse of that address or that name is being used and stuff like that…."

The statement shows that the case organisation has the practice of verifying the address and the name of the customer through CIFAS database, to check if that ID information has already been used in fraud. This helps the case organisation to decide on the order whether, it is genuine or fraudulent. Furthermore, the case organisation also verifies the identity information when account is opened:

"*We use systems such as we would check BT people finder. straight forward; check if they are on the electoral roll. Check if they are on a mortality database if they are registered as deceased"* (C1-R07).

Talking about this issue, the interviewee C1-R03 said:

"Sometimes we do a credit file search. We can actually search a credit file, have a look at the data that's on there, and question the caller around the credit information".

The statements show that the case organisation has the practice of verifying the identity information at the time of a new account opening and in case of any suspicious transaction. As mentioned earlier, the case organisation shares identity fraud related information with CIFAS and get its help to check if any of the account identity has previously been used in a fraud. It helps C1 to reduce the identity fraud chances. Moreover, the findings also show that the case organisation also uses phone directories, electoral roll and mortality database to challenge identity fraudster before any fraud takes place (Jamieson *et al.*, 2007).

These verifications help the case organisation to mitigate any identity fraud before it happens. Although, these records help C1 to verify the identity information, there are some limitations related to these usability of these record. Thus, these records may not be updated frequently, fraudsters can use it as their advantage.

Next the information on the credit file may be actually logged by the fraudsters. To prevent this, the literature suggests collecting documentary proof such as driving licence, passport, etc. at the time of account opening, which will help to mitigate any fraud at that moment and the later stage (Kahn and Liñares-Zegarra, 2016).

b) Order Reconfirmation

Reconfirmation of suspicious order helps to ensure that the purchase order has been placed by a genuine customer. The case organisation has that practice in action, which helps it to mitigate any fraudulent attempt. In response to a question on reconfirmation of suspicious orders, respondent R1-C04 replied:

"They will manually do it, they will pick up a phone, and they will speak to the customers on the genuine customer's telephone number to confirm if the order is genuine".

Responding to the same question C1-R07 informed:

"There be certain queues that accept such as a high value based order which may be suspicious, such as a thousand-pound laptop goes into an address that has not ordered such item before and further checks may be needed to be done on that just to clarify and even if it is genuine."

The statements show that the red-flagged transactions are then manually verified by calling the actual customers via their already given contact numbers. This practice can mitigate the frauds, which are attempted with original but stolen identity information, as it will confirm the genuineness of the customer.

c) Sharing Information on Incurred Frauds

Sharing information with other organisations makes it easier to detect identity frauds in any organisation. Regarding the significance of information sharing respondent C1-R08 stated:

Information sharing is very beneficial because whatever frauds they have, we get the cross-reference in our systems

Above statement claims that information sharing on incurred frauds is helpful to detect identity frauds using identical information. Further to that, respondent C1-R04 told:

"We report all of our fraud onto CIFAS. So if you are a member that is another search tool that we use when an account is open, and an order is placed. We will check on CIFAS to see if there is a record on there of misuse of that address or that name is being used and stuff.

The results show that the case organisation has the practice of sharing the information on incurred identity frauds with CIFAS. Such information sharing practice helps the case organisation to detect any identity frauds with the credentials used previously with any other CIFAS member for committing a fraud. Thus, the practice of information sharing on the incurred frauds helps all the member organisations in detection of identity frauds.

d) Having a Victims Support System

In some instances, the identity frauds are unearthed by the customers when they check their business or bank accounts or credit card transactions. In such a situation the accounts show an activity, which has not been done by a genuine customer but a confirmed identity fraud. Soon after receiving the victim's complaint about an identity fraud, the case organisation tries to mitigate it. This is the response of C1-R05 to the question about how the form deals with the victim of identity frauds:

"The account will be secured and be given another account and loss will be given back to customer financially, and they will also be given above and beyond that as well as a mark of respect for letting them down".

The statement shows that the case organisation has a victim support system that helps them to continue their business with them. The results show that the amount involved in identity fraud is credited to the victim and a new account is assigned for onward business. This shows that the case organisation victim support system helps the customers avoid the loss, and continued business.

e) Mitigation Training

In identity fraud mitigation, training has a critical impact on the performance of employees responsible for mitigating identity frauds. This is recognised by the managers of C1. According to C1-R11:

"We take them [the trainees] *on to the systems to understand what an account looks like, what a customer's account looks like and what actually happens on the process of a customer, customer journey, and then to understand from initially opening an account, what information and what data we ask for so then how we use that data and how themselves can use that data to help them recognise".*

Similar views were expressed by interviewee C1-R07:

"*Fraud team obviously need more training than ourselves because the other ones are experts in initially spotting the frauds".*

The results show that the staff in the mitigation department is given training on customers' accounts and the related activities. They are also given training on the nature and the type of collectable information from the customers and how to use it successfully to mitigate any identity fraud. Furthermore, the training of mitigation staff should take into consideration the quality of their past decisions as advised by Becker *et al*. (2010). Such customised training would help mitigation staff to enhance their capabilities. Therefore, the case organisation may be recommended to customise the training programme for each staff member to improve their productivity in IDF mitigation.

f) Dealing with Compromised Customer Accounts

Identity frauds are mostly executed by taking over the victim's account. The case organisation deals differently with these accounts. In response to a question about how their organisation deals with an account associated with a confirmed fraud, respondent C1-R02 replied:

"We will just reject it, close it, and then, send a letter to the person whose name has been used to say 'Sorry we think you'd been a victim of fraud".

The statement shows that the case organisation has the practice of closing the accounts, which have been taken-over by identity fraudsters. Such practice, as mentioned by respondent, is adopted when no loss is reported on the account. Any account with incurred identity fraud is dealt differently as mentioned by respondent C1-R05:

"We will call it purpling the account, then we stop that account we give the customer another account to use continuously, but we keep this fraudulently obtained account opened so that we can catch the fraudster".

It is apparent that the case organisation deals differently with accounts involved in certain losses. Such practice of keeping the taken-over accounts opened to catch the fraudsters is helpful in mitigating the fraud losses through recovery. On the other hand, this practice helps in catching the fraudsters and prosecution. It leads to the fraudster being punished and recovery of losses. Such practice of keeping the taken over account opened to catch the fraudsters is critical to fraud deterrence.

4.3.6 Analysis

The analysis stage in IDFs helps to understand the fraud type, methods, trends and losses. It also determines the weaknesses of prevention and detection systems that result in fraud occurrence (Jamieson *et al.*, 2007; Kumar et al., 2007; Wilhelm, 2004). Furthermore, Wilhelm (2004) argues that fraud analysis reports help to develop and update fraud policies and also work as a base for further investigations and prosecution. The following results confirm that the analysis stage is a critical part of IDFM. Processes and managerial practices at analysis stage at case organisation are discussed as under.

a) Hiring Experienced Fraud Analysists

The job of identity fraud analyst is critical to the overall management of identity frauds. The skills and capabilities of a fraud analyst significantly affect the performance of identity fraud management. Therefore, a fraud analysist should be an expert in their field. Regarding the speciality of fraud analysts, respondent C1-R06 pointed out:

*“So these fraud analysts are either ex-military or ex-police, so they know how to deal, most of them have been ten years in police, so they know the business well”***.**

The statement highlights that the case organisation has a practice of hiring experienced professionals for effective fraud analysis. This helps the organisation to analyse the frauds in a better way, as the experienced professionals input their expertise and experiences. Although, the practice of hiring experienced fraud analysts has a positive impact on fraud analysis, Coulson-Thomas (2017) suggests organisations to involve top-level management to seek their input for the improvement of identity fraud management. Therefore, the case organisations in addition to employing expert analysts, should also involve senior management to get their input to make fraud management more effective.

b) Reviewing Identity Frauds

The practice of reviewing identity frauds is helpful in its management. The case organisation has the practice of reviewing each identity fraud reported by the detection team. According to interviewee CA-R08:

“We receive information pack on frauds to see the trends and methods of frauds, all related information, including the personal and delivery address…….what we do is to suggest the weakness of the system or staff negligence if any and fraud cues to detect similar frauds…”.

In turn, respondent C1-R05 stated:

“So wherever we find new trends that get communicated to everyone in specialised position”.

These statements indicate that the case organisation has the process of reviewing identity frauds, which help it to improve its fraud system. Information on identity frauds is sent by the mitigation team to analysisists, who review the information on frauds and diagnose the weaknesses in the functioning of the systems and staff. The analysis process also identifies new fraud trends and methods. Based on the review, these experts develop proposal on how to improve the systems; they also suggest fraud cues to embed into the fraud screening system to detect frauds in future.

As mentioned in the detection section, these fraud cues are significant to detect suspicious transactions. Thus, the process of identity fraud review is critical to enhancing the effectiveness of identity fraud detection.

c) Setting Identity Fraud as Management Priority

Putting identity fraud on the management priority list would help to get input from the top management. According to respondent C1-R05:

"We hold weekly meetings for IT security breach and internal frauds, this, therefore, highlights the existing cases and also highlights progress of existing prosecution and also highlight any new fraudulent activity".

In addition, the same respondent argued:

"It is important because on the executive board there is with CEO and COO they have weekly Monday morning meetings that identify any threat any major problems. That's two big risks in our business; one is through dishonesty and serious data breach that's discussed every Monday morning".

The results show that C1 has the practice of organising regular meetings to review the position on security risks and internal frauds. Such meetings are attended by senior staff from different fields in the business, thus it's a significant practice to get the input from related fields to develop a comprehensive programme to manage the IT security risks. This shows that identity frauds are not given much priority, and the results are evident that still, the case organisation is suffering from significant identity fraud losses. Therefore, the case organisation should priorities issues related to identity fraud management, which will ensure a better management of identity frauds, and is also suggested by Coulson-Thomas (2017).

d) Managing the Identity Fraud Risk

Identity fraud is one of the most significant business risks faced by online retail organisations. The risk is not limited to financial losses. There is also reputational damage, which may result in a complete business failure. The starting point in risk management is to know the potential risk as mentioned by respondent C1-R05:

"Fraudsters now know that they can get away with more success on online fraud and that's not to say that our systems are weak.... I never underestimate the intelligence of

any criminal because they make the decision to cross the invisible line and also take conviction, so never underestimate the fraudsters".

Confirming the fraud risks, respondent C1-R07 informed:

"Yes, we (are) still losing significant and lot of money on fraud, they still get in through".

The results also show that even after many arrangements, case organisation is still losing on identity frauds, which confirm the prevalence of fraud risks. Furthermore, the findings demonstrate that the case organisation is aware that its IT systems are always under attack, such sense of risk helps to take measures to manage these risks. Regarding the management of information security risk, respondent C1-R10 informed:

We have a security risk management function which, the name suggests, handles all operational and business-based, IT-based risks".

On the same issue, respondent C1-R05 stated:

"The business risk director, head of group security, head of IT security and head of fraud prevention, all work together, but ultimately it would be the business risk director responsibility to not only mitigate the risk but bring ideas how to reduce even further.

The statements show that the case organisation has the practice of managing the information security risk, which leads to the security the customers' information. The results reveal that the case organisation has the practice of risk analysis, but that practice is limited to the security of information regarding identity theft or information breach risk. So far, the case organisation is still facing identity frauds and is losing a significant amount of these frauds. Therefore, the organisation should focus on the potential risks at each stage of fraud management to improve its effectiveness (Wilhelm, 2004; Jamieson *et al.*, 2007).

e) Evaluation of the Prevention and Detection Systems

The performance evaluation of any system helps to improve its performance. Regarding the evaluation of technical systems, respondent C1-R09 stated:

"As health checking where we validate all of the control requirements defined in that policy against all systems within the environment and confirm any violations to that policy exist, and those violations are then fully investigated and ameliorated where possible".

And the other interviewee C1-R06) commented:

"We also have a vulnerability scan service which again, on a cyclic basis, runs on intervals".

The statements show that the case organisation has the practice of evaluating its prevention system to ensure its performance in the light of related policy. The policy document (D07) regarding the evaluation of prevention system states:

"Vulnerability Testing: All public facing services must be vulnerability tested at least bi-annually including but not limited to: E-Commerce website · Remote Access portals · Web services · Firewalls".

This shows that the case organisation has the policy of vulnerability testing of the website, access portals, web services and firewalls, twice a year. These are the interacting points, where the fraudsters and hackers attack to breach information or any other malicious attack. The test helps the organisation to evaluate the vulnerability of prevention and detection systems and take necessary actions to enhance their performance.

f) Performance Measurement of the Mitigation Staff

The importance of IDF detection system lies in the performance of fraud advisors, who deal with the suspicious frauds and go through various checks to confirm any fraud. So far, the performance measurement of mitigation staff is advised by (Becker *et al.*, 2010). As explained by interviewee C1-R04:

"We'll actually then evaluate that persons (fraud advisors) to see actually, have they achieved that competent level. If they achieved the competent level, that's fine. If they haven't, then we'll do what we call a personal development plan".

The statement shows that the case organisation has in place, the process of measuring the performance of fraud advisors, who are dealing with the suspicious frauds. It helps to ensure that the staff is performing at par to detect IDFs. This process also determines the training needs of individual staff members and making development plans. The results also show that these advisors are also sent for further training if their performance is not found satisfactory. Thus, the practice of the performance measurement of mitigation staff helps the organisation to enhance its effectiveness. Such process helps the case organisation improving the performance of mitigation staff, which leads to better IDFs detection.

4.3.7 Policy

A policy has a significant impact on practices and activities carried out within an organisation, so organisations should create and maintain antifraud policies (Njenga and Osiemo, 2013; Bierstaker *et al.*, 2006). On having policies, respondent C1-R05 informed:

"We even have group security investigation policy; we have an IT security policy, email security policy (and) internet security policy".

The statement shows that the case organisation is aware of the importance of policies. It has policies related to the security of IT infrastructure, information security, e-mail and internet security. The extant literature has many studies on the importance of policies for the effectiveness of the related operations. Regarding the importance of security policy, Puhamainen and Siponen (2010) and Siponen, *et al.* (2014) argue that the visibility of an information security policy has a significant and positive impact on the behaviour of staff to comply with the policy. The case organisation's practices on policy development, updating, and compliance are mentioned in following sections.

a) Having Identity Fraud Management Policies

The practice of having IDFM policies has a significant impact on its management. Respondents from the case organisation have confirmed the existence of a number of policies. Thus, respondent C1-R05 pointed out:

"Most definitely, we have an IT security policy, email security policy internet security policy".

In turn, respondent C1-R10 confirmed:

"There is a reasonably robust information security policy which defines a whole post of external security and system basically to control".

The statements show that the case organisation has some policies but are mostly related to the information security. Furthermore, the case organisations has developed policy documents which include Information Security Mobile Computing (D-01), Information Security Email Acceptable Use Policy (D-01), Information Security Encryption Policy (D-03), Information Security Network Security Policy (D-04), Information Security Incident Management Policy (D-05), Information Security Protecting Employee & Customer Data Policy (D-06) and Information Security Internet Acceptable Use Policy (D-07). These policies are aimed to secure the customer information from theft and breach at the prevention stage. However, similar policies at other stages of IDFM are not developed and implemented, which may be a reason for the occurrence of IDFs.

For effective management, the significance of policies has also been highlighted by Singh *et al*. (2013) and Soomro *et al.* (2016). Furthermore, regarding the effective management of frauds, some researchers (Jamieson *et al.*, 2007; Kumar et al., 2007; Njenga and Osiemo, 2013) have suggested having related policies. Therefore, the case organisation should develop policies related to each stage of the fraud management.

b) Data Access Management Policy

In addition to the arrangements for prevention of external threats, the case organisation also has the policy to protect critical information from internal threats. In this regards the case organisation has a data access management policy, through which the staff is permitted limited access to organisational and customers' data. Regarding the data access policy C1-R09 informed:

"We endeavour to operate the least privilege policy. So we are only granted the privileges which you require to conduct the activity associated with your job with your role".

Regarding the validation of such access and updating the access, the same respondent said the following:

"We have a process which runs six monthly, which is called 'continued business need' which extracts everyone's user ID on the privileges associated with those IDs and the individual's manager is contacted and asked to revalidate whether the access of the individual hold is still conformed to the role that they hold".

These statements reveal that the case organisation operates the policy of least privilege on data access, which is helpful to minimise the internal information theft. The practice of regularly updating the data access privilege is also critical to comply with the data access management policy. Nevertheless, the case organisation has a data access policy, however, it is re-implemented every six months, which may lease some risks, so the case organisation should change the access of staff once their roles are changed, without waiting for six months to be completed

c) *Policy Compliance*

Although, the practice of having IDFM policies is significant but worthless without compliance with these policies. Such compliance is a guarantee of the fulfilment of the purpose of the policy in question. This is what C1-R09 said about compliance:

"We validate all of the control requirements defined in that policy against all systems within the environment and confirm any violations of that policy exist, and those violations are then fully investigated".

In response to the question of how the firm ensures policy compliance respondent C1-R10 stated:

"We have a full compliance team with quite a lot of people, and they look at different areas of the business".

This shows that the case organisation has a practice of ensuring the compliance of every policy, investigate any violation and take corrective actions. The results also show that the case organisation has a devoted team to monitor policies compliance. Although, the case organisation monitors the compliance it does not provide any training on compliance methods and process. Such training is strongly advised by Soomro *et al*. (2016). The training helps the staff to understand the compliance methods and process, which leads to positive compliance behaviour. Therefore, the case organisation should develop a training programme to enhance the policy compliance.

d) *Compliance Audit*

The audit has a significant role in ensuring policies compliance. It helps to locate any non-compliance and those aspects of the compliance procedure which make the compliance easier. In response to a question on compliance audit, respondent C1-R06 replied:

"Audits take place in the business to make sure that they comply; internal audit team themselves they do on a regular bases, and third party comes in every year to make sure (that) we are complying with our policies.

On the compliance and audit, respondent C1-R05 pointed out:

"Each department has to succeed and has to provide evidence of their compliance, so we internally audit the compliance and we externally audit".

The statements show that the case organisation has the practice of internal and external audit to ensure compliance with its policies. However, it was also confirmed during the interviews that customer data is shared with some contractors and vendors, for which no such arrangement has been found. The customer data may be stolen or breached at these third party organisations. Therefore it is recommended that the case organisations should conduct an audit of third party organisations to ensure the similar policies on information security and identity frauds, which is also advised by Liu *et al*. (2010)

e) Policy Awareness

A policy lacks its importance if the staff is not aware of it. So the policies should be communicated properly, and staff should be well aware of these policies. Talking about policy awareness and ready access, respondent C1-R09 said the following:

"There are internal e-learning packages, which are deployed throughout the organisation so that it gives individuals an overview of the content of the policy and directs them to the full portion of document should they wish to read further".

The results show that the case organisation has made the policies available to each staff member, which help them to discharge their duties in accordance with the policy guidelines. Although, the availability of policies may help the staff to go through the contents of the policies, but, there is no sure that the staff will read and comprehend these policies, to act accordingly, which is a significant weakness in the policy awareness. So far, training programs should be arranged to enhance the employee awareness and comprehension on policies, which is also recommended by Parsons, *et al*. (2014), Singh, *et al*. (2013), Siponen, *et al*. (2014) and Soomro, *et al*. (2016).

f) Policy Update

The updating of any policy is necessary to coup with emerging challenges. According to C1-R05, in C1:

"Any policy is … reviewed every twelve month, and it can only be an active live policy".

The statement shows that the organisation has the practice of updating the policies on a yearly basis. Annual review of policies may not be effective in identity fraud management as the trends and methods of the frauds are ever-changing. Therefore, after having policies on identity fraud management, the case organisation should update its policies more frequently to counter the emerging changes.

4.3.8 Investigation

Investigation of identity frauds is a significant part of its management. It helps the organisations to collect the evidence, locate the fraudsters and litigate for the recovery of losses and punishment of fraudsters. The investigations in the case organisation are carried out by fraud prevention team. The investigation is a fundamental step towards prosecution, so, for effective prosecution, there should be a sound investigation and evidence preservation practices. This is what respondent C1-R05 had to say about identity fraud investigations:

"We are working towards minimising the police investigation and fraudulent house courts …that fraud is sold to an independent organisation they do on their behalf, we do not do, we investigate"

The statement shows that the case organisation has the practice of investigating identity frauds by itself. Investigating at the organisational end is a significant practice that minimises the police role, which enhances the coordination with police and help in better investigations and prosecution. Thus, the results show that investigation is a critical part of identity fraud management.

a) Employing Specialist Investigators

The effectiveness of investigations depends on the expertise of the investigators. The case organisation has employed a team of specialist investigators to conduct investigations on the organisational end. This is how the situation was described by respondent C1-R05 informed:

"It's not a role that is civilian and without police background, without HM customs and revenue, military background you can't train someone to be a fraud manager who wasn't at the experience for conducting investigations".

A similar statement was made by respondent C1-R09:

"There is a dedicated fraud investigator team which is comprised primarily of former enforcement operatives and ex-military officers who are able to go and further investigate and directly engage with law enforcement bodies throughout UK".

It follows that C1 has employed a team of expert investigators. These investigators have related background in the police, revenue and military. The first statement underscores that the role of investigators is critical and for being an expert investigator in identity frauds they should have vast experience in investigations.

The statements also show that investigators should have a sound knowledge of state laws and legal procedures and investigation experience. Therefore, the case organisation has employed specialists with a sound experience in investigations, state laws and legal procedures. With background specialities, these investigators should also have knowledge of the organisational specific systems to work with as argued by respondent C1-R04:

"So basically, the people that we employ, who come into my team have always got some sort of law enforcement background. So their knowledge of the law and how to deal with the police is already there…the bit that I have to train my team up on is the systems within the company.

It follows that the fraud investigators are well experienced in the field, but company-specific training is necessary to understand the systems within the case organisation. So far, the case organisation, after hiring these professionals trains them on the organisational specific systems. Such training helps them to understand the organisational process and technologies available to get help in investigations and collection of digital evidence.

b) Investigate with Prosecution in Mind

Investigation of the fraud cases is significant to find the facts/evidence and to locate the fraudsters. The case organisation has the practice of investigating the identity frauds for prosecutions, as mentioned by respondent C1-R05:

"It is in our nature to investigate and produce those papers to prosecute"

Also the respondent C1-R09 told that:

"We take the evidence; we present that in such a way that it's enough for prosecution".

The statements show that in the case organisation, identity frauds are investigated privately, and evidence is collected to prosecute the fraudsters. This evidence is then given to the police for further investigations and prosecution. Thus, all the evidence are collected and preserved to be useful for prosecution.

c) Collection of Evidence

Collection of evidence is a critical part of investigations to proceed with legal action to recover the losses and prosecute the fraudsters. Regarding the collection of evidence, respondent C1-R05 stated:

"Very first thing we do is gain as much information and evidence we possibly can, to ensure that the allegation is beyond reasonable doubt"

Similarly, C1-R06 described the firm's tactic in the following way:

"We will piece everything together; where the fraud took place, IP addresses, IPs link to anything, look at things such as device ID, so the cookies on the device has been using more than once, use social media, eBay, Facebook and tweeter trying to get a bit of profile of the person potentially involved, profile of delivery address, like student accommodation. Once we get it, we will build a package".

The statements show that the case organisation collects evidence and identity fraud related information to ensure that the allegation is beyond any doubt. For evidence, the investigators at the case organisation collect IP address, which helps to identify its links with any device, geo-position of the IP address and use cookies to identify the device used in frauds. Further findings show that the case organisation also uses social media to check the profile of the fraudsters, and information on the delivery address. After collecting evidence, the case is prepared for prosecution.

d) Reporting Fraud Cases to the Police

The legal action against fraudsters is not possible without reporting these cases to police. Such reporting is necessary for police investigations and their actions for the arrest of the fraudster and prosecution. Regarding the reporting of frauds to local police, respondent C1-R01 informed:

"We give the police statements and all the evidence ...: when the account was opened, how it was, by telephone or internet, IP addresses and all the information we can put together".

Respondents C1-R05 and C1-R06 had the following to add:

"We are working towards minimising the police investigation and fraudulent house courts".

"We do all the work for police so for the job for them we do everything so from the police force perspective it is an easy arrest".

The statements show that the case organisation reports the fraud cases to police with all available evidence collected by specialist investigators. The police are also given statements of the victims confirming an identity fraud, with account details, contact details, IP address and other related information. The findings also show that the conduct of investigations at the organisational end helps to minimise the burden of police investigations.

The results show that all these arrangements regarding the investigations and preparation of the fraud case makes it easier for the police to arrest the fraudster and process the case. Such process of providing the statements and evidence helps to increase coordination with the police as they sometimes lack interest in small financial frauds. Thus, reporting a fraud case with a ready set of evidence based on investigation, leaves least for police, which enhances the coordination between police and the business organisations. Therefore, this study suggests e-tailers to conduct investigation at their end, and collect as many as evidence to enhance collaboration with law enforcement agencies.

e) Catching the Fraudsters

After collecting sufficient evidence, the case organisation tries to catch the fraudsters with the help of police. If the fraud is confirmed before the delivery of goods, the organisation tries to catch the fraudster upon the delivery, as told by respondent C1-R01:

Once you [the fraudster] *ordered that goods we believe if it is a fraud item what we then do we set up delivery, we know you are a fraudster we will attempt to deliver the goods for you. Once you signed for the goods, with the police help, we arrest the individual.*

The statement shows that once the case organisation is confirmed by the transition being a fraud, then a controlled delivery is set up. The police are also involved in this process, and once the fraudster accepts and signs for the delivery, the police arrest him. Doing such delivery is significant in arresting the fraudsters and leads to a successful prosecution based on collected evidence.

4.3.9 Prosecution

An effective prosecution has multiple advantages, as it helps the organisation to recover the losses, builds customer trust, reduces the operational losses and disseminates a warning message to potential fraudsters. It also results in effective deterrence. The case organisation works on the prosecution stage of identity fraud management:

"Last year we took 435 people to court, and we got 415 prosecutions, very good success". (C1-R05)

"We prosecute on every single occasion, whether that is internal theft or customer's account is being fraudulent compromised". (C1-R02)

"*If they (the fraud managers) take it to the police and police wants to take it on we will prosecute definitely.* (C1-R07)

These statements reveal that the case organisation has the practice of prosecuting the identity fraudsters. The results also show that the decision of prosecuting any fraud is at the discretion of fraud managers. Once they decide to take the fraud onward for prosecution, they give it to the police, and they decide whether they want to prosecute or not. As already mentioned that the decision on whether to prosecute depends on the effectiveness of the investigations and the supporting evidence. Thus, this shows that all the fraud cases are not litigated but once the fraud managers decide to take any fraud to prosecution the next step is to prepare it in such a way that the police department is ready to take it for prosecution.

A) Involvemen in the Prosecution Process

For prosecution to be effective, e-tail organisations should be involved in the process to present their case and defend their position in the courts of law. Continued follow-up of the prosecution process is also necessary to attain the objectives of the prosecution. The management of C1 fully understands this as follows from the comment of respondent C1-R04:

"We follow it right the way through until they get sentenced, and hopefully we get compensation given back to us".

The statement shows that the case organisation has the practice of being involved in the prosecution process and defend their standing, which results in successful prosecution. The practice of following up the fraud cases in the courts of law also helps the organisations to make a claim for compensations. The fraudsters' punishment turns into a significant identity fraud deterrence, which is the first line of defence against any fraud. Secondly, prosecutions help the organisations to recover their losses, and build a sense of security for their legitimate customers. The practice of being involved in the prosecution process is also recommended by Lewis *et al*. (2014) and Gogolin and Jones (2010).

4.4 Case Organisation C2

Organisation C2 is a large online retail organisation based in the UK. It also has a chain of stores throughout the UK and the Ireland. It has millions of online customers. The firm deals in a wide range of items from household to jewellery. It sales famous national and international brands in addition to its own brands. C2 offers credit purchase to its customers for a limited period and also charges a fixed interest rate after free period. To get such facility, customers have to open account with it by providing personal, banking and credit card information. The account holders set some login credentials to access their accounts, and theft of these credentials result in IDF losses to the case organisations. On the other hand, C2 also has some risks related to IDT and data breach because of possessing sensitive customer information.

4.4.1 Types of Identity Frauds Faced by C2

The findings show that the case firm assumes IDFs as a critical challenge to the business that results in significant losses. Although, C2 has no mechanism to categories the frauds by types, yet the findings reveal that IDF is the leading fraud type in the organisation. The results show that application fraud, account takeover, first party fraud and delivery fraud are commonly found in C2. This e-tailer is losing a significant amount of money every year as fraud losses, so is engaged in online IDFM process. It has a devoted team that deals online fraud issues and liaisons with other organisations.

The results reveal that despite of the arrangements in place, the firm was still losing significant amount of its revenues to identity frauds. Additionally, the results also confirm that identity fraud management at the case organisation consists of the eight stages earlier mentioned in the literature.

4.4.2 Deterrence

Deterrence was identified as a critical part of IDFM in C2. Thus, regarding the significance of deterrence, respondent C2-R07 had the following to say:

"I also know that these amateur fraudsters are really not worth our time in dealing with because once they get a scare, they never do it again".

Another interviewee C2-R04 pointed out:

"We disrupt the frauds by carrying them out. By disrupting that network, we may see fraud dropped in that area by maybe 10 to 20 times a month".

The statements show that case organisation has the deterrence related practices, which lead to a reduced number of fraud attempts. The findings suggest that some amateur fraudsters can easily be deterred by scaring them. The case organisations also adopt various managerial practices to deter the fraudsters. As a result, the fraud attempts are declined significantly. For deterrence, the case organisation works on two aspects, customer education and creating the fear of being caught and punished. Managerial practices for customer education and creating the fear of being caught and punished are explained as under.

a) Customer Education

As already mentioned, customer education is a significant practice to make them aware of the risks and countermeasures to minimise these risks. The customer education is getting more importance on identity frauds as pointed out by respondent C2-R15:

"The risk patterns are changing, a few years ago our systems were more vulnerable to identity theft, which are still at risk but now customer is more vulnerable to identity theft".

The statement signifies the importance of customer education in identity fraud management. Observing the importance of customer education, the C2 educates its customers regarding identity theft, as interviewee C2-R09 reported:

"It is expressed on our website that beware of phishing emails and stuff like that….it suggests to protect password, periodically change it and set a strong one".

Other participant C2-R05 mentioned:

"We sometimes email our customers suggesting them periodically changing their passwords and not to disclose their ID and password to anyone".

The results confirm that C2 has the practice of educating its customers on IDFs. First, the case organisation uses its website to make them aware them of phishing emails and other information security risks. The website also suggests the customers secure their passwords from stealing, periodically changing them and putting strong passwords. The case organisation also sends emails educating customers on changing passwords and not sharing the passwords with anyone. Such customer education helps to secure the customer’s identity information, which is used for IDFs. In addition, for the education of victims of identity frauds, interviewee C2-R03 put it:

“We would ask our customer to keep checking your credit file just in case if your account has been compromised anywhere else or anything else from many other credit lenders”.

It reveals that educating the victims on checking their credit history regularly would help to detect further frauds with other organisations. Such managerial practice helps the customers to be vigilant on their credit record, thus any fraud may be identified earlier and it would be mitigated at an earlier stage, resulting in reduced losses.

Nevertheless, these practices help in customer education, the persistence of these frauds indicate that some additional practices are required. First, the case organisation should create awareness of new identity theft trends and IDF methods and countermeasures, which are also suggested by Arachchilage and love (2014) and Seda (2014).

Furthermore, C2 uses emails and website as instruments of customer education. The customer education may be improved by the use of some additional communication channels, such as text messages and push messages through mobile app (McGee and Byington, 2015; Wright, 2007)and mass media (Bai and Chen, 2013). These channels have not been tested in e-tailing so far, which may be deterrent for their use, but significant results have been achieved in other domains.

This study also established that customer education is limited to the password protection and changing it periodically. However, the literature advises to educate customer on methods of identity theft and frauds and measures to avoid such risks (Arachchilage and Love, 2014; Seda, 2014). Therefore, C2 may be advised to educate its customers about the emerging identity theft and fraud trends and methods and measures to counter to enhance their awareness for effective prevention of identity theft.

The results also show that the case organisation recommends IDF victims to check their credit history. However, the literature suggests that all customers should be advised to check their bank account(s), credit/debit card transactions and credit history regularly and not to share personal information on social media (Arachchilage and Love, 2014; Seda, 2014). Furthermore, organisations should also send customised messages to specific customers and IDF victims, which is advised by Copes, *et al*. (2010). Such practices would secure the customers' identity, help to detect frauds and create specific awareness in targeted customers/victims. Therefore, case organisation may be advised to improve its customer education by adopting the practices of suggesting the customers for regularly checking their bank details, credit/debit card transactions, credit history and send customised messages to targeted customers.

b) Creating Fear Among the Potential Fraudsters

The extant literature suggests that creating the fear of being caught and punished is significant to discourage fraudsters attempting frauds on any organisation. Regarding that participant C2-R02 mentioned:

"Actually we go out and deal with the fraud. So we will knock on your door. We will come with the police. You know that we will chase anything that we believe to be fraud. We will gather evidence, and we will prosecute them. So I think that sends out the best signal".

It reveals that after collecting sufficient evidence, the representatives of the case organisation visit the fraudsters' addresses with police to arrest and prosecute them. The results also show the dealing with the frauds in that way sends a warning message to the potential fraudsters.

According to C2-R01:

"The first thing is we try to organise what we call a controlled delivery. So with the police, our delivery company, and ourselves, we will deliver the parcel if even knowing that it is a fraud parcel, knowing that the person that is going to receive it is a fraudster. What we do is we will deliver the parcel, and once that parcel's been delivered and signed for, the police will then arrest the individual".

The statement shows that C2 arranges a controlled delivery if a fraud is confirmed. In this process, once the fraud has been confirmed, a team of representative from case organisation deliver the goods, and once it is signed the fraudster is arrested by police. The arrest of fraudsters creates fear among other fraudsters. Thus, fraud attempts are deterred.

Although, the fraudsters are arrested, which turns it into a deterrent activity, such arrests are not publicised. Responding to a question regarding publicising such information, interviewee C2-R01 replied:

"Well you see, that's the problem. You don't really want to. You don't really want society knowing that you have all this fraud. Because if they know, they may not do business with you".

The statement indicates that C2 does not publicise the information on arrests for creating the fear of being caught because it is assumed that such information will put a negative impact on the society and customer will refrain doing business with it.

The results confirm that the case firm is not publicising the information on arrests and prosecutions, which would not create the fear, among other fraudsters. The literature suggests publicising such information as it has a critical impact on fraud deterrence (Akers, 2013; DeAngelo and Charness, 2012; Leasure and Zhang, 2017).

Furthermore, Akers (2013) and Leasure and Zhang (2017) advise to create the fear of being caught and punished to deter the frauds. Additionally, publicising of information on fraud means and methods, origin and identity of fraudster's are also suggested as significant to create the fear of being caught and punished (Shamsi *et al.*, 2016). Additionally, Leasure and Zhang (2017) and Sperdea, *et al*. (2011) advise sending explicit messages to the society regarding the creation of fear and Zadig and Tejay (2010) suggests making potential fraudsters aware of organisational arrangements of frauds.

The creation of fear among the potential fraudsters and making them aware of the anti-fraud arrangements have a significant impact on fraud deterrence. Therefore, the case organisation may be advised to create fear through publicising the arrests and prosecution, and sending warning messages to potential fraudsters. The case firm may also publicise the detected frauds, their means and methods and identify the fraudsters and disseminate anti-fraud arrangements to make its identity fraud deterrence more effective.

4.4.3 Prevention

The extant literature has various studies on the significance of prevention as a critical stage in identity fraud management. It helps the organisation to fail any attempt at information theft, security breach and identity fraud. In identity fraud management domain, prevention stage works at the cyber frontiers of the organisation. Regarding the preventive measures, respondent C2-R09 stated:

"We are getting better at it, greater prevention systems we use now from our side".

The statement shows that the case organisation works on the prevention of identity frauds and is continuously improving the prevention systems. The need for effective systems to prevent information theft and identity frauds is also highlighted by Cordell, (2013) and Devos and Pipan (2009). On the risks related to information theft and identity frauds, interviewee C2-R07 gave the following comment:

"The reputational damage, the stock share, the effect on the stock market would be extremely, extremely serious. So again, there's another good incentive not just to protect the customer, to protect everyone, everyone involved including the suppliers".

Thus, the results confirm that C2 has prevention practices to manage IDFs, which is also advised by Jamieson, *et al*, (2007), Kumar, *et al*. (2007) and Wilhelm, (2004). The processes and managerial practices for prevention of information theft and IDFs in the case firm are discussed in the following sections.

a) Sufficient Investments in Prevention Systems

Sufficient financial investment has a critical role in making the prevention system effective. The case firm in reflections of its customers' expectations, invests sufficiently in its prevention systems. Regarding the customers' expectations and investment in prevention system, interviewee C2-R05 reported:

"If I was a customer, I would expect you to protect me to that level. I have to say that we do and invest in that".

Talking about this issue, respondent C2-R09 mentioned:

"I think if you see where we were five years ago to where we are now, there's a massive improvement in the fraud loss. So, every year we're getting better and better at actually stopping fraud, and that's possibly with the systems that we're getting in all the time, newer systems, we're being more proactive".

The statements indicate that the case organisation is investing into its prevention system to meet the customers' expectations for the protection of their data and safeguarding the information resources. The findings also show that the induction of sophisticated technology has a critical impact on prevention. The practice of investing sufficiently in prevention technologies enables the online organisations to have sophisticated systems, which can prevent identity theft and data breach attacks effectively.

b) *Having a Secure Authentication System*

A secure authentication system is a useful security layer to prevent fraudulent access to the customers' accounts. Authentication system helps the e-tailers to verify the login credentials of customers with their records, thus prevent any unauthorised access (Usman and Shah, 2013). In response to how do you prevent the fraudulent access to customers' accounts? Participant C2-R013 said:

"We have a username and password login criteria. So we are also looking for extra security with fingerprint [biometric login] *eventually in this year".*

This shows that at the moment C2 has a traditional user ID and password authentication system. It also reveals that the case firm is considering on developing fingerprint authentication system. Talking about this matter, interviewee C2-R10 argued:

"We as a security, get the best authentication to sign in, we are trying for two tiers of authentication, we test every sort of password sign in, different functions, different usability, and pin codes".

The statement reveals that C2 tests various types of passwords and pin codes for secure authentication. Two layered authentication system is also under consideration. The results show that biometric authentication system is also being considered to improve the authentication system. The current authentication system is not much efficient, so it may be improved by adding another layer of security, such as a memorable word or a pin code, which is commonly used by banks and some other organisations.

The literature findings reveal that the fraudsters steal account credentials and commit frauds, in this case, the traditional ID and password authentication fails to prevent the access. Therefore, the authentication system of e-tailers may be improved by sending login alerts to customers, as advised by Kumar & Goyal (2016) and Wang *et al*. (2015).

Sending login alerts to the customers' registered contact may help in detecting any unauthorised access in real time, which will not result in IDF occurrence.

Additionally, one-time password may also enhance the effectiveness of authentication system, which is suggested by Bang *et al*. (2012). One time password is sent to the registered contact once the customer credentials are verified, before allowing access to the account. It adds an extra security layer to authentication system with least chances of fraudster's access to it. Although, C2 is considering for biometric authentication, which is also advised by Mansfield-Devine (2013), Teh *et al*. (2016) and Usman and Shah (2013).

However, the literature suggests some limitations related to biometric authentication. These may include as once biometric information is stolen, it is difficult to recover, legal issues, and limitations while using a desktop computer. Therefore, the case organisation may consider all related issues, before implementing biometric or any other layer for better authentication system.

c) Securing Customers' Information

Protecting customers' information from internal and external threats is the responsibility of organisations (Prosch, 2009). It is also a key to the prevention of identity frauds. The breach of such protection, not only results in identity fraud but a huge reputational and financial loss and sanctions from the regulatory authorities (Soomro *et al.*, 2016). In response to the question on how your firm protects customers' information, participant C2-R13 replied:

"One of the other things we do is we run an encryption bureau service. So that data going to and from third parties are secure. We manage the email. We manage the web. …. [name of third party organisation] *manages our antivirus for us".*

Interviewee C2-R05 confirmed the above statement:

From protection of fraud-related incidents by use of the tablet and Android or indeed a mobile system is controlled by IT security of … [name of a third party organisation] *and a number of systems are employed in association with …* [name of a third party organisation] *to protect the customer and indeed the business from any form of hostile intrusion.*

These statements express that C2 is trying to protect customer information by implementing various in-house and third party arrangements. The results show that the case organisation uses encryption services to secure the customer information during the transaction period, its emails and website are also secured through antivirus provided by a third party organisation.

Furthermore, the results also confirm that the customer information coming from their mobile or tablets is secured from any security attack. And also the third party organisation manages the prevention system to safeguard the customer database and the case organisation against any hostile intrusion.

Although, the organisational arrangements may be satisfactory, but literature findings show that account credentials are stolen at the customer end, which is a weaker link in identity theft prevention, however business organisations bear the most losses in identity frauds. Therefore, e-tailers may be advised to educate their customers to create awareness on technological measures to prevent identity information, which is also advised by Arachchilage & Love (2014) and Seda (2014).

Furthermore, in the interest of business organisations, Devos and Pipan (2009) suggest offering customers free information security software. Although, it may put extra burden on the businesses, yet e-tailers should analyse the cost and benefits and if reasonable, such security services may be extended to some customers.

d) Updating the Prevention System Regularly

Technologies are evolving very rapidly. Hence, new methods of identity theft and frauds are emerging. So updating the prevention system is necessary to intact its effectiveness as attested by respondent C2-R12:

"We're always bringing in new tools, and updating our prevention systems and we're always looking at it for".

Talking about this, participant C2-R09 stated:

"Our prevention system is latest one as we always bring in new technologies".

The statements indicates that C2 is continuously updating its prevention system. The case firm brings emerging tools and technologies and replaces the obsolete ones. Such continuous update needs investments, for which the results already mentioned that the case organisation sufficiently invests in technologies. The results also indicate that C2 always looks for new technologies to update its prevention system. Thus, the management of C2 ensures a sophisticated system to prevent information theft and IDFs.

4.4.4 Detection

Managerial practices at this stage help to identify the suspicious and fraudulent transactions (Wilhelm, 2004; Jamieson *et al.*, 2007). This is the borderline for fraud detection, if suspicious fraud is not identified at this stage, will turn into occurred fraud. The results confirm that the case organisation also observes this stage in IDFM. For identity fraud detection the managerial practices of the case organisation are detailed as under.

a) Having a Fraud Screening Process

The screening process highlight suspicious frauds based on embedded anti-fraud rules. E-tailers process hundreds of online transactions at one time, so to detect any suspected fraud, having a fraud screening process is inevitable (Carneiro *et al.*, 2017; Dorfleitner and Jahnes, 2014). Talking about this, interviewee C2-R02 said:

"They have different rules, trigger points that they set the system to pick up [suspicious frauds] *and obviously, their workers in fraud prevention team, pick them up from the system, and then obviously deal with them as appropriate".*

This shows that the case firm has implemented a screening process, which flags out the suspicious frauds and these transactions are then manually verified by the staff members in accordance with the nature of suspiciousness. On the functioning of the screening process, participant C2-R03 mentioned:

"I've got a risk attached to them or just classes as high value; high products start, we know there's a trend for fraud ... So we work these cues, and they can refer due to the, they're going to click store, alternative address, a high-value order that we know is a trend that fraudster may order".

The statement reveals that C2 puts queries on the screening system based on the IDF risks, which include, high-value orders, new customer starting with costly items, collection options, and alternative delivery address. Based on these queries, the screening process flags out the suspicious frauds, which are then manually checked at mitigation stage. Such process also helps the e-tailer to set up queries based on the information from previous frauds, as declared by participant, C2-R14:

"Red flagging system of previously identified fraud is really important, and we use it a lot to detect frauds".

It reveals that the screening process is also a significant tool to detect the transactions that have any link with previous frauds. In addition, it also highlights new account applications. For example, interviewee C2-R14 informed:

"However, the application comes through; it goes through like a filter [screening] *system, and it needs to be checked by fraud analyst, then it's basically red flagged for us to check".*

This statement reveals that the screening process helps C2 to verify the identity information from various sources and to know the customers before starting any business with them. The effectiveness of screening process is based on anti-fraud rules, which are developed by the fraud managers based on the previous frauds, emerging trends high value orders and other parameters. In spite of having such a process, some frauds still go through it, as participant C2-R06 mentioned:

"So obviously, we can't detect all frauds because I know it's going to get through the systems. Because obviously, you're going to have, just in the system there's going to be new ways of like fraudsters getting our systems. But I'm sure some will get through until we detect them really".

It indicates that even having the fraud screening process, some fraudulent transactions still pass through it, which shows that still the process has some limitations. A possible, reason of its limitations may be the lack of focus on human aspects. This has also been advised by Vahadati and Yasini (2015) that expertise, skills and knowledge of fraud managers significantly affect the performance of the fraud detection systems. Therefore, C2 may be suggested to focus on the human aspects of fraud detection process to enhance their knowledge, skills and capabilities to increase the performance of identity fraud detection system.

b) Updating Anti-Fraud Rules

The effectiveness of the fraud screening process depends on the anti-fraud rules implemented in it. With the passage of time new patterns of IDFs are emerging, so to keep the effectiveness of the process intact, firms need to update anti-fraud rules continuously (Carneiro *et al.*, 2017). Regarding the update of anti-fraud rules, participant C2-R12 commented:

"We do change our processes constantly, as patterns of the fraud do change. So, for example, they could do something today and then change the way they do it tomorrow. So, we are constantly changing what we do to try and keep one step ahead".

This regular update of anti-fraud rules was also confirmed by interviewee C2-R04. Although, C2 is regularly updating its anti-fraud rules but the earlier section confirmed that still some frauds are not detected, which shows that there are still some issues related to updating anti-fraud rules. The results also confirm that these anti-fraud rules are based on previous fraud occurrences, which may not be effective on new fraud trends and involving information previously not known. Therefore, C2 may be advised for information sharing with other firms, to know emerging fraud trends and methods, well before any attempt, to update its screening rules. Furthermore, e-tailers may also be suggested to link customer devices with their account, which will help it to flag out any suspicious fraud initiated through the unregistered device, as suggested by Al-JUmeily, *et al*. (2015).

c) Receiving Customer Complaints on Identity Frauds

Sometimes IDFs are detected at the customer end, when they check their bank account, or credit card statements. Regarding customer complaints about IDFs, interviewee C2-R07 mentioned that

"Customers also call us and complain that they haven't bought this item or they haven't ordered anything from us".

It has been established that some frauds go through even when a mechanism for the detection of IDFs is engaged, causing customers to complain. At the time of customers' complaint the frauds are completed, so mitigation would not result in zero losses. In this case, C2 may be suggested to adopt real-time detection of IDFs through sending login alerts to respective customers, which is also advised by Kumar & Goyal (2016) and Wang *et al*. (2015). The practice of sending login alerts may help the case firm to let the customers know on their account access. Thus, any untheorized activity will be reported by the customer. In this way, any IDF will be detected in real time and mitigated as zero loss.

4.4.5 Mitigation

The literature findings show that mitigation is a critical stage in identity fraud management, as it helps to minimise the IDF losses as least as possible (Jamieson *et al.*, 2007; Wilhelm, 2004). On the mitigation process, interviewee C2-R08 said:

"We deal with that, once we've confirmed its fraud and we'd remove that from the genuine part's details. We do that here, is try to stop the delivery. If we felt there was an investigation needed, we'd send it to group security, and they could take a look at the address, possibly visit the address".

The statement confirms that C2 performs the mitigation activities. First, it tries to remove it from actual customer records to minimise its impact on the customer and stop the delivery if it is detected in real time. Furthermore, that case is sent to the group security department for additional investigations are needed. Thus, investigations are initiated, and sometimes the delivery address is also visited. The purpose of visiting the fraudster's address is to collect the evidence for prosecutions. Therefore, the results confirm that mitigation is a significant stage in IDFM that deals with minimising the fraud impact. The mitigation process starts with detection of suspicious fraud, the processes and practices at mitigation stage are explained as under.

a) Verifying the Identity Information

After detecting suspicious fraud, first, the case organisation has a process of verifying the customer identity information to confirm, whether it is a legitimate customer or a fraudster. For example, interviewee C2-R03 remarked:

"So we would then go in, check the account, use all the tools that we've got to check to device they use and what IP address that's come from, check if there's any links to the application and verify their information on the database that they are registered at the address, try and verify contact numbers that they've given".

Talking about the same process, participant C2-R12 informed:

"We use Equifax to make sure that person has given us the correct information. So, it's more around, yeah, the address, what device they're using, and obviously around the customer's credit data, if you will, which would be on a credit report".

These statements indicate that after detecting a suspected fraud, the case firm starts verifying the customers' identity information. For that device and IP address of the customer are verified with previously used, delivery address is verified with already registered address and contact numbers are also verified with previous records. Additionally, the credit history is also checked to verify the address and the credit history.

Furthermore, the case organisation also calls the customers for some verifications as mentioned by participant C2-R09:

"Again, that can verify details with the customer and sometimes when they ring, or we ring, we can ask them information from that credit file, so we might just ask them, "What's your mother's name?" Sometimes, a fraudster won't know your mother's name, they might not know your mother's date of birth, so we try and catch them out by using different questions".

Talking about the same matter, participant C2-R11 said:

"As I said, we'd ask them to confirm previous orders on the account. We'd ask them to confirm any previous payments, or returns, or…. Because if that fraudster had hacked into that account, they possibly wouldn't be able to see all that information. We'd ask them how long they've had the account".

This shows that C2 also calls the customers for identity verifications. The customers are asked to verify their details with their credit files, such as mother's name, date of birth, previous orders, payments and returns. The findings show that such verifications help to identify hijacked accounts as the fraudsters will also not be able to know the period that the account was opened at.

The results also show that the case organisation is using various sources to verify the customer's information. However, this can still be improved by using additional external sources of information. These external information sources include but not limited to, electoral rolls, telephone directories, and address finder, which are also suggested by Jamieson, *et al*. (2007). Furthermore, C2 may be suggested to collect, a copy of driving licence or passport as a documentary proof of identity, to make verification more effective, as suggested by Kahn and Charles (2016). Therefore, the case organisation is suggested to use external sources of identity verification and collect any documentary proof of customer identity for better verification of customer identity.

b) Order Reconfirmation

The reconfirming the suspected purchase order helps to determine, whether it was placed by the genuine customer or a fraudster. Regarding that, in response to the question, how do you reconfirm a suspicious order from customers? Respondent C2-R08 replied:

"Using our telephone or email with the applicant, we'd determine whether it was genuine or not".

Confirming the above statement, interviewee C2-R09 stated:

"We try and contact the customer before the order is cancelled".

These statements indicate that C2 reconfirms any suspicious orders through a phone call or an email. It helps the organisation to validate if the purchase order was placed by a genuine customer. The case is a commercial organisation,so any sales refusal would result in negative impact on the customers and its business. Furthermore, the results show that the case organisation tries to contact the customers on any suspicious orders before any purchase transaction is cancelled on account of being a fraud.

c) Sharing Information on Incurred Frauds

Sharing the information on incurred frauds helps e-tail organisations to detect any identity fraud well before it occurs. Regarding that, respondent C2-R05 told:

"We compiled a database of known fraudsters. We share that with other organisations and police constantly, constantly with many constabularies right throughout the United Kingdom".

Further to it, participant C2-R11 informed:

"We work with many other organisations such as online reporting, direct on National Crime Agency. We have an online reporting system whereby if we have transactions of over a certain amount; we will report that to the National Crime Agency".

These statements represent that C2 has developed a database of known fraudsters, which it shares with other business organisations and law enforcing agencies. The practice of sharing such information especially among the e-tail organisations help them to detect any identity fraud in advance.

Furthermore, sharing the fraud information with law enforcing agencies helps the organisations on broader aspects and help them to attract the attention of government agencies. In response, the law enforcement agencies may help the e-tail organisations in managing identity frauds and support for lawmaking on punishments on identity frauds.

d) Having a Victim Support System

Having a victim support system helps the business organisations to maintain a favourable customer relationship. Once an identity fraud is confirmed, the case organisation takes supportive measures to help the victimised customers. Regarding the victim support, interviewee C2-R11 mentioned:

"So, we would then give you (the customer) a brand new account number..... But we will then protect you (the customer) and register your details on CIFAS, which is UK's fraud database, so then you're protected as well".

As stated by participant C2-R12:

"We also ensure that we deal with the victim of identity theft by making sure it's removed from their credit report, and offering them onward support if they need it".

These statements describe that C2 has a victim support system. First, the victim is assigned a new account for continued business, which helps to retain the customer. Furthermore, the case organisation registers the victim information on CIFAS database, which would help to prevent any further fraud using the same identity information, within the member organisations.

Additionally, the case organisation removes the victim's information-as defaulter-from the credit file and offers any further support. Thus, these practices help the victims to reduce the fraud effects and retain the customers, which is critical for e-tail organisations.

e) Mitigation Training

The mitigation training has a significant impact on the performance improvement of fraud analysts regarding, decisions on confirmation of IDFs, and timely mitigation (Becker *et al.*, 2010; Wilhelm, 2004). Regarding mitigation training, participant C2-R08 informed:

"This shows us what to look for and what would be…and we've done training on that, to recognise that and then it'll enable us to determine whether it's fraud or not"?

The training help the staff to recognise the suspiciousness in any transaction and effective means and methods to verify information and take the right decision. The results show that the training programme is continuous in relation to the performance of the fraud analysts regarding their decisions on transactions being fraudulent or not. For which respondent C2-R14 stated in detail:

"You might carry out all the checks and all the systems all correctly, but the account still turns out to be fraud. So if there is thing like that where an adviser okayed the account but then it turns out to be fraud, that can be captured in like reports basically. Or if I said this account is fraud, I think its fraud and it turns out to be definitely fraud, we have all these different reports that the risk team could capture to say, "Yeah, that was the right decision this time. When you did this that was the wrong decision." And obviously with wrong decisions we'd follow things like training and coaching".

It reveals that C2 evaluates the decisions taken by the fraud advisors, regarding the suspicious transactions to be a fraud or not. The results also show that regular reports on the decisions of fraud advisors are released that show the right and wrong decision. Based on these reports, the fraud advisors are given the training to improve their performance in mitigating the frauds. Such training improves the quality of decisions regarding the mitigation of identity frauds and continued business with letting the legitimate transactions being processed onwards for despatch of goods.

Although, a continuous mitigation training is given to the fraud analysts, however, the results at detection stage show that still some frauds pass through the screening process.

Therefore, the case organisation may be suggested to extend the training programme to the staff working at other stages, to improve the effectiveness of IDFM as a whole.

f) Dealing with Compromised Customer Accounts

Once an identity fraud is detected through a compromised customer account, the case organisation has to deal with that. On a question, how do you deal a compromised account? Respondent C2-R09 replied:

"It's fully secured, and it's closed down, so no activity can take place on their [account] *and we make notes as well to clearly state that this account has actually been compromised. So, all notes are on there, it's closed down.*

The statement shows that the case organisation closes any account that is compromised. The closing down of a compromised account will help to stop any recurring fraud on that account. Thus, the results show that permanently closing down the compromised accounts effectively help the organisations to stop any further frauds on that account. However, C2 may use such accounts for arrest of fraudsters if they try to purchase any item. Such practices of arresting these fraudsters have multiple advantages in IDF deterrence.

4.4.6 Analysis

Analysis stage has significant value in identity fraud management on account of the variety of activities and their impact on other stages of the fraud management (Jamieson *et al.*, 2007; Wilhelm, 2004). The case organisation analyses the frauds trends and organisational arrangements to improve fraud management, for that, participant C2-R09 informed:

"The risk team will look at the fraud incurred, the loss, for the previous week. If it's high for any reason, they'll try and look for trends, is there anything that we could've done differently, so that's more from the risk point of view that they'll look into that to see what they can do to prevent it".

The statement indicates that the case organisation works on the fraud analysis, which helps it to know the fraud trends and take countermeasures to detect these types of frauds in future. So the primary focus of analysis is on the risk management and preventing identity frauds. Thus, the results confirm that analysis is a significant stage in IDFM. The process of the case organisation regarding IDF mitigation is presented as follow.

a) Managing the Identity Fraud Risk

The management of IDF risk helps the organisations to assess the risks associated with identity frauds and suggest measures to minimise these risks. Describing the identity theft risks, interviewee C2-R05 mentioned:

"I don't think that the criminal organised gangs behind this virus will target the household. I think they'll target many large organisations at hold of personal information and data, NHS [National Health Services], *hospitals, universities, the commercial online retailers".*

The statement reveals that C2 is aware of the potential risk of identity theft, as the criminals may target them. Such risks arise on existing of personal and financial data of a large number of customers. In addition to assessing information theft risk, the case organisation also evaluates IDF related risks, as mentioned by respondent C2-R02:

"I think that you're obviously going to miss a certain amount because fraud changes so much at different times. And if the fraudster thinks that you're on to them, they may change the pattern of how they're, you know, defrauding a company".

It confirms that C2 is aware that in spite of all the arrangements, there is still a risk of identity frauds. The earlier statements indicate that the case firm is more focused on website hack and information breach. Although, it would help to minimise the risks however, identity fraud risks are not given more attention so far, C2 fails to mitigate some identity frauds. Therefore, the case organisation may be suggested to focus more on IDF risks and develop countermeasures to minimise the ratio of successful frauds, and it should be a continuous process to update the IDFM systems in time.

b) Reviewing Identity Frauds

The process of reviewing identity frauds helps to update the systems and enhance their effectiveness in IDFM. Regarding the review process, interviewee C2-R05 said:

"We'll also look at the amount that we lost in a fraudulent or hostile attack. We will review the frauds, types methods..... We have to ensure that we review and record a

minute all the levels of protection that are invested upon to prevent the business from frauds".

Talking about the same, participant C2-R11 told:

"Once we find any fraud trend and pattern, then what they are doing, then our risk team will change our systems so that certain orders or certain types of referrals are developed".

These statements indicate that C2 reviews identity frauds to know the trends and methods and incurred losses. Based on such reviews, the case organisation updates are security systems. New fraud cues are suggested, and existing ones are updated to counter the new identified methods and trends of IDFs. The feedback on fraud reviews helps the case firm to improve its detection system by putting some more filters and updating the existing ones. Thus, the process of reviewing identity frauds helps in updating the fraud systems to enhance their performance.

c) *Setting Identity Fraud as Management Priority*

The involvement of top management is already suggested in the literature, to enhance the effectiveness of fraud management (Coulson-Thomas, 2017). Regarding that, respondent C2-R14 informed:

"Very senior level [is] *being given the information on a regular basis. How many hits, how many deters, how many loses, what is our good lost in transit, you know that, what is our debt record, and how are we managing the debt. All these things are regularly reviewed by the risk assessment team".*

Such practice would help to get more attention from senior executives for effective IDFM. These meetings are significant to enhance the effectiveness of identity fraud management through reviewing the existing identity fraud situation and managerial practices in action. The results show that top level management is not directly involved in the management of identity frauds, and they are given just the reposts on these frauds. The results also show that the case organisation is losing on identity frauds, which shows that these frauds need to be a management priority, which may lead to a better management of identity frauds.

d) Evaluation of the Prevention and Detection Systems

The efficiency and the effectiveness of preventive and detection systems are significant to manage IDFs. Regarding the evaluation of these systems, interviewee C2-R13 explained:

"We get an independent third-party *to come in and we ask them to, you know, effectively try and hack the website. So we're asking them to look for vulnerabilities. So the normal method is that they will run an automated scan, which will identify potential areas of vulnerabilities. And they will then handcraft attacks to see, whether those vulnerabilities are real or whether they're just false positives. So that tends to be how they are done. I've used a variety of firms to do those assessments".*

Talking about the same issue, participant C2-R04 mentioned:

"So that is the risk assessment, and vulnerability test and strategic assessment that we do on a regular basis".

The statements represent that C2 is actively evaluating its prevention system. For that, the services of an independent firm are hired to assess the vulnerabilities of these systems. Furthermore, these vulnerabilities are also checked through handcraft attacks. The system is not evaluated by the same organisation every time as to minimise the weaknesses related to any firm. These evaluations are done on a regular basis to keep the prevention system intact. Although, the prevention system is being evaluated in the case organisation, but, IDF detection system is not, which may leave several risks associated with it, and a possible reason for successful IDFs. The screening system is critical to detect identity frauds. Therefore, the case may be suggested to adopt the measures for the evaluation of detection system to enhance its performance, which is also advised by Wilhelm (2004).

e) Learning New Fraud Trends

Learning the new and emerging fraud trends significantly helps the organisations to take a better position to encounter these frauds. Talking on learning of new frauds, interviewee C2-R14 pointed out:

"So if an adviser gets a certain trend from a certain work type ………and we can feed that information back to our risk team to say we've had this trend. It could be from anywhere……. We can get that kind of information from absolutely any kind of source. Even things like things watched in the news…..".

This statement indicates that C2 is active in learning on fraud trends and methods. The fraud advisors actively seek to learn on new identity frauds from the inside organisation and outside, such as customer, any report, a friend outside the organisations, third party customer services, news and any other sources. Such learning on identity frauds is much helpful to develop countermeasures before any of these trends are applied to the case organisation. Based on this information, the risk team develops or make changes to the existing fraud cues to detect emerging frauds. The case firm communicates these fraud trends and methods through email, as stated by respondent C2-R08:

"Well, we get emailed new frauds. That's emailed daily. The fraudulent areas, things like that".

It reveals that C2, after learning on new fraud trends and methods communicates to related staff members. Such information is communicated on a daily basis and is much helpful to get ahead of the fraudsters, as the risk team take measures to encounter these fraud trends by developing new fraud cues and embedding into the screening system to detect such frauds.

4.4.7 Policy

The policy is a set of guidelines to perform day-to-day business activities. Organisations should create and maintain effective anti-fraud policies to guide the staff (Njenga and Osiemo, 2013). While asked about the fraud policies, respondent C2-R12 informed:

"Our policies are a lot around about how we use our systems which is in our process document".

It indicates that the case organisation has a number of policies but mainly these policies are focused on the operations of the systems. Regarding the responsibilities of developing the policies, respondent C2-R01 maintained:

"So each individual area of the business has responsibility for their area's policies and procedures".

The results indicate that C2 has policies related to various systems and are developed by the respective business area. Identity fraud management related policies and procedures are discussed as under.

a) Having Fraud Management Policies

Anti-fraud policies are critical to managing the identity frauds in any organisation effectively. These policies help firms for effective and uniform actions in IDFM. In response to a question on, whether they have identity fraud management policies, respondent C2-R14 informed:

"We have a lot of different policies but not specifically for identity theft. Obviously, we have information security policies and .... but not just an identity theft policy or a fraud prevention policy".

Answering the same question, respondent C2-R02 mentioned:

"There's money laundering policies, but as for the initial fraud policies, we don't have…They may be available on the fraud intranet, but we don't have them".

Furthermore, respondent C2-R13 informed of the policies:

"There isn't a specific e-commerce security policy now".

Although, these policies may somewhat help in identity theft prevention, however, the management of identity frauds is a broader field, for which the results show no policy. The absence of such policies is a critical weakness, which may result in inappropriate practices for effective management of identity frauds. Furthermore, in the absence of fraud management policies, the staff works in isolation and uncertain conditions to deal with any fraud related issue.

The significance of related policies to effectively manage the issues has also been highlighted by Singh *et al*. (2013) and Soomro, *et al*. (2016). Furthermore, on effective management of frauds, many researchers such as; Jamieson *et al*. (2007), Kumar *et al*. (2007), Liu, *et al*, (2010), Njenga and Osiemo (2013) and Wilhelm, (2004) have emphasised the existence of related policies. Therefore, e-tailers may be suggested to develop policies at each stage of IDFM.

b) Policy Awareness

Creation of policy awareness among the staff members is critical to achieving its objectives (Soomro *et al.*, 2016; Parsons *et al.*, 2014). Regarding that respondent C2-R01 told:

"All policies are made available on our internal communication system, so anyone can access the policies".

Although, it's a good practice to make the policies available, however, it may not assure that all the staff members understand these policies. Therefore the case organisation should develop some policy awareness training programs and employee's evaluation to ensure that the staff is well aware of existing policies. Such awareness training is also recommended by Albrechtsen and Hovden (2010), Parsons *et al*. (2014) and Soomro *et al*. (2016) in information security context. Further on the awareness of any policy update, respondent C2-R12 told:

"Any update in policy is communicated to the staff through emails".

Nevertheless, email is an efficient way to communicate any information but, policy updates require that the staff should fully understand the changes, for which the case organisation has no system. Therefore, C2 may be advised to get feedback from the staff, that they understood the changes (Bierstaker *et al.*, 2006), and similar arrangements of policy awareness may also be made as discussed earlier.

c) Data Access Management Policy

Data access management policy is helpful in minimising the customers' information theft from insiders. Readily available customers' information to non-concerned staff increases the chances of the theft. In response to a question on data access policy, respondent C2-R13 informed:

"Well, access to customer data is only permitted to people, who are authorised and have demonstrated need in their job to have access to that customer data. ...people who have

access to that data should acknowledge to abide by the Data Protection Act, et cetera, et cetera".

It indicates that the access to data is linked to the nature of the job, if a job requires specific information, only related data access is given to staff to fulfil their jobs. Furthermore, the results show that anyone at access of customer information has to abide by the data protection act and other related laws. However, the literature suggests that organisations should have the system to monitor and keep the record of who accessed what information. Such system may help e-tailers to stop any unnecessary and unauthorised access to identity information, which is also suggested by Alrashed, (2016). Furthermore, data access may be re-evaluated on a regular basis, to keep it updated with changing roles of employees.

d) Policy Compliance

Policy compliance is critically important to attain the objectives of developing the policies (Chen *et al.*, 2015). An effective compliance with anti-fraud policies can ensure the achievement of organisational goals on IDFM. Regarding the policy compliance at the case organisation, interviewee C2-R05 told:

"I can say that the business, its compliance is quite simple. They will always operate above and beyond compliance as best practices".

It reveals that in C2, staff is expected to comply with policies and adopt the best practices. However, the results show that the case organisation has no system for monitoring the policy compliance. Compliance monitoring helps the organisation to ensure that policies are complied with, and any non-compliance will be resolved well in time. The close monitoring of policy compliance is also advised by Chen, *et al*. (2015). Furthermore, the case firm may be suggested to introduce compliance training, which will help the staff to understand the policies and learn how to comply efficiently (Soomro *et al.*, 2016) Therefore, C2 may be suggested to implement a compliance monitoring system and train its staff to comply with anti-fraud policies as desired.

e) Compliance Audit

Audit is a useful measure to ensure that policies are adequately complied with. The literature shows that having a policy without compliance is the same as having no policy at all (Soomro *et al.*, 2016). Although, the case organisation has no specific policy related to the management of identity frauds, yet it has the audit procedures for the existing policies. In response to a question on policy compliance audit, respondent C2-R05 replied:

"It's internally audited and externally audited, and any issues are dealt accordingly".

Further to compliance audit, respondent, C2-R07 told:

"Our audit teams regularly check on the compliance of policies and violations are further investigated, and they take actions".

These statements indicate that the case firm has the process of compliance audit to ensure that the staff are adhered to the laid down policies. The compliance audit is conducted by internal and external auditors. In that process, auditors investigate, whether the policies are adequately complied with, issues with compliance process, and any violations. As a result of any policy violation or non-compliance, the auditors recommend the management for further investigations and management actions. However, C2 does not audit the policy compliance of third party organisations which are holding its customer information, which creates a risk of identity theft. Therefore, C2 may be suggested to conduct the audit to ensure the compliance of security policies of third party organisations to certify the security of its customers' information, which is also suggested by Liu *et al.* (2010).

f) Policy Updates

The practice of regularly updating the policies is significant to ensure the continued effectiveness of the objectives of the policies (Bechtsoudis and Sklavos, 2012). On the question, how frequently do you update a policy? Respondent C2-R01 replied:

"I think it's every 12 months".

, policy update takes place regularly, however in identity fraud management domain, the technologies are ever-changing, and the methods and trends of fraud are also changing. In order to counter the ever-changing fraud conditions, C2 may be suggested to update its policies more frequently or continuously. Thus, frequent update of policies may enable the e-tailers to make better arrangements for IDFM.

4.4.8 Investigation

It has a significant impact on the identity fraud management, as it helps the organisations to dig out the facts, collect the evidence and locate the offenders (Jamieson *et al.*, 2007; Wilhelm, 2004). In response to a question regarding the investigations of frauds, participant C2-R14 offered the following information:

"We will document everything about the accounts, everything about the address, whether there's been account openings at the address, who lives at that address. Any deliveries from other accounts to that address… anything we can find, the type of orders, the orders they have placed, whether there's been anything in the past delivered there which could be relevant".

The statement describes that the case organisation investigates the identity frauds, from the start and collects every bit of the information. During the investigation process the representatives also physically visit the address of goods delivery to investigate the fraud further. Therefore, the results confirm that the case organisation is also involved in IDF investigations, and it is a significant stage of IDFM. The investigation process and practices are explained as below.

a) Employing Specialist Investigators

The case firm has appointed a team of specialist investigators, and their responsibilities are to conduct investigations and catching the fraudsters with the help of police. Regarding these investigators, respondent C2-R02 mentioned:

"A lot of our regional loss prevention managers, the investigators, a lot of them are ex-police"

Further to that, respondent C2-R09 told:

"We get the special investigators [loss prevention managers], *the group security to go out and actually investigate that to try and catch them out".*

The statements confirm that C2 has appointed a team of specialist investigators. These investigators are designated as loss prevention managers. These investigators already have experience in crime and fraud investigations as the most of them are ex-police officers. These loss prevention managers conduct investigations inside the organisation and got out physically for further investigations and trying to catch the fraudsters with the help of police. These managers help organisations to investigate at its end and reduce the dependency on the police force for closer cooperation with them. Regarding their role, respondent C2-R06 informed:

"Sometime if the police won't assist us, Well, we have the regional managers do knock on doors and investigate themselves. Not everything goes to the police. We do knock on and do jobs. That's what their job really investigating. We do go with the police with some stuff going on that requires police involvement".

At this stage, as the results show, the loss prevention managers prepare the case for prosecution with the definite evidence necessary to catch and prosecute the fraudsters. Thus, the findings confirm that employing specialised investigators is significant to the field investigations and collection of as many as evidence and preparing the case for the prosecution, which also minimises the police role, enhances coordination with law enforcing agencies and make the police's job easy. Therefore, e-tailers may be advised to have a team of specialist investigators for better cooperation with police in effective IDFM.

b) Investigate with Prosecution in Mind

The investigation of IDFs should lead to prosecution for effective management of frauds. Regarding the investigation process the interviewee, C2-R12 told:

"Well, I would do all the investigation side here and put the case together. It would then be sent to our group security team, and they will be the ones who would liaise with the police, attend court [for prosecution], *stuff like that".*

The statement shows that C2 has a process of investigation, which is initiated by collecting the evidence. First, the frauds are investigated inside the organisation, afterwards, these are handed over to group security team, who will collect field evidence and share with police for prosecution. This shows that the case firm investigates IDFs keeping the prosecution in mind.

c) Collection of Evidence

The core purpose of the investigation is to collect the evidence and identify the fraudsters. In this regard, the case organisation uses its investigators to collect as much evidence to put out any chance of doubt. The case organisation uses internal and external information sources to collect as many as evidence. Regarding the internal sources, respondent C2-R01 mentioned:

"So we can look at all that type of information through our systems. We then have a look to see any other information at all that we can get for the address or the individual. If we get everything that we need, then again, it's all statements, and that's put into the police".

Similarly C2-R02 explained the process in the following words:

"If we're dealing with fraud deliveries, we use Teradata. On Teradata, if we put the account number in, it will bring back the IP address, and the IP address, we'll then obviously put the IP address into the internet, and it will give us the map location, and whatever, server, and the details that we pass to the regional loss prevention manager to deal with. Sometimes the police use that in their evidence".

For evidence collection, C2 uses internal data mining systems. The investigators put the account number in the database system to locate the IP address. That IP address helps to locate the geolocation of the fraudsters and identify the server used in the online transaction. Such information is further used as evidence and bases for field investigations. Therefore, the company uses it internal systems to collect evidence for further investigations and preserve these as evidence. In addition, C2 also keeps the proof of the delivery of goods, as mentioned by respondent C2-R01:

"We have a GPS system. So we'll have a look where the delivery was made".

Further to the benefits of keeping the proof of delivery, interviewee, C2-R15 told:

"So we can then have a look to see whereabouts that signature took place or did it take place at the address or did it take place a mile down the road..... With the signatures, we check all the driver's previous signatures.... Let's have a look at what the signature looks like. Is that the same as what the customer's is normally?

The statements confirm that for evidence collection, C2 uses GPS to know about the exact location of delivery, which helps to check, whether the delivery was made at the customer's door or any other place leading to the delivery driver's fraud. The delivery driver also gets the recipient signature, which helps to match it with customer's previous signatures. The results also indicate that these signatures help to identify any fraud committed by the delivery driver by matching it with deriver's previous signatures.

In addition, to collecting evidence from internal sources, C2 also uses social media. Regarding its use in the collection of identity fraud evidence, respondent C2-R01 informed:

"But the business can use this for other sellers as well, social media, tracking the activities on the social media, their shares, their locations. They can use that data as well for investigation and prosecution".

The practice of using social media in identity fraud investigations helps e-tailers to know more about their customers and fraudsters, their geo locations and activities to collect adequate evidence.

d) Reporting Fraud Cases to the Police

Legal action against the fraudsters has multiple advantages in IDFM. It helps to get fraudsters punished, loss recovered and creates fear among the fraudsters. Reporting the frauds is preliminary to the police investigations and prosecution. Regarding the reporting of fraud cases, respondent C2-R14 stated:

"We generally take it to the police and then we'll often find the police come back to us for more information".

Talking about the same, participant C2-R10 informed:

"We pull everything from application all the way down to the fraud being committed. All of that will be documented and provided to the police".

These statements indicate that C2 after preparing fraud case, reports to the police for further actions. Reporting identity frauds to the police helps to initiate an enquiry against the fraudsters. The reporting of identity fraud cases to the police sometimes is not enough to get their input, as informed by respondent C2-R10:

"I mean the police are obviously more concerning to things like…. So, that's why we fall so low down so that's why we offer to do it ourselves rather than waiting in the queue. We offer to do it, give the results back to the police then show where it is. Our technology is better than most police forces".

It reveals that the police are concerned with more critical issues and delay the business frauds. In that situation, the case organisation further investigates the frauds and collect more evidence. For online frauds, the police sometimes lack the technology to extract digital evidence. Further to reporting the police on identity frauds, interviewee C2-R04 made the following point:

"We're the small cog in terms of the prosecution. We wouldn't actually write up the statements for the police or obviously the government body but we would provide all the evidences and documentation, suggestions, and proposals to the regional loss prevention manager and then obviously it's regional loss prevention manager as a representative of the business do obviously exhibit evidence to the police".

The statement indicates that the staff at C2 do not write the evidential statements, which are the base for prosecution. One of the primary reason for lack of the police interest in business issues may be the absence of such statements with the evidence pack. The loss prevention managers at the case firm collect the cases from the analysis team, investigate further and present to the police.

The results confirm that C2 has the practice of providing evidence to the police. Such provision of evidence helps the police to prepare the case efficiently and prosecute the fraudsters on the basis of these evidences. Although, providing the evidence to the police is significant practice to get the police involved in fraud investigation and prosecution, but the findings indicate that C2 does not write customer statements, confirming the frauds and fraudsters' statements on the false representation, which make a case prosecutable. The practice of not writing the statements puts a negative impact on the fraud cases, as being incomplete or not prosecutable.

Therefore, C2 may be suggested to get involved in further investigations and write these statements to link it with the related state laws for making its cases prosecutable, which is also suggested by Jamieson, *et al*. (2007) and Mogaghan (2010). Furthermore, such practice may also minimise the police role, which is also recommended by Amori (2008), Brooks & Button (2011), Cross & Blackshaw (2014) and Lewis *et al*. (2014) for getting more police involved in fraud issues.

e) Catching the Fraudsters

Catching the fraudster with the help of police is a significant part of fraud investigations. The case organisation, after collecting enough evidence, gets the police help to arrest the fraudsters, for that, participant C2-R09 told:

"We get the special investigators, the group security to go out and actually investigate that to try and catch them out. We sometimes liaise with the police as well to try and catch the fraudsters…. So, we've had a number of arrests over the years especially in the … [name of an area] *area because that is the hotspot at the moment".*

The statement shows that the investigators at C2 personally visit the delivery address of the fraudsters to collect more evidence, and based on this evidence try to catch the fraudsters with the help of police. For catching the fraudsters, the investigators liaise with the local police with evidence and satisfy them to take action for arresting the fraudsters. Further to catching the fraudsters where the goods are not yet delivered, the case organisation performs controlled deliveries, as mentioned by respondent C2-R01:

"The first thing is we try to organise what we call a controlled delivery. So with the police, our delivery company, and ourselves, we will deliver the parcel…. What we do is we will deliver the parcel, and once that parcel's been delivered and signed for, the police will then arrest the individual".

Respondent C2-R11 had the following to add:

"So, if we detect a confirmed fraud, if we can, we will do a controlled drop on that fraud and let that item go through. And obviously, our intelligence unit in place are waiting to, obviously, intercept that parcel and capture that fraudster who is going to take that parcel in".

These statements confirm that to catch the fraudsters; the case organisation manages controlled deliveries. Furthermore, on the certainty of the arrested being fraudsters, the respondent was asked: "So how many among those deliveries are the fraudsters and are some real customers? Respondents confirmed that all those arrested through this delivery system are the confirmed fraudsters. Thus, the case organisation actively seeks to arrest the fraudsters. Therefore, it may be confirmed that the controlled delivery system helps to catch the fraudsters and initiate litigation process, and arrest of fraudsters create the fear of being caught and punished among potential fraudsters, which lead to better deterrence.

4.4.9 Prosecution

The prosecution has multiple benefits in identity fraud domain. First, it helps the organisation to recover the losses. Secondly, it helps the organisations to develop a bold image against the potential fraudsters. It creates fear among the fraudsters, which has a significant impact on their behaviour. Regarding that, participant C2-R10 mentioned:

"So if you can see, we don't just care about stopping the identity theft, we will take you all the way, and we're more than happy to stand up in court".

Respondent C2-R04 further added:

"We do regularly get our regional loss prevention managers prosecuting fraudsters from numbers of years or suspended sentences or agreeing to pay the debt back basically".

Above statements confirm that C2 has been prosecuting the fraudsters since many years. The regional loss prevention managers are directly involved in the prosecution and try to recover the losses and get the fraudsters punished. Furthermore, on the recovery of losses respondent C2-R05 informed:

"We don't only want the money back for the items you stole, we want all the money back for the time you had cost us, and how much you had put this company at cost to prosecute you".

The statement indicate that C2 is serious in dealing with the fraudsters so actively prosecute the fraudsters. The case organisation does not only ask for direct losses, but the investigation and prosecution expenses are also claimed. Thus, the results confirm that C2 is actively involved in the prosecution process. It does not go for the recovery of losses but also tries to get the fraudsters punished. Such punishment of fraudsters creates fear among potential fraudsters. Hence, deterrence is enhanced and a positive picture of the case organisation is developed against identity frauds.

a) Involvement in the Prosecution Process

To the organisational satisfaction and learning for effective prosecution, the representatives of the case organisation attend the courts during the prosecution process. Regarding such involvement, respondent C2-R01 informed:

"And what we then do is we then obviously prosecute with the police that individual in court...... I would then, my role would be then to, if prosecution goes ahead, is to go to court and stand up in court and give my evidence".

This shows that the case firm is actively involved in the prosecution process and its investigators attend the courts. The results confirm that such practice helps to represent the case in an effective way and learn to prosecute efficiently in future, so e-tailers may be advised to adopt this practice for better IDFM.

4.5 Case Organisation C3

C3 is one of the large online retailers in the UK. It has a chain of stores and a website for online business. It sells its own and various other brands and deals a variety of clothing and other household items. It has over 25, 000 employees dealing in chain stores and online business. The firm revues for the year 2016/17 was over £4 billion. Like two other firms this also is a credit lending company that allows its customers to open an account with the company and make purchases on credit. The credit is granted free of interest for a certain period of time and a fixed interest is charged beyond the specified period. Although, credit lending is a good scheme to attract customers, it also is prone to IDFs. These frauds and organisational practices to manage them are explained in the following sections.

4.5.1 Identity Fraud Types faced by C3.

The findings confirm that C3 is suffering from significant losses on account of IDFs. Most of the respondents informed that IDF is one of the leading challenges in online business. Respondents C3-R02 and C3-R05 told that mostly they face frauds when the customers refuse to acknowledge any order and receipt of goods. Respondent C3-R06 informed that fraudsters open accounts with stolen information, make a purchase and avoid the payments. The results also reveal that sometimes staff members steal the customer information and commit fraud within the company. Respondent C3-R07 told that sometimes friends of the victims steal the account credentials and make purchases to avoid the payments. Managerial practices to manage these frauds at C3 are detailed in the following sections.

4.5.2 Deterrence

As already mentioned, deterrence works to stop the fraudsters before any IDF attempt, for which customer education and creating the fear are critical aspects. The process and the practices of the case organisation at the deterrence stage are given below.

a) Customer Education

Customer education motivates them to take precautionary measures to reduce the chances of IDF attempts. The results disclose that C3 educate its customers on the security of their credentials through its website and emails, as mentioned by interviewees C3-R04 and C3-R02:

"There is security guidance and security statements upon the e-commerce sites".

"We send emails to customers advising them to put a strong password and do not share with any".

This shows that C3 educates its customers to create awareness of security and protection of their credentials. Such guidance is given through the company website and emails. The findings show two major limitations in customer education. First, only website and emails are used to educate the customers. The extant literature suggests social media, mass media (Bai and Chen, 2013) and text messages enhance the impact of customer education (Wright, 2007). Furthermore, the customer education is limited to the security of the password. Although, it may help in IDF deterrence, however, the literature suggests educating customers on identity theft trends and IDF methods and measures (Arachchilage and Love, 2014; Seda, 2014). Additionally, respondent C3-R01 stated:

"At the moment we use push messages through the mobile app but just for marketing purpose, not for education".

The statement indicates that C3 has a mobile app which is also used for messaging the customers, but, these messages are limited to marketing purpose only. However, such facility can be used for customer education to create awareness of identity frauds and countermeasures (McGee and Byington, 2015; Wright, 2007). Therefore, the case firm may be suggested to use push messages service to educate its customers on IDF issues and countermeasures, to enhance the deterrence.

b) Creating Fear of Being Caught and Punished

The literature findings suggest the creation of fear of being caught and punished to deter frauds. Regarding that, the results reveal that the case firm believes that any effort to create the fear among the potential fraudsters will put a negative impact on the business, as informed by C3-R06:

"Really speaking as a business, we don't want the society know that we are at risk".

Respondent C3-R02 further added:

"We don't want customers know that we are at risk".

This shows that the case firm is not sending any warning messages to the society to enhance its deterrence through creating fear. Additionally, the results confirm that C3 also gets the fraudsters arrested and prosecuted, however such information is again not publicised due to the reason that customers will assume that C3 is at risk of fraud attacks. Although, C3 is a business firm and does not want its customers to know that it is on the risk of frauds, however, C3 may still create fear. For that, C3 may not need to threat the fraudsters but publicise information on arrests and its measures to detect and prevent frauds. This will create fear for the fraudsters and will assure the customers that it has sufficient measures to secure its customers from being victims of IDFs. While publicising its measures against IDFs, C3 may consider the language and contents of the messages, as it should be ensuring the maximum security of its customers against IDFs, which will also result in the creation of fear for potential fraudsters. The practice of publicising the firm's arrangements on fraud prevention and detection is also advised by Zadig and Tejay (2010) on account of its effectiveness in fraud deterrence.

4.5.3 Prevention

The purpose of prevention is to secure identity information from any theft or breach and stop any unauthorised access to customer's' account. Defining the significance of prevention in IDFM, participant C3-R04 stated:

"I know it [IDF] *is down a lot and its use all the prevention methods, especially we use the computerised methods".*

The statement reveals that C3 has various arrangements at prevention stage, which are helpful to minimise identity frauds. These prevention methods are mostly technology-based and work to fail any attempt at identity theft or security breach. For effective prevention, Boss, *et al*. (2015), Holt and Turner, (2012) and Meinert, (2016) advise for the creation of severity of IDT and create awareness and train staff. But the results do not show significant efforts to prepare staff to counter the challenges of internal IDT.

Additionally, C3 may also be advised to educate its staff on IDT risk and measures to combat these threats, as recommended by Arachchilage and Love (2014) and Seda (2014). Therefore, C3 may be suggested to focus on human aspects of IDT prevention, which is a critical element in the security of information.

Additionally, the findings do not show significant measures on internal IDT prevention, which is a riskier exercise. In this regard, Alrashed (2016) and Wang *et al*. (2006) suggest the screening of staff handling the personal data, and a system that keeps the log of who accessed what information. Therefore, C3 may also implement staff screening procedure, which would be effective in preventing internal IDT. Some more preventive arrangements of C3 are mentioned below.

a) Sufficient Investments in Prevention System

A firm's strength against IDT depends on the efficiency of its prevention system. For effective and efficient prevention system, businesses have to invest significantly. The literature is evident that higher investments have a direct impact on the efficiency of these systems (Boyer, 2007). Regarding investments in IDT prevention systems, respondent C3-R01 mentioned:

"We have good trend of investing in our security systems; we try to get latest systems to prevent attacks on our systems".

The statement shows that C3 has the practice of investing in the technology that secures its IT systems and prevents information theft. But answering the same question another respondent claimed:

"I think more investment in technology would be substantial to enhance the IT security and especially more investment in professionals would give better results".

It reveals that C3 is more focused on investing in technology, yet for better results, more funds are required to enhance the prevention systems. Additionally, more investment in human skills development and knowledge enhancement is also needed for a better prevention system. Thus, the analysis forward that there is still room for improving the prevention system, by investing especially in human development. Therefore, C3 may be advised to focus on every aspect of IT security and information theft prevention especially investing in sophisticated technology and human resources for better deployment of the technology in the appropriate domain.

Although, sometimes it is difficult to invest more resources, but the firm should analyse the long run cost-benefit, as a single data breach may result in many times higher than real investments. Sufficient investments in prevention system are also advised by Boyer

(2007), Devos and Pipan (2009) and Goyal *et al*. (2012) in different domains and are not tested in e-tail sector. Therefore, C3 may be advised to revise its decisions on investments, based on long-term benefits and risks, and increase the focus on human development along with facets of prevention.

b) Securing Customers' Information

The security of customers' information is critical for e-tailers, as such information always contain the customers' payment details such as credit/debit cards and bank account details. To prevent the customers' credentials and financial information, C3 has various security measures in place. Mentioning on the communication security, respondent C3-R02 argued:

"Our internal and external communication is secured by end to end encryption, so whatever information we send or receive is encrypted".

It confirms the firm's arrangements for data security. Further to the security of customer information database and IT infrastructure, the same respondent confirmed that they have various security arrangements such as anti-virus, anti-malware, firewalls, anti-phishing and intrusion detection systems to fail any data breach attack.

Although, C3 has implemented these measures to protect critical information, but results reveal that these security arrangements are managed by third party organisations. When asked on the performance evaluation and monitoring of these preventive technologies, most of respondents told these systems are not evaluated or regularly monitored by the business, but the third party manages and reports to the senior management on their performance.

However, the preventive system works satisfactorily, its performance evaluation and monitoring are significant to confirm that it is engaged in proper domain. In this respect, the results show no arrangements for information security at the business end, but the firm only depends on the service provider, which may be riskier, as the ultimate responsibility lies with the e-tailers. Therefore, C3 may be advised to employ experts to evaluate the performance of security measures and monitor their deployment in the appropriate domain, which is also advised by Alrashed (2016), Goyal *et al*. (2012), Meinert, (2016) and Mithas and Rust (2016) for the effectiveness of prevention system.

c) *Updating the Prevention System Regularly*

Information technologies are evolving very quickly, so are the security threats. To keep the security measures uptodate, e-tailers need to upgrade their prevention systems on a regular basis. Regarding the updating of the prevention system, respondent C3-R02 emphasised:

"We have to stay at the top of methodology and have to employ the better secure systems but the fraudster will always employee another angle another method to try and beat the existing system so we regard this has been an evolving cycle of improving, it can't stop it has to be continued".

Respondent C3-R04 further added:

Because there's always new techniques that the fraudster finds to get around your firewall, basically. So you've always got to be keeping up".

These statements indicate that C3 has the practice of continuously updating the prevention systems. Although, the practice of updating the preventive software is helping to meet the challenges of ever-changing threats, however, the results also show that preventive arrangements are managed by a third party. So the issues on updating the preventive systems are not directly monitored by the management of C3, which may leave some risks related to system updates. As already discussed, the sole responsibility of customer information lies with the business management, so C3 may be advised to be directly involved in the management of preventive systems and actively seek to update the preventive systems, to face the emerging security challenges.

d) Having a Secure Authentication System

At C3, customers have to access their account to make an online purchase through an authentication process. The authentication system is the first line of defence against any identity fraud. C3 uses a single layer of authentication that includes the customer identity and password. This single-layered authentication is more prone to IDFs, as with stolen credentials fraudsters can easily access the account. So the e-tailer may enhance the effectiveness of authentication system by adopting one-time password sent through email or text message. The one-time password is sent to the registered contact, once the first layer of authentication is successfully passed. Thus, it helps to access the account with a temporary password, and any IDF attempt fails for having no access to the temporary password (Bang *et al.*, 2012).

Additionally, C3 may also be advised to adopt the practice of sending login alerts to the customers, once their account is successfully accessed (Kumar and Goyal, 2016; Wang *et al.*, 2006). It supports to detect any IDF at an earlier stage, which can be stopped and mitigated without incurring any losses. The practice of sending login alerts is currently adopted by many financial institutions. This practice is also utilised by Google and many other organisations, if the account is accessed through a new device.

4.5.4 Detection

In IDFM domain, detection has the role to identify suspicious frauds. E-tailers use data mining techniques to detect frauds, based on the pre-determined queries. The results show that C3 uses fraud screening system to identify suspicious frauds.

a) Having a Fraud Screening Process

Fraud screening process works on data sets to identify any suspicious frauds based on the rules. The findings confirm that C3 has a fraud screening system that processes every transaction to determine any link of the transaction with pre-set rules. The screening system is linked to the dataset, and fraud cues are embedded into that. Based on the information in these anti-fraud rules the screening system triggers out suspicious transactions, as participant C3-R05 pointed out:

"We also have the Falcon system which is a rule-based system which obviously works on rules in the background to stop or pop up orders in the pending queue which we then can investigate each customer whether it is genuine so not to just lose it, so we do our background check."

The statement shows that C3 has embedded various anti-fraud rules into the screening process to flag out suspicious fraud. These rules are mostly based on information from previous frauds, delivery address, the amount involved, IP address and device recognition. Thus, the system flags out suspicious frauds, which are then processed for further verifications. C3 is a business firm, so it cares about the customers and tries to confirm a scam before rejecting it. In e-tail domain, rejection of sales on the basis of suspicious fraud would result in losing customers, so C3 does a lot of background check before making any decision. These checks are detailed at mitigation stage.

Although, C3 is using screening system to detect any suspected fraud, a significant number of scams are not detected. In the IDF domain, new trends and methods are emerging continuously, as emphasised by interviewee C3-R07:

"And we will do strong controls around mitigating that. We're never going to stop it. People are always going to find a way".

Confirming it, participant C3-R01 added:

"I've got to say in our company that they can always get better because we're losing money. It's not as if we're stopping fraud completely".

These statements indicate that despite of the screening process some identity frauds go through, causing C3 losses. One of the possible reasons may be that fraudsters acquire access to authentic information. The effectiveness of a screening system also depends on human skills, which, as the findings show, is not adequately appreciated by the firm. Therefore, C3 may enhance the performance of IDF screening process through the development of human skills and knowledge regarding the fraud detection.

The findings also indicate that anti-fraud rules are frequently updated to detect IDFs using emerging trends and methods. The development of new fraud cues and updating the existing is based on the information from newly identified frauds, as stated by participant C3-R03:

"So if we get a fraud, we'll change the rules that we have. So we have a rule set that pushes stuff to fraud…we can notice daily of a change and we can implement that really quickly, push the data to our system to detect it.

This confirms that C3 frequently updates its fraud cues based on the fraud trends and methods used in detected frauds. Although, the fraud rules are frequently changed yet C3 is facing a significant number of successful IDFs. This shows that until fraud is confirmed and rules are changed, there occurs so many frauds. The results confirm that successful frauds are confirmed after a month or so, in some conditions it takes six months to prove an IDF. In such situations, many frauds take place before the fraud rules are updated, which may be one of the reasons for continued frauds.

Thus, the findings reveal that C3 has a reactive approach to updating the fraud rules, which may not work effectively. Therefore, to enhance the efficiency of fraud screening process, C3 may be suggested to adopt a precautionary approach and implement intelligent systems. In this regards C3 should enhance its learning on IDFs, through information sharing on fraud rules with other organisations (Power and Power, 2015). Likewise, C3 may also be suggested to emphasise on human aspects, as skills, knowledge and expertise of related staff can also improve the productivity of fraud screening process (Vahdati and Yasini, 2015).

b) Having a Device Recognition System

Recognition of devices used by customers to shop online is to some extent helpful to detect IDFs. With the help of cookies, the system recognises the device's make and model. Most of the participants confirmed that C3 has the system to recognise the devices used in any previous frauds. The system identifies the IP address and the device make and model. The device recognition system helps to detect any fraud coming through a device, or an IP address previously used in fraud. Regarding its functioning, interviewee C3-R05 mentioned:

"In device recognition system, if we put on there a fraud confirmed on a certain device, certain IP link, obviously this will feed into the database and then it will actually just jump out to us if that same device has been used again".

It indicates that it is a good system to identify frauds committed by organised groups, as they use same devices again and again to commit identity frauds. Thus, the system detects multiple accounts using the same devices and same account using multiple devices.

Although, it's a good system that recognises the device previously used in identity frauds, however, again it has some limitations in IDFM domain. At the outset, it only identifies the devices used in previous frauds; it means the system is not capable of detecting frauds attempted with other devices. Such limitation has also been mentioned by respondent C3-R05, when he was asked to how is the system efficient for new devices? He replied:

"No. I think that what the device recognition is for known fraud. So in the past, if that device has been used to open fraud accounts or with us, we know that that possibly is going to be a fraud account as well".

The customers use different devices to access their accounts as noted by participant C3-R02:

"Of course people do change their devices, people do, you know, you can use your iPad then your laptop then your mobile. But for us as a company, we wouldn't allow that order to go if it did change until we spoke to our customer. Sometimes they say they haven't placed that order".

This shows that the system detects new devices used either by customers or fraudsters. Further verifications lead to confirm, whether it's a fraud or not. Although, the system has some success in detecting IDFs, however, it only recognises the make and model of the device, and IP addresses change with the location of the customer, thus leaving a room for fraudsters. To improve the detection of IDFs through customers' devices, C3 may use a more intelligent system to identify not only the make and model but also the IMEI number and MAC address of the device and register the customers' devices with their accounts. The IMEI number is specific to each device, so linking the customers' devices with their accounts will further improve the detection of IDFs.

4.5.5 Mitigation

The findings demonstrate that once an IDF is suspected through the fraud screening system, it is then manually verified by a fraud analysts. The purpose of this stage is to discontinue any fraud, minimise the losses and try to reduce the effects of fraud on the customers and the firm. To achieve these objectives, C3 verifies the identity of the customers, reconfirm the order from the customers, support the IDFs victims and train its fraud managers.

a) Verification of Identity Information

The results confirmed that after detecting a suspected fraud through the screening process, the flagged transactions are then manually verified by the fraud analysis. The first thing fraud analysts do is to check the personal information, for which they use the various system, as mentioned by participant C3-R07:

"So there's no way that we would get one system that gives us all the information we need. Like I said, the RSA, basically a system purely used for the device recognition and the IP recognition, whereas obviously, the credit file search is Equifax. Equifax can't really give you much than that. The TraceIQ, the trace file system we've got, obviously that gives the information from the electoral roll and passport, and we do have a tool in the Tracesmart if someone's got a Facebook account, you can match up with that".

These techniques help to recognise the devices and IP address used, matching information with credit files, electoral registers, passport and social media accounts. The verifications done through these systems may help in detecting any false or engineered information. However, Identity frauds with genuine details may not be discovered using these methods, as mentioned by C3-R07:

"Sometimes you're going to have the case where you can't get through, and you need to make a decision. But I usually find, from when I was an adviser, the phone call is the decider. I may have done all the checks, and it was fine, but that phone call completely turned my decision. So we do rely heavily on the phone call and the questions that we ask for that phone call".

The statement indicates that though C3 uses the systems mentioned above, but identity frauds with genuine information need further verifications through a telephonic call. The questions asked on the telephone are very effective for detecting frauds with stolen identities. The results also reveal that combined use of verification technologies and telephonic calls gives very strong results as confirmed by interviewee C3-R02:

"Sometimes if we're talking to a customer, we don't believe they're genuine, or there's something not right, we can then ask them to provide us with the passport details and the system will then verify whether it's a correct passport or not".

The telephonic call has multiple advantages in deciding on suspected fraud. First, the call is made on the contact number taken from the account, which may vary from given in the order. Secondly, fraud analysis quiz the customers on the history of purchases and payments and additional information is also sought to verify during the call.

Nevertheless, these verifications may help in confirmation of identity frauds, but C3 may be advised to collect some documentary evidence at the time of opening a customer account, which can be verified at the time of any suspected fraud (Kahn and Liñares-

Zegarra, 2016). Furthermore, for the verification of personal information of new account applications C3 does not have a uniform policy, as two conflicting statements were discovered given by C3-R06 and R02 respectively:

"And it's a rule of thumb; you're supposed to call out on every new account. Because you might use all the systems in the world, but the person that you're speaking to is still not the right person. So we rely heavily on, on phone calls and the security questions we ask from those phone calls as well".

"So we don't actually do checks at application stage, but we'll do other stage, so you can get an account, but you might not get another".

These statements indicate that C3 has not laid down a policy for the verification of new account applications, which may leave some doors open to fraudsters. These fraudulently opened accounts turn into identity frauds, so C3 may be suggested to implement a process to verify each new account application and should also collect any document as a proof of identity (Kahn and Liñares-Zegarra, 2016).

b) Having a Victim Support System

The results disclose that once an identity fraud is unearthed, C3 has some practices to help the victims. First, the order is rejected, and the victim is assured of every possible support. In dealing with the financial losses, most respondents mentioned that the credit on the victim's account is waived off. And for recovery of credit history, C3 removes that amount from the victims account on credit record. These practices help to set the customer free from any obligation related to the fraud. Additionally, respondent, C3-R06 explained:

"So I think we'll register them at CIFAS, protect their identity that way, tell them to get credit report. Tell them if they're interested to get an alert on their credit file".

Participant C3-R04 also confirmed it by adding:

"We'll register them (victims) at CIFAS as part of protection and then we advise them on the credit file and have them the alert on the credit file because we tell them that CIFAS will protect them with other CIFAS lenders. Because obviously if CIFAS lender gets the referral, they'll get the alert".

The statements indicate that the victim support of C3 is not limited to its internal records but also register their information with CIFAS to avoid the victim any fraud with the associated organisations. It also suggests the victims get an alert service if their credit history is accessed, to timely detect any fraudulent attempt in future.

c) Information Sharing on Incurred Frauds

The results demonstrate that C3 has the practice of sharing information with other associated business firms. Identity information of the victims and confirmed frauds are made available to other business enterprises to help each other in the detection of IDFs. Confirming this, interviewee, C3-R02 mentioned:

"We share victims' information with other retailers so that this fraudster does not leave us and go next door like …."

The practice of sharing the victims' information within the associated firms also helps C3 to detect any recurrence of IDF. Such information sharing is beneficial for e-tail industry, so it may be adopted by each firm and coordination may be enhanced against IDFs.

d) Order Reconfirmation

The results confirm that C3 reconfirm some orders from the customers, after identity verifications. The results show that high-value orders, alternate delivery and collection services orders are reaffirmed through telephonic calls. The phone call helps to verify the identity and confirmation of the placed order. The telephone call also helps to detect any IDF using genuine information.

e) Mitigation Training

Mitigation includes practices to expose IDFs from suspicious transactions. At this stage, fraud analysts try to verify all the given information for being real and provided by genuine customers, which makes the role of the staff more significant in IDF management. To enhance the knowledge and skills of mitigation staff, C3 has implemented some training programs, as mentioned by C3-R07:

"I train them basically, initially, into the fraud area. That initial induction is 12 weeks training".

In addition to primary training, staff are also given training based on their performance in mitigation. The results show that the performance of mitigation staff is based on the quality of their decisions to unearth IDFs. Regarding the training for performance improvement, the same participant explained:

After they're referred to the training, they're taken into the areas of fraud, which obviously, are the prevention and detection areas. So obviously, they're actually there to detect and prevent it coming through, to stop things going out, which obviously are fraudulent".

Thus, the statements reveal that C3 has the practice of providing training, especially for mitigations staff. Because of the significance of mitigations staff in detecting IDFs, they are also given continued training to improve their decisions to unearth IDFs. The results indicate the significance of mitigation training, so e-tailers may be suggested to adopt such practices within their firms.

f) Dealing with Compromised Customers' Accounts

The findings confirm that C3 has the practice of closing down the compromised customers' account, soon after fraud is confirmed. The customers are then given new accounts to continue their shopping with the firm. The results also reveal that frauds are further analysed and initially investigated, but frauds involving a small amount of money and without concrete evidence are just ignored, and no further actions are taken.

4.5.6 Analysis

Within this stage, staff analyse the fraud occurrence and review the organisational arrangements and weaknesses that caused the success of frauds. The results reveal that C3 has sets of managerial practices at the analysis stage. The managerial practices at this stage are related to hiring experienced fraud analysts, reviewing IDFs occurrences, managing the fraud risks, evaluation of prevention and detection systems and performance measurement of mitigation staff.

a) Hiring Experienced Fraud Analysts

The role of analysts is central to the management of IDFs, so the firms employ experienced and highly skilled professionals. The results disclose that C3 has employed senior and experienced staff members as the fraud analysts. These analysts have vast experience in working in various positions related to the fraud management, as stressed by participant C3-R07:

“The team of fraud analysts are senior staff members and highly experienced in various fields related to the fraud prevention”.

Supporting it, respondent C3-R02 added:

“Most of our fraud analysts are the senior staff members; they have vast experience of working in different sections of fraud”.

These statements indicate that C3 has employed experienced staff members for the analysis of IDFs. Their experiences at different sections in IDFM may yield better results in reviewing the frauds, managing the IDF risks and performance improvement of mitigation staff. These analysts input their experiences, which help other stages to improve their performance. In response to the question, do you share your experiences with other staff members? Participant C3-R07 replied:

“Absolutely, it wouldn't work otherwise. So everything that is relevant, then absolutely, it's passed on… so it's easier just to give it out as early as I can”.

This shows that the analysts share their experiences with other staff members, such sharing helps the staff at mitigation stage to enhance their skills and knowledge and policymakers to develop better fraud management policies. Although, experienced analysts have a significant impact, however, the involvement of senior management in fraud analysis would return more input regarding extra resources and more authority. Therefore, C3 may be advised to involve senior management in fraud analysis to improve IDFM, which is also advised by Coulson-Thomas (2017).

b) Reviewing Identity Frauds

Effective IDF countermeasures depend on the knowledge of fraud trends and methods. To learn these methods and the extent of fraud losses C3 has the process of reviewing previous identity frauds. Such learning supports to enhance the effectiveness of fraud detection and mitigation practices. The results indicate that C3 has a process of evaluating the frauds and feedback the findings. Most of the respondents confirmed that all the incurred frauds are sent to the fraud analysts. They examine each fraud and try to locate the weaknesses of the reasons for the frauds being successful. The outcomes of these analyses are given to related offices to improve the fraud management. Regarding that feedback, the participants C3-R03 and C3-R02 informed respectively:

"So wherever we find new trends that get communicated to everyone in specialised position".

"If they see a certain fraud trend, we all keep each other up-to-date. So, the whole floor knows what to look out for; it can be a particular item or a trend…".

These statements confirm that the review team communicate the frauds trends and methods to the related staff members to enable them to be more vigilant on specific fraud trends. Information sharing on emerging fraud trends helps the staff members at other stages to develop countermeasures for effective management of frauds with new and emerging trends. It also enhances the skills and knowledge of the staff at various stages of fraud management. The results also indicate that the fraud prevention and detection systems are also updated in the light of fraud review reports. Regarding that interviewee C3-R04 stated:

"Once we find that trend and what they're doing, then our risk team will change our systems so that certain orders or certain types of referrals will refer out to us. So, they can change the rules to spot a trend".

It confirms that the fraud reviews are helpful to detect the emerging fraud trends and update the prevention and detection systems to counter these emerging patterns of frauds. Thus, the process of IDF review helps in learning on new frauds trends and methods, enhance the skills and knowledge of staff members regarding the fraud management and provide bases to update the prevention and detection systems to counter the frauds more efficiently.

c) Managing the Identity Fraud Risk

Risk management critically helps in minimising the occurrences of IDFs. The results indicate that C1 is facing significant losses in identity frauds, for which the statement of respondent C3-R07 affirms:

“Yes, we [are] *still losing significant and a lot of money on fraud, they still get in through”.*

Interviewee C3-R01 was a bit more optimistic:

“The fraud rate is lowering for us. Maybe not in the attempts, but certainly in the loss because of the systems being exceptional. I've got to say in our company that they can always get better because we're losing money. It's not as if we're stopping fraud completely”.

These statements indicate that C3 continues to face a substantial number of frauds, which shows that there is still significant fraud risk in the firm. The results show that C3 has the process of reviewing the fraud risk and develop countermeasures to minimise these risks. The findings also indicate that risk is there even after implementing more systems, but frauds trends and methods are emerging so the firm also continuously manage the IDF risks. The results reveal that the risk analysis in C3 is reactionary, based on fraud reviews, as elaborated by C3-R06:

“But it’s about trend analysis, and then what we’ll do from there is we’ll just keep tightening our controls. So, if somebody’s found a loophole, we’ll keep tightening it up”.

The results express that based on the fraud reviews C3 tries to tighten the control systems. It is a reactionary approach to risk management, which may be a reason for some frauds. On the other hand, the results expose that fraud management is a trade-off between stopping the frauds and messing up the customers, as mentioned by C3-R07:

“But at the same time, the point is, as I keep saying, it’s a balance between how much you affect the consumer and how much you stop the fraud”.

And:

I think that’s the golden question in fraud: How much security do you implement to slow fraud and also not piss off the customer? Because if you start annoying the customer and you lose legitimate business, then that’s the most important

These statements are significant in IDFM because being a business firm, C3 has to make a favourable trade-off between two extremes i-e stopping the frauds and annoying the customers. The results illustrate that C3 is cautious about balancing the two extremes.

Although, balancing is necessary, but an adequate education and awareness can let the customers understand the situation and cooperate with the firm to manage IDFs more effectively. The results also indicate that the business does not create fear for fraudsters to enhance the deterrence, only because of the risk of an adverse impression.

However, better education and awareness can create a sense of security for customers, and such threatening messages may be treated positively by the customers. Therefore, C3 may be suggested to more focus on the customer education that may result in support from customers to tighten the control systems to stop more frauds without annoying them.

d) Performance Measurement of Mitigation Staff

The performance of mitigation staff is critical to spot the frauds through different verifications. To enhance the effectiveness of IDF mitigation, C1 measures the performance of staff involved in mitigating the frauds. The results disclose that the performance of mitigation staff is evaluated regularly, as reported by C3-R05:

"My staff are managed and graded at the end of the year on their performance, and if any performance issue they are given training".

The statement reveals that C3 measures the performance of staff annually, and training are recommended to improve their performance. The results indicate that the analysis stage does not provide feedback to the mitigation staff on their decisions. Thus, no training is given to improve the quality of their decisions as a reflection of the feedback. As the fraud trends and methods are rapidly evolving, so annual training may not help to improve the performance of staff at mitigation.

The absence of timely feedback and related training may be an obstacle towards the quality decisions on fraud mitigation, which may result in weaker mitigation process. Therefore, C3 may adopt the practices of performance feedback and timely training of mitigation staff to minimise the number of triumphant frauds and the extent of IDF losses.

e) Evaluation of the Prevention and Detection Systems

The prevention and detection technologies have a crucial impact on the management of IDFs. The results reveal that C3 has no process to evaluate the performance of these systems regularly. For detection technology, participant C3-R06 informed:

"The suppliers of these technologies demonstrate us their performance… whenever we buy or update a technology they show us their performance".

It indicates that the performance of prevention technology is evaluated at the time of its implementation and update. This shows that C3 does not have any process to evaluate the performance of prevention system on a regular basis, which may be a risk of data breach. Technologies are evolving with the time and the old one become absolute and ineffective to prevent attacks with emerging trends.

Based on the findings, C3 may be recommended to adopt the practice of regularly evaluating the performance of the internal staff and the external professionals to keep the defence enacted against any data breach or identity theft attack. The performance evaluation of prevention tools is also advised by Seda, (2014), through penetration test, vulnerability assessment and overall defence analysis.

The findings also reveal that C3 evaluates the performance of the detection technology related to the update in fraud rules to verify if it is adequately working on the newly implemented rule(s).

Although, it's a good practice to check the performance with new updates, but C3 may also be advised to involve external professional organisations to evaluate the performance of prevention and detection technologies. The performance evaluation of detection technology is also advised by Bierstaker *et al*. (2006) to be done through statistical and false positive ratio analysis.

f) Setting Identity Frauds as Management Priority

The results show that the top management is not presented reports specific on IDF issues and losses. They are forwarded with regular reports on overall fraud losses. As already mentioned more than half of the total frauds are the identity related, so the senior management may be given detailed reports on the losses and arrangements on IDFs. Thus, detailed reports on IDFs and countermeasures would catch the attention of senior management, which may make the IDFM more effective. The practice of involving the senior management in IDFM is also suggested by Coulson-Thomas (2017).

4.5.7 Policy

Fraud management policies provide guidelines to adopt the practices which help to achieve desired goals. For the effectiveness of policies, their development, communication, awareness and compliance are significant processes. The fraud policies and related issues in C3 are mentioned below.

a) Having Fraud Management Policies

The results expose that the case organisation had some policies but limited to the security of information. When asked about IDFM policies, the participants told:

"We have a security policy, so group security policy that covers every eventuality". (C3-R04)

"So there is anti-money laundering policy, there is a fraud policy, and within those, there are certain elements that relate to frauds". (C3-R01)

The statements show that C3 has the policies related to the IT infrastructure security, information and communication security and money laundering. The results indicate that C3 is more focused on the policies linked to information security and internal frauds. The significance of having related policies is also advised by Singh *et al*. (2013), Soomro *et al*. (2016) and Soomro *et al*. (2017) for the security of information and implementing change.

Nevertheless, these policies help but are limited to the security of identity information at the prevention stage only. It would assist in securing customers' identity information which is used in IDFs. However, an effective IDFM needs a comprehensive set of policies related to each stage of the fraud management. When asked about IDFM policies, all of respondents replied in negation. The absence of such policies may lead to a variety of responses to the same situation, which may cause chaos within the firm in dealing with IDFs.

Therefore, C3 may be advised to develop a comprehensive set of IDFM policies at each stage of the fraud management to provide proper guidelines to their workers for a uniform and planned actions. The need for comprehensive fraud management policies is also emphasised by Bierstaker *et al*. (2006) and Njenga and Osiemo (2013). The IDFM policies should be dealt at the top management level, and input from operational level staff should be sought to make effective policies (Coulson-Thomas, 2017; Albrechtsen and Hovden, 2010).

b) Policy Update

The policy update is necessary to enact their effectiveness with diverse environmental challenges. IDFM challenges are ever changing with the advent of new technologies and fraud trends. Although, C3 has no set of IDFM policies, however, the results show that the firm has the practice of reviewing and updating existing security policies every year. The fraud trends and methods are ever-changing, so once IDFM policies are developed, these should be updated on a continuous basis. The practice of updating the policies is also advised by Bechtsoudis and Sklavos (2012).

c) Policy Awareness

The awareness of policies is necessary for their compliance. In this regard, the results show that all the polices are make available through the organisational database, so any staff member in need of any policy may access to it. Although, the ready access to the policies is supportive of staff for getting awareness on various policies, but policy awareness can still be enhanced through active learning system.

To increase the policy awareness, C3 should actively reach each with related policies and ensures that every staff member is well aware of the policies in fulfilling his/her job. To ensure the policy awareness, C3 may develop awareness training and campaigns. The practice of creating the policies' awareness is also highlighted by Siponen *et al*. (2014) and Soomro *et al*. (2016). Furthermore, Bierstaker *et al*. (2006) suggest for getting a written acknowledgement that each staff member has received a copy of related policies and understood it.

d) Policy Compliance

An active policy compliance process is indispensable to achieve the objectives of any policy. The results show that the compliance of policies is regulated through internal and external audits. Regarding the regular internal and external audit for policies' compliance respondent C3-R06 told:

“Every department that is annually audited by the head of compliance ... each department has to succeed, and has to provide evidence of their compliance, so we internally audit the compliance and we externally audit”.

The practice of conducting compliance audit helps in ensuring that the policies are complied with at their spirit. In the absence of the policies, compliance practices do not add towards the IDFM, so C3 may be suggested to develop policies at each step of the fraud management and ensures better practices, with continuous monitoring of compliance through direct supervising staff. Additionally, C3 may also develop a mechanism for policy compliance that would help to ensure a positive staff behaviour towards the compliance.

e) Data Access Management Policy

The policy for access management on critical information is significant to prevent any unauthorised access and minimise the probabilities of internal IDT. The results express that C3 has data access policy, which describes that the data access to the staff members is limited to their job roles. As a member of staff mentioned:

“We are given limited access to the customers’ and other data in relation to our responsibilities”.

This shows that each staff members do not have access to customer and the organisational information beyond their nature of duties and responsibilities. The access is limited to the information necessary to accomplish their job roles. The findings confirm that the data access is annually reviewed and restored in accordance with the access management policy. Although, it’s a good practice to have such policy but access privilege should be monitored more frequently with the change of the duties and responsibilities of related staff members.

4.5.8 Investigation

IDF investigations are necessary to find out the facts and collect as many as evidence to fix the responsibilities and prosecute in the court of law. The results indicate that C3 has managerial practices for investigating IDFs, which confirms that investigation stage is also observed as a stage of IDFM. The results of the processes and managerial practices for IDF investigations are mentioned as under.

a) Employing Specialist Investigators

The effectiveness of IDF investigations depends on the knowledge and expertise of the investigators. The results pass on that, for effective investigations, C3 has employed a team of expert professionals, as mentioned by participant C3-R04:

"Our proper investigators are mostly from police officers, as when we have a case even down so write in the statements we do all the work, so the police are concerned for odds part, while everything else is done from us".

These investigators come with many years of experience in related field. Some interviewees also informed that these investigators are given proper training on the firm-specific technology to enable them working with these systems. These investigators try to minimise the role of the police and prepare the IDF cases at the business end by collecting enough evidence.

The results also reveal that the investigation team also comprises of technology experts to extract information from the live systems to present as evidence for frauds. Thus, the results confirm that C3 has employed a team of legal and technical experts to make the investigations more efficient. The results confirm that employing specialists for IDF investigations have significant effect, so e-tailers may be advised to have this practice for better IDFM.

b) Investigate with Prosecution in Mind

There may be multiple reasons for investigating IDFs, but the ultimate goal is to collect evidence which may help in effective prosecutions. The results reveal that the investigators at C3 get the evidential statements and attach evidence that is enough for trial, as argued by C3-R07:

"Whereas we do that as an organisation, we follow fair investigations, so we want them prosecuted".

The results reveal that the evidence is preserved in accordance with the related laws and connections with legal acts are developed, to make the fraud prosecutable. Such practice of investigating the frauds with an aim for prosecution will help at the later stage to provide evidence to the court of law to prove the fraudsters guilty.

c) Collection of Evidence

Evidence is the base for the prosecution of a fraudster. Prosecutions in IDFs are effective when sufficient evidence is provided to the courts to determine a fraudster being guilty of committing an IDF. Thus, the e-tailers have to collect, preserve and present a set of evidence to the police and prosecution. On the significance of evidence, respondent C2-R06 informed:

"Yeah, it is just as much as evidence to build a bigger picture to confirm the identity fraud ... you cannot go to the police just say we think this is a fraud. You need some evidence to back it up".

The statement shows that the collection of evidence is significant for prosecution, so it has the practice of investigating IDFs to collect as many as evidence, as reported by interviewee C3-R02:

"If we can get the evidence, not just the devices, we can get the individuals and have them with the goods have the telephone conversations, have the IP addresses, all goods stuff to get the initial arrest".

Respondent C3-R03 confirmed this view:

"We take all the types of information through our systems. We then have a look to see any other information at all that we can get to the address or the individual. If we get everything that we need, then again, it's all statemented, and that's put into the police as evidence".

The findings show that C3 has the practice of collecting evidence from their systems, which are mostly related to the used devices, IP address and information related to the individual and the delivery address. Thus, the results confirm that C3 has the practice of collecting the evidence and provide these to the police for further investigation and prosecution in the court.

The results also reveal that these evidence are obtained only through the internal resources and information systems. However, C3 does not use the external sources for evidence collection. Confirming the significance of evidence collection, this study suggests that e-tailers should adopt this practice to improve IDFM.

d) Reporting Fraud Cases to Police

Reporting the fraud cases to the police is a preliminary step towards further investigations and prosecution. The results show that C3 reports the IDF cases to the police, as mentioned by participant C3-R02:

"In certain circumstances, they're reported to the police, and that goes through action fraud which is the UK's fraud management system for reporting. And the police can then investigate it as well as they can".

It confirms that C3 has the practice of reporting the IDF case to the police for further investigations and prosecutions. The results also show that mostly the frauds are reported to the police, but all the claims are not entertained by them, as mentioned by participant C3-R03:

"The police probably wouldn't look something of without value, but it would be reported of a fraud account".

And

"Sometimes police take action, and some time they don't because they say a bit like already said why don't you stop the parcel".

These statements describe that not all the reported cases are taken by the police. The results also reveal that mostly the cases with a small amount of money and with lack of evidence are not entertained by the police. The literature findings also suggests that the police force are already busy in other more critical issues, so they are reluctant to take the fraud cases with insufficient evidence and less valued items. In this regards e-tailers may be suggested to improve its investigations and collect and present evidence in such a way that the police get involved in fraud issues. Such practices are also forwarded by Jamieson, *et al*. (2007) and Monaghan, (2010) for better investigations and developing coordination with police.

Furthermore, it is evident from the extant literature and the results that the police force are busy in more critical issues, so fraud cases get less of their attention. In this situation, e-tailers have to come forward and develop close coordination with the police force to get their input in investigations and prosecution of IDFs. Regarding such coordination, respondent C3-R04 said the following:

“The police are so understaffed that if we want our prosecutions to go ahead, we need to assist them. So we investigate at our end, that's so important to have that cooperation”.

The statement shows that C3 has the practice of coordinating with the police force because of the lack of resources and less interest in small fraud cases. The results also indicate that the appointment of ex-police officers as the investigators is a significant practice to develop such coordination with the police. The findings results also show that C3 has the practices of investigating the cases at its end, making evidential statements and collecting evidence, which is helpful in developing coordination.

Although, C3 workouts on fraud cases, however the lack of police response show that the firm should prepare and present IDF cases in such a way that require least efforts from the police force, which would develop better coordination. The practice of coordinating with police force by reducing their role is also advised by Amori (2008), Brooks and Button (2011), Cross and Blackshaw (2014) and Lewis *et al*. (2014).

e) Catching the Fraudsters

The purpose of IDF investigations and prosecution may not be accomplished if the fraudsters are not arrested. The results show that the firm has the practices of collecting as many as evidence and doing controlled delivery system to get the fraudsters caught by the police, as highlighted by respondent C3-R03:

“So we actually go with the police and actually arrest, is with technical support group, known fraudsters who we identify through IT security systems and through the fraudulent orders”.

Although, it’s a good practice to stand with police for the arrest of fraudsters, however, the results show that most police are reluctant to get involved in small-scale fraud cases. Therefore, the firms should improve its investigations to develop substantial grounds for the arrest of fraudsters. Such improvements may include field investigations and using external resources for evidence to make it as an easy arrest for the police, which would be a motivating factor for the police to arrest the fraudsters.

4.5.9 Prosecution

In IDF domain the prosecution has multiple advantages. First, it helps to get the fraudster punished. It helps the e-tailers to recover their losses and maintain their position against fraudsters. The punishment decisions create a fear among the potential fraudsters, thus enhancing the deterrence. The results indicate that C3 has not an aggressive strategy to prosecute every fraud, yet with concrete evidence and police support, it prosecutes the fraudsters, as mentioned by participant C3-R04:

"*We will then meet with police show them the concrete evidence and apply with police for arrest warrant and prosecution".*

The statement indicate that after collecting the evidence and preparing the case, C3 approach the police for prosecution. The results also reveal that not all the time police entertain the case and take action to arrest the fraudster and prosecute. To make the trial more effective C3 may be advised to improve its investigations and prepare the cases in such a way that requires fewer actions from the police force. The fraud cases may also be prepared in accordance with the law, and legal issues should be addressed to enhance its chances to be accepted for prosecution.

a) Involvement in the Prosecution Process

For successful prosecutions, it is necessary for e-tailers to be involved in the courts and help the court by providing additional evidence and other information if required. The results confirm that C3 is represented by a senior staff member from investigations team, as mentioned by the interviewee C3-R01:

"So I might do more evidence, more statements and then it goes to the crown prosecution service, they then ask lots of questions, and again, you might need to change your evidence….not change it, but add to it. And then obviously we go to court …."

The practice of being involved in the prosecution process was also confirmed by other participants. The results indicate that for effective prosecution the representatives of the e-tailers are directly involved in the prosecution process and follow up the trial, to respond any enquiry and provide any further evidence. It confirms that following the prosecution process is helpful in getting the prosecution successful by defending the business position and getting their plead granted. So e-tailers are suggested to take active part in prosecution process for better IDFM.

CHAPTER 5
CROSS-CASE ANALYSIS AND DISCUSSIONS

5.1 Introduction

In this chapter, identity fraud management practices are compared between the case organisations. Managerial practices at each stage of the underpinning framework are discussed for their significance and suggestions are made to improve these practices to achieve an effective identity fraud management. The individual results of each firm are dsicussed in the previous chapter. This chapter presents the cross-case analysis of the data. Cross-case analysis is widely used to synthesise the results produced by small number of cases based on replication logic (Yin, 2014).

At first, results on the types of identity frauds are presented. Then managerial practices at each stage of the fraud management are compared within the case organisations. The limitations regarding the managerial practices are introduced, and improvements are suggested to make IDFM more efficient for each case firm. The framework extension is explained in IDFM context, and research contribution is explained.

5.2 Methods and Types of IDFs in E-Tail Sector

At the outset, the findings confirm that the case organisations are facing significant losses on account of identity frauds. It was also established that identity theft and IDFs are the leading challenges in e-tail business. It was known that application fraud, account takeover, friendly fraud, first-party fraud and internal identity theft are the most common identity related frauds faced by the e-tailers. The literature identifies these types of identity frauds as the most common too. Additionally, delivery fraud was also found in these firms, which is an addition to the research. The delivery fraud occurs when the delivery driver does not deliver the parcel and fraudulently sign it, as delivered.

The data reveals that most of these frauds are committed through stolen identity information and account credentials. The findings demonstrate that although, fraudsters mostly steal identity and account credentials from customers rather than from e-tailors, the latter face the risk of internal identity theft and the breach of sensitive customers' information, especially their bank details. To counter these risk e-tailers have implemented various preventive technologies. The managerial practices for IDFM and IDT prevention are presented in the following section.

5.3 Analysis of Managerial Practices of IDFM in the E-tail Sector

The managerial practices of case organisations for IDFM are analysed and discussed below with respect to the each stage of framework.

5.3.1 Deterrence of IDFs

Deterrence is a set of precautionary practices to minimise the chances of IDF attacks (Jamieson *et al.*, 2007). Deterrence practices reduce fraud attempts through customer education and creating fear of being caught and punished. Customer education helps to minimise the chances of identity theft-which is a pre-requisite for IDFs, whilst fear of being caught and punished averts the behaviour of fraudsters towards not attempting any fraud.

Educating the customers regarding the risk of identity frauds significantly minimise the chances of a successful IDF attempt (Albrecht *et al.*, 2011). It also enhances the customer awareness of the risk of IDFs thus motivating them to take countermeasures. Our analysis reveals that all three firms educate their customers regarding identity theft and advise them not to share their credentials with anyone. Such practice is also highlighted as significnat for IT security, ID theft and e-commerce frauds by Arachchilage & Love (2014), Seda (2014) and Sperdea *et al*. (2011) respectively.

Managerial practices addressing customer education at each firm are summarised in Table 5.1. C2 goes a step ahead and warns its customers of phishing emails and other methods of identity theft, which helps the customers to be vigilant in respect of identity theft attacks and take countermeasures to mitigate associated risks. These practices are in line with the suggestions of Arachchilage and Love (2014) and Seda (2014).

Educating customers on possible IDT methods and counter measures is an effective instrument of fighting IDFs. Therefore, C1 and C3 and other e-tailers may be advised to pay greater attention to customer education of the IDT methods and countermeasures to enhance the efficacy of identity theft prevention. Additionally, e-tail firms may also educate their customers not to share personal data on social media, as advised by Ann

McGee and Ralph (2015) to minimise the chances of account takeover and application frauds.

Table 5. 1 Comparing the cross-case managerial practices at deterrence stage

Processes	**Managerial Practices**	C1	C2	C3
Customer Education	- Advise the customers to secure their credentials.	Yes	Yes	Yes
	- Suggest customers putting a strong password and periodically change it.	Yes	Yes	Yes
	- Customers are warned of phishing emails and other sources of identity theft.	No	Yes	No
	- Use website and email for customer education.	Yes	Yes	Yes
	- Suggest customers check their credit history regularly.	No	Yes	No
Creating fear	- Get the fraudsters arrested and prosecute them.	Yes	Yes	Yes
	- Publicise successful prosecution and arrests in local media.	Yes	No	No
	- Conduct controlled deliveries to arrest fraudsters.	Yes	Yes	No

Table 5.1 presents managerial practices at the deterrence stage in each case firm. It shows that managerial practices adopted by these firms are nearly identical. In customer education C2 has adopted more practices as compared to the other firms, whereas the C1 has a better process and additional practices in comparison to the other two e-tailers.

The findings show that C2 educates its customers to check their credit history regularly, as this helps to recognise any identity fraud attempt or occurrence at an earlier stage. But C1 and C3 do not have such practice, which may result in detection of frauds at a later stage, where mitigation may not be possible. In order to detect IDFs at an earlier state, C1 and C3 may be suggested to advise their customers to check their credit history regularly, and may also offer free access to credit history to their customers. For the same reason, the case firms may also advise their customers to check their bank and credit card transactions regularly, as IDFs uncovered at an earlier stage can be mitigated to minimise the losses, as suggested by Alrashed (2016).

The findings also reveal that all the companies are using websites and emails to educate their customers. Although, these channels may work, but the impact of customer education may be enhanced further by using more active channels, such as using text messages and push messages. C3 uses push messages but they are limited to marketing information. Additionally, the use of social media may also help to enhance the customer efficacy in IDF deterrence. In order to enhance the impact of customer education for pursuing them to adopt preventive measure, e-tailers may use push messaging and text messing services, and social media. The limitations for existing practices and suggestions to improve these are detailed in Table 5.2.

Table 5. 2 Suggestions for improvements of IDF deterrence

Limitations of existing practices	**Related to**	**Suggestions**	**Valid for**
Advise the customers to secure their credentials.	C1, C2 and C3	Customers should be educated on methods of identity theft and countermeasures.	C1, C2 and C3
The e-tailers are using push messages for marketing.	C3	Push messages service should also be used for customer education on IDF	C1, C2 and C3
Suggest customers check their credit files regularly.	C2	Customers may be offered free access to their credit history accounts.	C1, C2 and C3
Only website and email are used for customer education.	C1, C2 and C3	Should also use texts and push messages.	C1, C2 and C3
Publicise arrests and prosecutions in local media.	C2 and C3	Publicise such information in mass media to ensure the customers of their security, and a message to fraudsters on the certainty of fraud detection and legal action.	C1, C2 and C3
Does not conduct controlled deliveries to arrest fraudsters.	C3	Controlled deliveries should be made to catch the fraudsters.	C3
Customers are only advised to change their passwords regularly.	C1, C2 and C3	Advise customers to check their bank and credit card transactions regularly, to detect IDF at an earlier stage.	C1, C2 and C3

Table 5.2 presents the limitations of existing managerial practices adopted by the case organisations and suggestions are forwarded to improve these practices. These suggestions are based on cross-case analysis of the empirical findings and literature reflections.

The literature findings suggest that the fear of being caught and punished can be created by apprehending and prosecuting the fraudsters, publicising information about prosecutions and the stance that the organisation takes in respect of IDFS. In this regard, the collected data demonstrate that all the case firms try to get the fraudsters arrested and prosecuted, with a varying degree of effort.

The deterrent effects of catching and prosecuting the fraudsters can be multiplied through publicising such information in mass media. The practice of disseminating the information on caught and punished is only adopted by C1. C2 and C3, as already mentioned in the previous chapter, are reluctant to disseminate such information because they worry that this would deter potential customers from making purchases online. The details regarding each firm are given in Table 5.2.

This attitude of C2 and C3 is in contrast with the recommendations one can find in the literature on banking frauds, accounting frauds, cyber-attacks and IT misuse deterrence (See D'Arcy *et al.*, 2009; Dorminey *et al.*, 2012; Guitton, 2012; Leasure and Zhang, 2017; Workman and Gathegi, 2007). However, so far no research of this issue has been done in e-tailing. E-tailers operate in a challenging environment, in which competition is very intense. E-tailers are likely to be particularly sensitive to spreading messages that may have a negative impact on customer confidence. This puts them in a difficult position. On the one hand, as my results show, e-tail firms seek to minimise the risk of losing such confidence.

On the other hand, lack of deterrent communication increases the threat of identity frauds. Therefore, e-tailers, especially C2 and C3, should consider publicising information on threats and fraud deterrence in such a way that it should not make an unfavourable impression on potential customers. For this, they should set the content of the messages in such a way as to show the certainty of fraud detection and consequent legal actions. Presented in such a way, information is more likely to reassure the customers that the firm they are dealing with has a modern and efficient detection system and their identity information and accounts are safe. At the same time, such content will forward a warning to potential fraudsters of the inevitability of being detected and punished if they transgress against these organisations. The detailed suggestions for IDF deterrence are presented in Table 5.2.

C3 also lacks a controlled delivery system, which is likely to undermine their chances to catch the fraudsters red-handed. As the findings from C1 and C2 suggest, a controlled delivery process has a deterrent effect and sends a warning signal to potential fraudsters. For this reason all e-tailers may be recommended to consider arranging controlled deliveries. The practice of helping the police with making arrests may also enhance the cooperation between the e-tailers against identity fraud investigation and prosecution.

5.3.2 Prevention of IDFs

Prevention is a critical stage in IDFM, as it helps to secure the information, which is used for frauds. It was revealed that e-tailers have specific processes and practices, which help them to secure the identity information. The significance of a prevention stage is also highlighted by Jamieson, *et al*. (2007), Kumar, *et al*. (2007) and Wilhelm, (2004) for internal frauds, identity theft and common frauds.

Sophisticated prevention technologies, their implementation and operations are expensive and require substantial investments. It was confirmed that e-tailers have sufficiently invested, but these investments are limited to the acquisition of sophisticated technologies. The analysis illustrate the all case firms are more focused on investing in technology, whereas the human related issues are given less attention. The significance of human aspects of information security and IDT prevention has been emphasised by many authors, including Boss *et al*. (2015) and Meinert (2016) but it appears that firms are not investing enough in this critical aspect of IDT prevention.

Lack of investments in staff training and awareness may lead to employee ignorance, insecure use of IT systems and lack of skills required to make the most of these systems, which may facilitate information theft and breach of information security. Additionally, only the experts can ensure the appropriate deployment in preventive technologies, so for the effective use of these systems, e-tailers should also focus on investing in human development and related fields. Thus, prioritising investments in developing human skills and awareness for a better prevention system would help to enhance the performance of prevention stage. Better preventive measures may ensure the security of customers' data and lessen the chances of IDT. The detailed suggestion on improvements in prevention stage are given in Table 5.4.

This study has established that all the firms have taken measures and adopted various practices to secure customers' information (see Table 5.3). For the security of the internal network, firewalls have been installed to fail attacks on the firms' databases. All communications are monitored for security purpose, and all the incoming and outgoing customer information is protected by the end to end encryption, to prevent a man-in-the-middle attack. Additionally, anti-virus and anti-malware software is used to protect e-mails and other internet traffic from any malicious attack. These technological arrangements are in line with the suggestion by Ahamad *et al*. (2014), Alrashed (2016), Devos and Pipan, (2009), Geeta (2011)and Goyal *et al*. (2012) for cybersecurity.

Information technology is evolving very fast, so various challenges continue to emerge almost on a daily basis. To keep the IT security and prevention systems operational, firms need to evaluate their efficiency and update them constantly. My results show that prevention systems of the case firms are managed through outsourcing, thus putting their evaluation and update also in the hands of external firms (especially in the case of C3). It was affirmed that C1 evaluates its system by itself on a regular basis, so the decisions on updating it are taken by the management.

In the case of C2, the services of a neutral third party professional firm are hired to evaluate its prevention systems, hence updates are recommended by the external party. As for C3, no evidence was found that the firm had any evaluation practices; only reports from the supplier of these technologies were reviewed at the time of installation. With the developments in technologies and emerging risks, the best systems of the past become ineffective. The details of managerial practices of the prevention stage are given in Table 5.3.

It was also discovered that updates related to preventive technologies are also offered by the suppliers of these technologies. Although, out-sourcing has many advantages, still the C2 and C3 should get involved in evaluating the performance of their prevention systems, because the end responsibility of the security of sensitive information lies with these firms. Their management is suggested to employ professionals or train internal staff enabling them to ensure the performance of preventive technologies. Furthermore, the decisions of system updates should also be based on the regular evaluation reports and efforts should be made to have the latest versions of hard and software.

The findings highlight that even when IDT occurs on the customer side the e-tailers bear fraud related losses. Because of this, e-tailers have to adopt better managerial practices to prevent information theft at the customer end. The findings show that the case firms do educate their customers, but such education is limited to securing and regularly changing their passwords. The practice of suggesting the customers on the security of their credentials is not workable, if possible methods of IDT and countermeasures are not communicated. Therefore, e-tailers should create awareness of potential IDT risks and countermeasures, which is also supported by Archchilage and Love (2014) and Seda (2014) in IT security and IDT prevention.

Additionaly, Devos and Pipan (2009) suggest that organisations should provide their customers free software to help them to avert IDT. Such practice is already adopted by some banks in the UK. Although, this practice may help customers to avoid IDT it may create a financial burden for the e-tailers. The e-tailers should study the cost and benefits of offering free anti-virus and other preventive software and act as appropriate.

Table 5. 3 Comparing cross-case managerial practices at the prevention stage

Processes	Managerial Practices	C1	C2	C3
Sufficient investments	- Sufficient investments are made in the prevention technologies.	Yes	Yes	Yes
	- Human aspects of IDT prevention are given an appropriate share in investments.	No	No	No
Securing customers' information	- The internal network is protected at all entry and exit points with firewalls.	Yes	Yes	Yes
	- The flow of communication is monitored for security purpose.	Yes	Yes	Yes
	- Emails and internet traffic is secured through anti-virus and anti-malware.	Yes	Yes	Yes
	- All the incoming and outgoing customer information is encrypted.	Yes	Yes	Yes
	- Regularly train staff on security risk and safe use of IT sources.	No	No	No
	- Should having effective arrangements for internal IDT prevention.	Yes	No	No
	- Information theft prevention systems are evaluated regularly	Yes	Yes	Yes
Update prevention systems regularly	- Life-cycle management for all systems to update regularly.	Yes	Yes	Yes
	- Upgrade every system to its current level.	Yes	Yes	Yes
Authentication system	- Standard, based on ID and password.	Yes	Yes	Yes

Table 5.3 presents managerial practices found in the case firms. This shows that the case organisations have similar processes and practices for the prevention of IDFs. It also reveals that these firms are more focused in the technology and less attention is given to the human aspects especially training and development of IT professionals, which may one of the reason of recurring IDFs.

The human related issues also have a significant impact on information security and preventive measures. There are two main aspects in the current domain, first is the knowledge and skills of professionals managing these systems. In this regard, the findings show that the case firms mostly rely on the capabilities of third party professionals. Although, security and preventive arrangements are outsourced, still e-tailers are advised to employ own professionals in the field to ensure that the third party arrangements are best serving the objectives of the business.

The other human-related facets of IDT prevention are the awareness and education of IT users. The case firms have been found not having any comprehensive programme to educate and increase awareness of staff members. Although, some policies and initial training are there to guide the staff, but these are not flexible and updated to counter the emerging threats. Therefore, to minimise the human-related problems and to improve the performance of preventive measures e-tailers may introduce a continuous education and training programme as advised by Arachchilage and Love (2014), Boss *et al*. (2015), Meinert (2016) and Seda (2014) for IT security, banking frauds and IDT. These awareness and training events have been proven instrumental in directing the staff efforts towards minimising human errors and advancing own skills helping them to achieve organisational objectives.

In line with the literature the study confirms that an authentication system is the first line of defence against IDFs. The system verifies the identity information and authorises the access to the customer account. The findings demonstrate that all the e-tailers have simple authentication process consisting of ID and a password. However, the e-tailers report that these accounts are sometimes hijacked with stolen credentials, which shows the limitations of their authentication systems.

The e-tailers are looking for new solutions. Firm C2, for example, is considering an authentication system that uses biometric information. Additionally, a two-layered authentication system is also an option, which is already being used by many banks, and various researchers (Prakash *et al.*, 2015; Sharma *et al.*, 2015; Teh *et al.*, 2016; Usman and Shah, 2013) have also suggested it for better authentication.

Table 5. 4 Suggestions for improvements of IDF prevention

Limitations of existing practices	Related to	Suggestions	Valid for
Fewer investments are made to create awareness among the staff for IDT prevention.	C1, C2 and C3	The e-tailers should be more focused on human aspects of IDT prevention and develop programs to increase their awareness to prevent IDT.	C1, C2 and C3
A third party organisation manages the prevention system, so its evaluation and update are also at its discretion.	C3	The firm should ensure the performance, update, and evaluation of prevention system either by its staff or hire the services of a neutral party.	C3
Educate customers on securing and regularly changing passwords.	C1, C2 and C3	Educate customers on possible IDT risks and countermeasures.	C1, C2 and C3
The e-tailers rely on third parties and the skills and knowledge of their staff.	C2 and C3	The e-tailers should have a team of experts to ensure that third party arrangements are best serving the objectives of IDT prevention.	C2 and C3
The e-tailers have simple authentication process, consisting of ID and a password.	C1, C2 and C3	The e-tailers should improve the authentication system by implementing bio-metric, login alerts or one-time password process.	C1, C2 and C3

This table highlights the limitations of existing managerial practices at the case forms. These suggestions are more related to focusing on the human aspects of prevention. The table portrays that e-tailers use more resources on acquisition of sophisticated technology, which is a good practice but literature findings reveal that skills and knowledge of staff is also significant to make the most of acquired technologies. Therefore, more emphasis is suggested for human aspects related to the secure use of technology and acquisition of skills and knowledge about the preventive technologies.

The literature findings show that bio-metric is the most secure authentication (Teh *et al.*, 2016; Usman and Shah, 2013) but it also has some legal implications and once compromised it is not possible to change. Furthermore, the e-tailers should also consider using a one-time password, whenever a customer wants to access the account. Such practice would help to stop unauthorised access, using stolen credentials. The one-time login password is sent to the registered contacts of the customers. As a result the customer is made aware of any unauthorised access to the account, and is also recommended by Bang *et al*. (2012).

E-tailers can also detect frauds at an earlier stage, by sending login alerts to the customers on their registered contacts (Kumar and Goyal, 2016). Such process already exists with some banks and other organisations. It may help to detect any unauthorised access soon after the victim gets the alert. Thus, the customer contacts the firm making it aware of the fraud. Detailed suggestions on improvements at prevention stage are mentioned in Table 5.4.

Although, additional preventive measures like bio-metric authentication, one-time password and sending login alerts may have some impact on effective authentication system, but these measures have not been tested in business sector. Now a days e-tailers operate in high competition, so they try to minimise the operating costs and increase the ease of online shopping. In the given situation, these measures may have some negative implications, if these are implemented on their own. Therefore, e-tailers may be suggested to test the measures as these have trade-off between better prevention and reduced ease of online business. These measures may also have financial implications, therefore e-tailers should study the benefits of implementing these measures against all the potential risks.

5.3.3 Detection of IDFs

Detection of IDFs is central to IDFM, as it supports other stages such as mitigation, analysis, policy, investigation and prosecution (Wilhelm, 2004). The outcomes of my research reveal that all the case firms have certain managerial practices that deal with identity fraud detection.

All the case firms have in place a screening system to detect frauds. This is in line with previous findings (Allan and Zhan, 2010; Carneiro *et al.*, 2017; Dorfleitner and Jahnes, 2014; Phua *et al.*, 2010; Swathi and Kalpana, 2013) on fraud detection in credit card industry, banking and non-banking financial industries and identity frauds in credit applications. It is apparent that screening system is widely used for detection of fraud in various sectors.

A screening system is an embodiment of anti-fraud rules. These rules reflect the nature of the item on sale, its value, alternative delivery address and other fraud trends based on the analysis of data from previous frauds such as IP addresses and devices used. The screening system flags out suspicious activities which are then manually verified during the mitigation stage.

The managerial practices for a screening process at all three organisations are similar except for the verification of newly opened account. Companies C1 and C2 verify the identity information on every new account application, but C3 does not have this practice. Not verifying the customer information at an earlier stage may lead to IDFs (application fraud), as some fraudsters open account with fictitious identities. To counter application frauds, C3 may adopt the process of verifying identity information before allowing them making any purchase.

In the course of this research it was also established that counter fraud rules tend to be regularly updated however, some frauds still evade detection. One of the possible reasons may be the reactive approach to updating these anti-fraud rules. The managerial practices from all firms confirm that anti-fraud rules are updated, based on the information from previous frauds, while it takes a long time to verify an identity fraud. In this regard, the case firms may take anticipatory measures and try to identify emerging fraud trends through information sharing and install precautionary rules into their screening system. It may help to detect emerging frauds even with no history of such scams.

The practice of regularly updating anti-fraud rules is also suggested by Allan and Zhan (2010), Carneiro *et al*. (2017), Dorfleitner and Jahnes (2014), Phua *et al*. (2010) and Swathi and Kalpana (2013) in relation to credit card fraud, loan fraud, IDF and other fraud detection in various industries. This shows that anticipatory approach of updating anti-fraud rules is significantly effective in detection of IDFs, which may be advised to the online retailers.

Because the performance of screening system is based on fraud analysts, so e-tailers should also focus on the enhancement of the skills and knowledge of the staff working with screening system. Such knowledge and skills have a significant impact on the efficiency of fraud detection system (Vahdati and Yasini, 2015). Therefore, in addition to focusing on the technologies e-tailers should also emphasise on the skills development of the staff dealing with the screening system. Managerial practices at the detection stage are presented in Table 5.5.

The study has revealed that firm C2 has the practice of verifying each application for a new account opening. It helps to detect any fraud using stolen or fictitious identity information at an earlier stage much before any fraud occurs. It also helps to discover duplicate applications. Firms C1 and C3 do not have such practice, which may result in confirmed fraud if stolen or engineered identity information is given at the time of account opening. Therefore, e-tailers especially, C1 and C3 may be suggested to verify each of the new account application manually, which will help in detecting any fraudulent account application. Also, to make it more useful, these firms may ask the suspicious applicants for any documentary proof, which can also be helpful in fraud detection in future (Amori, 2008). The detailed suggestions on improvements at detection stage are given in Table 5.6.

Table 5. 5 Comparing the cross-case managerial practices at the detection stage

Processes	Managerial Practices	C1	C2	C3
Fraud screening	- Every transaction is screened for fraud suspect	Yes	Yes	Yes
	- Fraud rules are implemented to flag out the suspicious frauds.	Yes	Yes	Yes
	- Odd items, expensive products and alternative delivery address orders are put out for manual verifications.	Yes	Yes	Yes
	- Data of previous frauds, such as email address, delivery and IP address etc. are also embedded into the screening system to detect any transaction having links to prior frauds.	Yes	Yes	Yes
	- Update the rules frequently to detect frauds with emerging trends.	Yes	Yes	Yes
	- Every new account application is manually verified.	Yes	Yes	No
Device recognition system	- Recognise customer IP address.	Yes	Yes	Yes
	- Recognise customer device.	Yes	Yes	Yes
	- Put cookies on to detect devices previously used in fraud.	Yes	Yes	Yes
	- Detect any device accessing multiple accounts.	Yes	No	Yes
	- Detect customers accessing with an unusual device.	Yes	No	Yes
Receiving customer complaints	- Receive customer complaints on identity frauds	Yes	Yes	Yes

The table above presents managerial practices for the detection of IDFs at each case firm. The processes and practices at each firm are similar in action so are the issues in IDFM. This suggests that large e-tailers have similar procedure implemented for detection of

IDFs. Therefore, the limitations regarding IDF detection are also similar, which are mentioned in the next table.

Table 5. 6 Suggestions for improvements of IDF detection

Limitations of existing practices	**Related to**	**Suggestions**	**Valid for**
In spite of fraud screening, some frauds are still not detected.	C1, C2 and C3	Focus on human skills and knowledge to develop more effective fraud rules.	C1, C2 and C3
Fraud rules are based on incurred frauds.	C1, C2 and C3	Be proactive and learn emerging trends to develop rules to detect IDFs with new patterns.	C1, C2 and C3
Fraud detection methods are not shared with other e-tailers.	C1, C2 and C3	Share information with other firms on the fraud rules to make the screening process more efficient.	C1, C2 and C3
Device recognition system for recognising the make and model of the device	C1, C2 and C3	Use intelligent system and get IMEI and MAC address of customers' devices.	C1, C2 and C3
Recognise customer IP address.	C1, C2 and C3	IP addresses may not be effective in public Wi-Fi, so link customer devices with their accounts.	C1, C2 and C3
Customers call and report identity frauds.	C1, C2 and C3	Provide free phone service to society for reporting any fraud or suspicious activity anonymously.	C1, C2 and C3

Table 5.6 presents the limitations of the practices implemented in the case firms for detection of IDFs. The suggestions forwarded in the table above are related to human aspects, knowledge sharing, customer education and technology related.

It was also revealed that all three firms were using the device recognition technology to detect devices or IP addressed previously involved in frauds. With the help of cookies, IP address and devices implicated in frauds are recognised and put into the system that identifies any transaction using them. The use of such technology in fraud detection is also advised by Al-Jumeily *et al*. (2015), Carneiro *et al*. (2017), Dorfleitner and Jahnes (2014), Swathi and Kalpana (2013) and many other researchers.

Additionally, C1 and C3 are also using it to detect devices accessing multiple accounts or a new device used to obtain a customer account, which helps to distinguish a suspected fraud but the C2 is not utilising that technology for such a purpose. The significance of using device recognition technology has already been highlighted by the C1. Therefore, C2 may be advised to use the device recognition technology to detect a new device accessing the customer account and the device accessing multiple account to make its IDF detection more effective. However, the results also suggest that information on the make and model of the device is sometimes not enough to detect frauds. Therefore, e-tailers may adopt more intelligent technology to register customers' devices with IMEI number and MAC address, which are unique to each device, where possible.

5.3.4 Mitigation of IDFs

The findings show that all the case firms have some practices related to the mitigation stage in IDFM. At this stage, these companies have the managerial practices concerning the verification of identity information of suspicious frauds, order reconfirmation, information sharing with other business firms about the confirmed frauds and victim support. The training of mitigation staff and practices related to dealing with compromised accounts are also a part of this stage.

The mitigation process starts once the screening system flags out a suspicious transaction. The results reveal that in the first instance, these firms verify the identity information of their customers. The verification processes is very similar in all three firms. At first, they check the information provided by the customer they suspect of fraudulent intentions against the historical data collected when the account was opened. It helps to identify recent changes to the account, which may be done by the fraudster soon after taking over the account, and any variations are validated.

The results also reveal that all three firms keep the record of historical data, which allows them to verify the suspicious updates of the accounts by contacting the customers using original contact details. Such process of verification is also advised by Cheng *et al*. (2015) and Tan *et al*. (2016) e-commerce and credit card IDFs. The findings from the extant literature also support for contacting the customers to verify the information on suspected frauds (Jamieson *et al.*, 2007; Wilhelm, 2004). This helps the firms in detecting any fraudulent attempt once the account has been taken over by fraudsters.

Findings also show that the e-tailers under study, also use the CIFAS database to check if that information has any link with previous frauds in member organisations. The findings also reveal that the case firms use BT people finder, electoral roll, mortality databases and credit files for identity verification. Such use of third party database for the confirmation of identity information is also recommended by Jamieson, *et al*. (2007) to manage IDF in banking and public sector organisations. These sources of verifications are critical to identifying any fraud using stolen information, as electoral roll may also help to locate other related information such as the address and other peoples living at the same address. But C2 and C3 are not using mortality databases, which may be a risk as the fraudsters can still use the credentials of deceased people. The detail of managerial practices at mitigation stage are presented in Table 5.7.

Table 5. 7 Comparing cross-case managerial practices at mitigation stage

Processes	Managerial Practices	C1	C2	C3
Verification of identity information	- Match information with previously given, at the time of account opening.	Yes	Yes	Yes
	- Check for updates on the customer account.	Yes	Yes	Yes
	- Use CIFAS database to check if previously involved in fraud.	Yes	Yes	Yes
	- Use BT people finder.	Yes	Yes	No
	- Verify through electoral roll for name and address.	Yes	Yes	Yes
	- Check mortality database for identity fraud.	Yes	No	No
	- Credit file checks for identity verifications.			
	- Call the customer and quiz on information on their credit file.	Yes	Yes	Yes
	- Verification of device	Yes	Yes	Yes
	- Ask customers to verify previous order and	Yes	Yes	Yes
	payments	Yes	Yes	Yes
	- Verification of Passport information	No	No	Yes
	- Identity information of each new account application is verified.	Yes	Yes	No
Order reconfirmation	- Reconfirm the high-value orders by calling the customers' on already given contact numbers.	Yes	Yes	Yes
Sharing information on identity frauds	- Develop a database of known fraudsters.	Yes	Yes	Yes
	- Share data on IDF with other firms.	Yes	Yes	Yes
	- Data on frauds is also shared with police and national crime agency.	Yes	Yes	Partially
Having a victim support system	- Give the victim a new account for continued shopping.	Yes	Yes	Yes
	- Remove the credit from the victim account.	Yes	Yes	Yes
	- Register the victim's information on CIFAS to prevent further fraud using that information.	Yes	Yes	Yes
	- Additional support is offered to IDF victims.	Yes	Yes	Yes
Mitigation Training	- Fraud analysts are given training on customer accounts.	Yes	Yes	Yes
	- They are trained to extract information from various sources for identity verifications.	Yes	Yes	Yes

	- Training is given on how to verify suspicious frauds.	Yes	Yes	Yes
	- Feedback training is given on wrong decisions	Yes	Yes	Yes
Dealing with compromised customer account	- Reject the order / stop the delivery.	Yes	Yes	Yes
	- Close the customer account if no loss has incurred.	Yes	Yes	Yes
	- Inform the account holder of being a victim of IDF.	Yes	Yes	Yes
	- Fraud amount is withdrawn from the victim account.	Yes	Yes	Yes
	- All compromised customers' accounts are closed.	No	Yes	Yes

Table 5.7 shows that for mitigation of IDFs all the case forms have implemented some processes and at each process they have multiple practices, which have similarities. A large number of processes and practices show that IDFs mitigation stage needs more focus and attention, because of its significance in deciding a transitions being a fraud or not. This stage is also critical as wrong decisions on suspected transactions have negative impact on the business operations and reputation.

C3 also has the practice of verifying the passport details if other sources would not help in determining the existence of a fraud. The practice of verifying the customer's identity through passport may yield better results compared to other forms of identification in unearthing any identity fraud. Considering the significance of passport verification in mitigating IDF, this study suggests that C1 and C2 may consider adopting this practice, after the cost benefit analysis, to enhance the effectiveness of mitigation.

Firms C1 and C2 have the practice of verifying the identity details on every new account application. It helps to mitigate any fraudulent account opened to make purchases and skip the payments, which is called application fraud. As discussed in the literature, these frauds are attempted with fictitious identities. Once a fraudulent account is opened, the verification of information upon the detection of suspicious activities would not bring results because the original record itself is compromised. Therefore, the verification of identity information at the account opening stage would minimise the chances of these frauds. In the absence of such practice, C3 may be at more risk of application fraud, so C3 is recommended to adopt the practice of verifying identity information on all new account applications.

Additionally, e-tailers may also ask the customers to provide any documentary proof of identity, after persuasion that it would help them to stop any identity fraud on their account. The practice of collecting any documentary evidence of identity is helpful in IDFs in health sector (Amori, 2008). Adopting this practice also be helpful in mitigating IDFs in e-tail sector, therefore, businesses may be advised to collect documentary proof of identity. Literature findings show that firms should collect customer information as minimum as possible, but such documents may only be collected for suspicious accounts, which would help in mitigating IDFs.

It was also confirmed that once identity information is verified, all the firms have the practice of reconfirming the orders by calling the customers and in some instances these orders are detected as fraud. This shows that suspected orders even with genuine information may be an account takeover fraud, which can be mitigated by calling the customers. It confirms that reconfirmation of suspected purchase orders is a significant practice to mitigate account takeover frauds, so e-tailers may be suggested to adopt it.

This study confirms that the case firms have developed a database of known fraudsters and share it with law enforcing agencies and other e-retailers through the CIFAS platform. The results make it evident that such practice helps in detection and mitigation of identity frauds. Information regarding the incurred frauds is fed into the screening system that highlights any transaction having link with the information in the database, which is also recommended by Cross and Blackshaw (2014) as significant to mitigate online frauds. Although, the sharing of information on frauds attempts helps, but benefits are limited to the detection and mitigation stages.

To maximise the advantages of information sharing, e-tailers should disclose relevant data on IDFM. Such information may be related to each stage suggesting various practices to manage IDFs more effectively (Feledi and Fenz, 2012). By contrast, Chohan *et al.* (2014) in a study on information theft prevention argue that organisations are reluctant to share information on IDFM, because of the lack of trust. Therefore, this research argues in favour of the e-tail organisations creating an atmosphere of trust and confidence to facilitate sharing successful practices and related achievements to develop a better IDF resistant environment.

Managerial practices at the victim support processes of all the firms are quite similar. On the confirmation of fraud, the credit is written off on the customer account, their information is fed into the CIFAS database to avoid further frauds at member organisations, and the credit history is restored. Furthermore, the victims are given a new account for continued business and suggestions are provided to avoid further losses in future. For business firms, victim support is critical to retain good customer relations. Although, these suggestions would help the victims to prevent any future IDF, but the benefits of such advises may be multiplied by forwarding these suggestions to more customers before any incident of IDF. The suggestions on the improvement in IDF mitigation are shown in Table 5.8.

Table 5. 8 Suggestions for improvements of IDF mitigation

Limitations of existing practices	**Related to**	**Suggestions**	**Valid for**
Match information with previously given, at the time of account opening.	C3	Information given by the customer at the time of account opening should be verified to detect any fraud after account takeover.	C3
Check mortality database for identity fraud.	C2 and C3	The database may not frequently be updated, so the e-tailers should not depend on these.	C2 and C3
No verification of identity information through the passport.	C1 and C2	Should implement passport information verification system	C1 and C2
ID information of each new account application is not verified	C3	Should verify information at the time of account opening to detect any account takeover fraud.	C3
Share data on IDFs with other firms	C1, C2 and C3	Companies should also share information on the effective management of IDFs.	C1, C2 and C3
Additional support is offered to IDF victims	C1, C2 and C3	Customers should also be advised to implement security software in their devices to prevent any IDT.	C1, C2 and C3
Mitigation staff is given training.	C1, C2 and C3	The e-tailers should also develop the specialities of mitigation staff in accordance with the types and nature of IDFs.	C1, C2 and C3
Close the compromised accounts with incurred losses.	C2 and C3	Keep the compromised accounts open with a view to getting the fraudster arrested and recover the losses.	C2 and C3

The table above presents the limitations of existing managerial practices at each case firm. Based on these limitations and reflections from the findings of extant literature improvements are suggested to e-tailers to enhance the effectiveness of mitigation stage.

Training has a critical role in improving the skills and knowledge of the members of staff responsible for the mitigation stage, accordingly, determining the ultimate success of this stage. The analysis reveals that all the investigated firms train their staff in two phases. First, an induction training is offered to enhance the employees' skills in fraud mitigation, which is compulsory for all newcomers. During the second phase a mamber of staff undertakes controlled fraud analysis of her own.

The decisions taken by the analysts are evaluated and the staff is given feedback that help them to improve the quality of her decisions. Although, such retrospective training is useful, to enhance the performance of mitigation staff, it is important that they should also be trained on new and emerging fraud trends. The staff may be educated in dealing efficiently with red-flagged transactions and how to minimise contacts with customers that may have a negative impact on customers' attitude towards the e-tailers.

The benefits of such training to fraud analysts are also highlighted by Becker *et al*. (2010) and Wilhelm (2004) in mortgage, insurance, retail banking and telecommunication industries. Furthermore, it may also be helpful to e-tailers to develop the capabilities of mitigation staff by the types and nature of IDFs.

The findings show that on the confirmation of an IDF the order is cancelled, and the process of despatch or delivery of the item is stopped. The compromised account with no losses incurred is closed, and the information is fed into the fraud database to prevent any fraud in future. In case of incurred losses on any account, C1 keeps the account open to get the fraudster arrested if another fraud is attempted, while C2 and C3 close such accounts.

Although, for a business enterprise it may not be a cost-effective practice, however, for the recovery of significant losses, the other companies may also follow C1. Using a compromised account as a trap, may help to catch the identity fraudsters and recover the losses.

5.3.5 Analysis of IDFs

The process of IDF analysis helps to identify the causes and effects of frauds, and provides a foundation for adopting more efficient managerial practices. The process includes fraud risk assessment, identification of fraud trends, diagnosing the methods and patterns of frauds and exposing the weaknesses of the prevention and detection system (Aple and Nagin, 2017; Rose *et al.*, 2015).

The findings reveal that the case companies have hired external professionals or have employed experienced and senior staff members from within the firm as fraud analysts. Thus, firm C1 has hired experienced fraud analysts from retired staff of HM Revenue and Customs, the police and other investigational agencies. Once hired they are then given training in firm-specific procedures and technologies. While, C2 and C3 have the practice of employing senior personnel having vast experience in various fraud-related fields within the firms.

Although, the practice of employing fraud analysts in the case firms vary, yet no significant differences were found in the effectiveness of identity fraud analysis. Therefore it may be assumed that experience related to fraud management is essential whether gained from within the organisation or from other law enforcing agencies. These fraud analysts receive information from the previous stage on incurred frauds and start a reviewing process. They try to understand the means, methods and trends of attempted frauds.

Based on the outcomes of their investigations, the analysts forward suggestions and countermeasures to improve the defence line against such frauds. The practices of staying informed about the fraud trends and methods are also advised by Apel and Nagin (2017) and Yelland (2013) for help in improving fraud management in IT security and mobile network frauds.

The findings also show that the process of reviewing the frauds is nearly same in all three firms. The information of the fraudsters/victims and the delivery addresses are collected and a database is built to prevent any fraud in the future, using that identity information. The case organisations also have the practice of sharing the database of known fraudsters with the CIFAS, to enable the member organisations avoiding frauds using such information. Thus, the practices of developing a database of notorious fraudsters and sharing it, are critical to help and get helped to prevent certain IDFs using the same information.

The identification of new fraud methods and trends from various external sources have a significant role in setting the organisational stance against detection and mitigation of such frauds. The respondents from C2 confirmed that the staff members in the fraud management field actively seek information on new IDF trends and methods through external resources. It helps C2 to assume the anticipatory practices to detect and mitigate such frauds, which the C1 and C3 are lacking.

The staff at the C2 also have the practice of communicating such IDF trends and methods within the IDFM team. To help in detection and mitigation of IDFs with emerging trends and techniques, C1 and C3 may adopt the practices of learning new frauds trends and ways from various sources external to the firms and share such information with related staff. The existing managerial practices in fraud analysis in the case firms are presented in Table 5.9.

The findings reveal that the process of reviewing the IDFs helps the case organisations in discovering the weaknesses of technology employed to detection identity frauds and the performance of the staff involved in mitigation of IDFs. All the case firms have the practices of updating the existing fraud rules and developing new ones, based on the outcomes of the analysis process. The fraud analysts recommend these rules to the management of screening system, and they implement them to detect suspicious frauds with emerging frauds trends.

The findings also show that all the case organisations have the practice of communicating these new and emerging fraud trends to the staff related to the detection and mitigation processes. Thus, the process of reviewing IDFs helps the businesses to enhance their detection and mitigation mechanism against IDFs. Such process of fraud analysis is also suggested by Apel and Nagin (2017), Rose *et al*. (2015) and Yelland (2013) to develop anti-fraud strategies.

The managerial practices of case organisations for identity fraud analysis are compared in the following table.

Table 5. 9 Comparing cross-case managerial practices at the analysis stage

Processes	Managerial Practices	C1	C2	C3
Hiring experienced fraud analysts	- Hire or employee well-experienced personnel for fraud analysis.	Yes	Yes	Yes
Reviewing identity frauds	- Disclose the trends and methods of frauds.	Yes	Yes	Yes
	- Collect identity information regarding the fraudsters and delivery addresses.	Yes	Yes	Yes
	- Diagnose the weaknesses of systems and staff at previous stages.	Yes	Yes	Yes
	- Suggest fraud rules –based on occurred frauds- to detect such scams in future.	Yes	Yes	Yes
	- Communicate the new fraud trends and countermeasures to related staff members.	Yes	Yes	Yes
Put identity fraud on management priority	- Hold regular meetings on identity fraud to improve its management.	Yes	Yes	No
	- Monitor the progress of existing prosecutions.	Yes	Yes	No
	- IDF issues are reported to the senior management.	Yes	Yes	No
Manage IDF risks	- Understand the potential risk of identity theft.	Yes	Yes	Yes
	- Take measures to minimise the fraud risks.	Yes	Yes	Yes
	- The business is still losing on IDFs.	Yes	Yes	Yes
	- Focus on balancing the customer ease and stopping frauds.	No	No	Yes
Evaluation of prevention and detection systems	- Validate all the control systems by related security policies.	Yes	Yes	Yes
	- Check for any policy violations, investigate these and take remedial actions.	Yes	Yes	Yes
	- Run vulnerability scanning of the prevention systems, website, access portals and firewalls on a regular basis.	Yes	Yes	No
	- The screening system is regularly evaluated to assess its effectiveness in IDF domain.	No	No	No
Performance measurement of mitigation staff	- Evaluate the performance of mitigation staff through their decisions.	Yes	Yes	No
	- Make plans for individual staff to develop their performance.	Yes	Yes	Yes
	- Feedback training is given based on the decisions of fraud advisors	Yes	Yes	No
Learning fraud trends from external sources	- Fraud advisors actively learn new fraud trends from external sources.	No	Yes	No
	- New frauds trends and methods are shared with related staff.	No	Yes	No

The table above presents the processes for IDF analysis, which are common to all the case firms. For each process the table presents the list of managerial practices adopted by these firms. Like at other stages, managerial practices for IDF analysis are similar at all the case organisations.

The findings show that C1 and C2 hold regular meetings in which the management of IDFs is discussed. These sessions are attended by senior management, and issues and the organisational strategies are debated and reviewed to achieve better management of IDFs. These meetings help to evaluate the overall IDFM process and to explain the situation to the top management to get their input, including extra resources if needed. The practices of involving the senior management is also advised by Jamieson *et al*. (2007) and Wilhelm (2004), to improve the performance of fraud management process.

The results from C1 and C2 show that the practices of holding regular meetings regarding the management of IDFs and putting the issue on top management are advantageous, but C3 has no such practices, which may result in lack of interest from top managers. This may lead to a shortfall of resources, which again would result in ineffective management of IDFs. Therefore, this study recommends the e-tailers, especially C3, to put IDFM issues on priority and get the senior management contribution, which may help it improving the management of IDFs.

This study found no evidence on the evaluation of the performance of each stage of IDFM in the case firms. Such practice is critical to improving the overall management of IDFs, but no data has been found indicating the existence of such evaluation practices. The significance of evaluating and improving each stage of fraud management is also highlighted by Jamieson *et al*. (2007) and Wilhelm (2004), for the improvement of IDFM.

The evaluation process is helpful in identifying the limitations and weaknesses of employed technologies, processes and human deficiencies, and based on this, management of enterprises may develop strategies to overcome these deficiencies. Therefore, it may be suggested to e-tailers for evaluating the performance of technology, processes and peoples at each stage of IDFM and plan strategies to overcome the deficiencies to improve IDFM process. The detailed suggestions on improving managerial practices in IDFM are presented in Table 5.10.

All the firms have the process of managing the risks related to IDFs. It starts with understanding the risks of IDT. In this regards, the findings show that these firms are aware of the risks associated with IDFs, which creates a sense of insecurity. To minimise these risks, all the case companies take technological and organisational measures, which also help to reduce the chances of IDFs. The representatives from all the firms confirmed that in spite of the arrangements, these firms are still losing on IDFs, which proves that there is still a room for improvements in managerial practices in IDFM.

Business organisations always seek to make it easier for their customer to shop online. It was confirmed that un-necessary security checks and verifications may put a negative impact on the customers buying behaviour. The analysis show that firms with dispensable security layers and un-necessary verifications could irritate customers, so there should be a balance between security and ease of doing online business.

The findings on C3 show that the firm is trying to have a favourable trade-off between its counter-fraud operations and the negative impacts of undue security on the business. On the contrary, the interviewees at C1 and C2 have not shown any concern regarding such trade-off, which may put adverse impact on their existing and potential customers. C1 and C2 are business firms operating in a high competitive environment, so they may be suggested to focus on the trade-off between the security layers and customer ease of doing business. Better customer education can help the case firms adopt extra security layers to stop IDFs, once the customers are informed of the potential risks of IDFs. Therefore, e-tailers may still have added security layers without adverse impact on their customers through better customer education and awareness.

The practice of evaluating the efficiency of the prevention and screening systems is crucial for effective IDFM. It helps to assess the effectiveness of these measures against the potential risks of identity theft and frauds, and suggests measures for improvements. The findings show that the case firms validate all the control system regularly in accordance with established information security policies.

The results disclose that C1 and C2 have the practice of evaluating the prevention system through vulnerability scanning on the website, access portals and firewalls on a regular basis. Such scanning allows to identify the system’s weakness and improve their effectiveness in IDT domain, but no such process was seen in C3. The absence of such practice may lead prevalence of severe risks, which may lead to data breach and identity theft. Implementing the process of evaluating the effectiveness of prevention system against possible threats would help to improve its performamnce, so e-tailers may be advised to evaluate the prevention system in related domain (Dorminey *et al.*, 2012; Seda, 2014; Vahdati and Yasini, 2015).

The absence of such evaluation practice may lead to the system weaknesses, which may be a possible reason for IDF occurrences in all the case companies. Some researchers, (Apel and Nagin, 2017; Bierstaker *et al.*, 2006; Rose *et al.*, 2015) have also proposed to evalute the detection system for enhanced detection of frauds. Thus, evaluation of detection system in IDFs domain may result in reduced number of IDFs, so e-tailers are advised to evalute their detection system to controll the number of successful IDFs. The detailed suggestions on improving fraud analysis are presented in Table 5.10.

Table 5. 10 Suggestions for improvements of IDF analysis

Limitations of existing practices	Related to	Suggestions	Valid for
External sources are not utilised to understand emerging fraud patterns.	C1 and C3	Utilise media channels to gain information on emerging frauds and share with related staff.	C1 and C3
Ease of online shopping is not focused while making IDT prevention strategies.	C1 and C2	Focus on balancing the customer ease and preventing IDT.	C1 and C2
The vulnerability of prevention systems is not tested.	C3	Run vulnerability scanning of the prevention systems and firewalls regularly.	C3
Fraud screening system should regularly be evaluated in IDF domain.	C1, C2 and C3	Screening system should regularly be evaluated, to assess its effectiveness in IDF domain.	C1, C2 and C3
Performance of mitigation staff is not evaluated by their decisions.	C3	Evaluate the performance of mitigation staff through their decisions.	C3
Mitigation staff is not given feedback training on their decisions.	C3	Feedback training should be given, based on the decisions of fraud advisors.	C3
Fraud trends and methods are learnt only through the analysis of incurred frauds.	C1 and C3	Fraud advisors should also actively learn new IDF methods and trends from external sources.	C1 and C3
Suggest fraud rules –based on occurred frauds- to detect those in future.	C1 and C3	Fraud rules should also be suggested based on trends learned through various external sources	C1 and C3
IDFM performance is not evaluated.	C1, C2 and C3	Evaluate the performance of each stage of IDFM	C1, C2 and C3
Personal development plans are designed for every staff members.	C1, C2 and C3	Development plans of IDFM staff should be designed to enhance their expertise in specific doman.	C1, C2 and C3

Table 5.10 presents the limitations of existing managerial practices at IDF analysis stage for each firm. This shows that the e-tailers have the process of analysing IDFs, but is not meant for evaluating the performance of technologies and the processes at each stage of the framework, which is signified in the extant literature. The findings expose that the decisions of mitigation staff are also analysed at this stage. The results from C1 and C2 confirm that the analysis stage also include the evaluation of the performance of mitigation staff through their decisions. These decisions are evaluated against the actual occurrences of IDFs. The analysts give feedback to the mitigation staff on their decisions regarding the approval of fraudulent transactions or rejection of genuine orders.

Evaluation of screening system for the detection of suspicious frauds is also help to improve its performance. Despite this, no significant results were found to evaluate the performance of the screening system. The findings express that the case firms just asses the screening system when a new fraud rule is implemented or updated. Although, at the start of applying a fraud rule, the system is checked for its effectiveness, but this does not quantify the overall performance of the system.

Keeping in view the significance of these decisions, C1 and C2 have the practice of feedback training to the mitigation staff. Such training helps them to know their weaknesses and provide opportunities to improve their performance. It is a cyclic process that enhances the quality of decisions to minimise the risk of losing business and mitigating IDFs. These results are in line with Vahdati and Yasini (2015) in online frauds. Keeping in view the advantages of such practices, e-tailers, (especially C3) are advised to implement the practices of evaluating the performance of mitigation staff and providing them feedback training.

In addition to the feedback training, all the case firms have the regular plans for the development of staff including those in mitigation stage. Such plans help the personal development of individual staff members. This study suggests that e-tailers should design specific development plans for staff in the DIFM domain to develop their expertise.

5.3.6 Policy for IDFs

Business firms develop policies to manage various business operations effectively. The policies provide guidelines to the staff, regarding the fulfilment of day to day job obligations in a systematic and strategical manner to achieve organisational goals. In

IDFM, policies have a critical role in determining the course of actions against the frauds. The results expose that all the enterprises have implemented policies but are limited to identity theft prevention.

Generally, all the businesses have policies to secure the information from theft and system hacking. Mostly, these policies are related to information security, communication security and infrastructure security. Furthermore, the findings indicate that all the case firms have similar arrangements to secure their information. Although, these policies are significant to prevent any information theft, which is used for IDFs, but they focus on only one stage of IDFM - prevention. However, for effective IDFM businesses need policies at each stage of fraud management, which are missing at all the e-tail firms. The need for anti-fraud policies is highlighted by Bierstaker *et al*. (2006) and wright (2007) for better fraud management.

The absence of policies at other stages of fraud management leaves weaknesses in the process of IDFM. It also shows that the firms are more focused on the prevention of information theft, which may be one of the valid reasons for a significant number of successful frauds. In the absence of a set of comprehensive policies at each stage of IDFM, there is a lack of strategic actions against the fraud activities, which may allow some frauds to happen. This situation also creates confusion for the staff in dealing with issues related to the fraud management. Therefore, it is advised that all the firms should develop a set of policies for each stage of the fraud management (Njenga and Osiemo, 2013).

In addition to having appropriate policies, their communication and awareness are also important. The findings disclose that all the firms have made their policies available to their staff members through the internal communication system. The readily available policy documents are helpful to the staff for getting guidance in case of any confusion. In addition, the case organisations have the practice of sending policy updates through email in order to make the staff aware of the changes in existing policies. This practice helps the staff to get up to date with these changes. The practice of making the staff aware of policies is also suggested by Parsons *et al*. (2014) for better IT security, so it may also be applied in e-tailing. Managerial practices of each firm at the policy stage are mentioned in Table 5.11.

Table 5. 11 Comparing cross-case managerial practices at the policy stage

Processes	Managerial Practices	C1	C2	C3
Having fraud management policies	- Have information and technology security policies - Have IDFM related policies at each stage. - Every policy is reviewed annually	Yes No Yes	Yes No Yes	Yes No Yes
Policy awareness	- E-learning packages are developed to help the staff learn about the contents of policies and understand them. - All the policies are available in the internal communication system. - New and updated policies are communicated effectively. - Policy awareness and understanding is acknowledged.	Yes Yes Yes No	Yes Yes Yes No	No Yes Yes No
Data access management policies	- Staff should have least access to personal information. - Only job-related information is allowed to access. - Assessment of data access privilege.	Yes Yes Six Monthly	Yes Yes Annual	Yes Yes Annual
Policy compliance	- A mechanism to for policy compliance. - Internally audit the policy compliance. - Invite external experts for compliance audit.	Yes Yes Yes	No Yes Yes	No Yes Yes

Table 5.11 presents the processes and practices on IDFM policies at each case firm. Managerial practices for policy awareness and compliance are also given. This shows that a comprehensive set of IDFM polices guiding at each stage of fraud management is missing in all the case firm, for which suggestions are given in the next table.

The findings also show that C1 and C2 have an online learning system that helps the staff to get access on any policy contents. This practice is essential to let the employee learn about the policies and interpret them to comply with. C3 lacks such a learning system, which may result in the policies been not readily available and may lead to non-compliance with the policies. Ready availability of policies is necessary to direct the staff responses in accordance with the organisational objectives, therefore, e-tailers may consider developing a policy learning system to help their employees getting ready access on policies for effective compliance.

Furthermore, this investigation has confirmed that the firms just make the policy documents available. Although, it’s a good practice to enable the staff access any policy document regardless of the time, but this research has reveal that the case firms do not have any mechanism to ensure that these documents are read and properly understood by the staff members. Lack of policy understanding is one of the biggest obstacles towards policy compliance. Therefore, these e-tailers may be suggested to arrange a feedback mechanism, to ensure that each staff member read and understand the related policies. Additionally, the firms should also develop a training programme to create policy awareness, understanding and learning compliance process and develop a positive attitude of staff, which would result in better compliance (Parsons *et al.*, 2014; Singh *et al.*, 2013; Soomro *et al.*, 2016). Detailed suggestions on policies and related issues are mentioned in Table 5.12.

Table 5. 12 Suggestions for improvements of IDFM policies

Limitations of existing practices	**Related to**	**Suggestions**	**Valid for**
Policies are limited to the information security.	C1, C2 and C3	The case firms should develop policies at each stage of IDFM.	C1, C2 and C3
Data access privilege is evaluated annually.	C2 and C3	The data access privilege should be assessed more frequently.	C2 and C3
Policy compliance is ensured only through an audit.	C2 and C3	Develop a mechanism for policy compliance.	C2 and C3
Policies are made available only on the firm's database	C3	Develop a learning package to make staff aware of policies.	C3
Policies are annually reviewed.	C1, C2 and C3	Fraud related policies should be updated continuously to counter emerging challenges.	C1, C2 and C3

Table 5.12 gives the limitations of existing managerial practices at the each case firm. This portrays that e-tailers have no set of comprehensive policies on IDFM to direct the behaviour of staff at each stage of fraud management. On the other hand, mechanism on policy awareness and compliance also has some critical limitations, for which suggestion are given in the table.

The findings also reveal that the case firms review their policies on an annual basis. However, this may not be often enough to effectively counter the IDF challenges, so e-tailers may adopt the practice of continuously updating their IDFM policies for better response to IDF issues. This would also help in ensuring the better countermeasures against the emerging fraud trends and methods.

The case firms hold sensitive information related to vast number of customers. To secure such information from external challenges, prevention measures may be adopted, and policies related to the minimum standards of information security would helpful if implemented.

In addition to external challenges, the firms also have threats from the insiders. To minimise these risks, the case organisations have least access policies to data access. They allow only minimum access of their staff to sensitive information in regard to customers and the organisation itself. Staff members are given access to information which is essential to disposing of their duties. This helps to minimise the chances of internal data theft. It was also established that in C2 and C3 data access privileges are assessed on an annual basis, which is not frequent enough and may leave compromised data access privileges undetected for some time. For this reason, C2 and C3 may be advised to assess the access privileges more frequently like it is done in C1, in which they do it every six months. Additionally, e-tailers are also advised to review data access privileges, once any change in the position of the staff members takes place (Alrashed, 2016; Wang *et al.*, 2006).

For the management of IDFs, the significance of policy compliance is as important as the policy itself. The respondents indicated that all the case firms have the practice of internal and external audit for the policy compliance. Such audits help the top management ensuring that the laid down policies are properly complied with, which may support achieving organisational goals.

However, to ensure the policy compliance in real time C1 may need to develop a mechanism through which the immediate supervisors ensure that the policies are complied with, without waiting for an audit. Such practice helps to closely monitor the compliance process and correct any errors and weaknesses of staff about the policy understanding and compliance procedures. Such mechanism may also help to enhance the staff performance for compliance through training and awareness. The practices of closely monitoring the compliance process and having compliance mechanism are also highlighted by Chen *et al*. (2015) and Parsons *et al*. (2014) for IT security policy compliance. For effective IDFM, C2 and C3 may be advised to develop a policy compliance mechanism, to ensure policy compliance in a timely manner.

5.3.7 Investigation of IDFs

The findings confirm that the investigation of IDFs takes place at all the e-tailers under study. The investigation process starts with the reports from the analysis stage and includes various procedures and practices to collect the evidence and submit the cases for prosecution. Therefore, it was confirmed that the investigation stage is also a part of IDFM. The practice of conducting investigations at the business end is also recommended by Brooks and Button (2011) and Lewis *et al*. (2014) to reduce the dependency on police force and develop close coordination with law enforcing agencies.

For effective investigations, a team of professional investigators is necessary, with a sound knowledge of working in the field. The results demonstrate that the e-tailers investigate IDFS at their end, so they have devoted staff members to perform investigations. These investigation teams consist of specialist investigators, such as ex-police as in C1 and C2, who are given firm-specific training to retrieve digital evidence from the firms' systems. C3 has a team comprising of senior and experienced fraud managers with sound knowledge of state laws and investigation procedures.

Although, there is a difference in the composition of the investigation teams, this study does not reveal any significant variation in the success rate between the teams. Therefore, it may be deduced that employing ex-police or experienced civilian staff for IDF investigations does not affect performance, given that they possess sound knowledge of related state laws and investigation procedures. The suggestion on appointing a team of experts for fraud investigations is also advised by Amori (2008) to reduce burden on police force and collect evidence for prosecution.

It has been found that the fraud investigators directly engage with the law enforcing agencies in the course of preparing cases, collecting additional evidence and forwarding it for the prosecution process. It reduces the business dependency on law enforcing agencies, thus developing better coordination, which lessens the police role (Lewis *et al.*, 2014).

Nevertheless, the purpose of investigating the IDFs is to collect information on the involved fraudsters and evidence to prove their guilt, the benefits would be limited if the investigations are not conducted with the prosecution in mind. Through analysis, it came to know that all the case firms seek to prosecute most of the fraudsters. These firms collect and preserve evidence in such a way that it is suitable to be presented in the courts of law, which is also recommended by Furlan and Bajec (2008) and Rose *et al*. (2015) for effective prosecution. Managerial practices at the investigation stage are presented in Table 5.13.

Table 5. 13 Comparing cross-case managerial practices at the investigation stage

Processes	Managerial Practices	C1	C2	C3
Employing specialist investigators	- Establish a dedicated investigation team. - Investigators are experienced in related fields. - Investigation team consist of ex-police officers. - Investigators directly engage with law enforcing agencies and have the experience to work with police. - Train investigators on firm-specific digital systems.	Yes Yes Yes Yes Yes	Yes Yes Yes Yes Yes	Yes Yes Yes Yes Yes
Investigate with prosecution in mind	- Investigations are conducted to collect the evidence and fulfil the legal requirements to prosecute the fraudsters.	Yes	Yes	Yes
Collection of evidence	- Collect as many as evidence to prove fraud. - Use external databases for collecting evidence. - Collect digital evidence including IP address, device identification and related addresses. - Use GPS system to identify the location of delivery. - Use social media to collect more identity information of the suspects. - With all the evidence prepare a case for the onward process. - Record the victim's statement confirming the occurring of an IDF.	Yes Yes Yes Yes Yes Yes Yes	Yes Yes Yes Yes Yes Yes No	Yes Yes Yes Yes Yes Yes Yes
Report fraud cases to police	- Report fraud cases to the police with all the evidence. - Work with police for further investigations to reduce the police role.	Yes Yes	Yes Yes	Yes Yes
Catching the fraudsters	- Help the police to arrest the fraudsters. - A controlled delivery system to catch the fraudsters on the spot.	Yes Yes	Yes Yes	Yes No

The above table lists managerial practices for IDF investigations at each case organisation. This shows that the case firms have specialist investigators that collect the evidence, liaise with the police and follow up the fraud cases in the courts of law. The table represents that investigational process at all the case firms have similarities with a minor difference of adopted practices.

The findings reveal that the e-tailers use internal and external sources to collect evidence to prove a fraudster's guilt. For internal evidence collection, all the firms use technologies to identify the IP address, recognise the device used in fraud, and GPS location service to determine the exact location of the goods delivery. Information collected through internal systems help the e-tailers to match this information with previously used addresses and location of the victims. Furthermore, this information also helps to identify and locate fraudsters and may stand as evidence in the court of law.

In addition to the internal sources, the e-tailers also use external sources of information for evidence collection. It was known that the case firms use various external databases (such as electoral roll, IP address locator and others) to collect evidence related to the fraudster and the delivery addresses. These e-tailers also use social media to obtain information on the fraudsters and their activities.

The data reveal these external sources of information help to identify the fraudster and gather evidence. Although, the e-tailers are using these sources, the validity is questionable as the fraudsters may not give their actual details in social media accounts, whilst external databases may not be updated frequently enough. Therefore, these e-tailers are advised to use external sources very carefully and try to get evidence from robust databases for more authenticate information. The use of both the internal and external sources for evidence collection is similarly advised by Cross and Blackshaw (2014) and Wilhelm (2004) in collection of evidence and verification of personal information.

The results demonstrate that C1 and C3 get victim statements to prove the occurrence of an IDF. For prosecution, it is necessary to establish that a fraud has taken place. Therefore, both organisations have the practice of getting an evidential statement from the victim and preparing the case. However, C2 does not take such statements, leaving it to the police.

As already mentioned in the literate, the police force has less focus on small frauds so leaving some jobs on the police may cause lack of coordination, which will negatively affect the firms standing against these frauds. It is therefore, suggested to the e-tailers to take the initiative, collect evidential statements and complete investigations to minimise police involvement. These practices are also forwarded by Amori (2008), Cross and Blackshaw (2014) and Lewis *et al*. (2014) for enhanced role of private firms and better coordination among the business firms and law enforcing agencies. It may also enhance the firms' capabilities in fraud investigations and quick processing of fraud cases.

The findings reveal that after collecting some evidence, the fraud cases are reported to the police for further processing. It was also confirmed that it was the discretion of senior staff members to take fraud case to the police. These decisions are mostly based on the amount of frauds and collected evidence. It was also reported that sometimes these case are not advanced by the police especially when the goods are not delivered, or a small amount is involved. In this regards, the extant literature (see Table 2.10) recommends firms to organise effective investigations at the business end and develop coordination with the police force. Therefore, e-tailers need to be more involved in private investigations, and supporting and minimising the role of the police, to process fraud cases for prosecution. The detailed suggestion for improving the investigation stage are presented in Table 5.14.

Table 5. 14 Suggestions for improvements of IDF investigations

Limitations of existing practices	**Related to**	**Suggestions**	**Valid for**
Use only internal systems for collecting evidence.	C3	The firm should also use external sources (such as electoral roll, people and property finder 192, IP address locator and other) for evidence collection. Should also use social media for getting more evidence.	C3
Does not get statements from the victims of IDF.	C2	Get victim's statement, confirming the IDF as required by the law.	C2
Do not do controlled deliveries to catch the fraudsters.	C3	Adopt a controlled delivery process to catch the fraudsters.	C3
Sometimes police are not ready for controlled delivery.	C1 and C2	Improve the system to minimise the police role and saving their resources.	C1, C2 and C3
Sometimes these case are not entertained by the police.	C1, C2 and C3	Improve investigation process to enhance the police cooperation.	C1, C2 and C3
Decisions on reporting the fraud case are mostly based on the number of frauds and collected evidence.	C1, C2 and C3	Improve the investigations process and prepare the fraud cases more effectively to enhance their acceptability and effectiveness of successful prosecutions.	C1, C2 and C3

This table presents the limitations in the existing practices on investigation. These firms are given some suggestions to improve their practices at IDF investigations, which are mainly related to conduct the investigations at the firm end and reduce the dependency on the police, which may improve their position for better IDFM.

It was also revealed that after the collection of sufficient evidence, and identification of fraudsters, these companies supply these to the local police and try to get them arrested to initiate the prosecution. Therefore, findings confirm that investigations conducted to collect evidence are critical for the arrest and prosecution of the fraudsters. Catching and prosecuting fraudsters have deterrent impact on IDFs, so e-tailers may be suggested to improve the investigation process for sufficient evidence and maximise the chances of police involvement and arrest of the fraudsters.

Additionally, C1 and C2 have the practice of catching the fraudsters through a controlled delivery system. After confirming a fraudulent attempt, these firms coordinate with police, and once the delivery is accepted, the police catch the fraudsters red-handed. The controlled delivery system is an important method of catching fraudsters and providing prosecution with sufficient evidence. C3 and other e-tailers may improve their standing against the fraudsters by adopting the practice of controlled delivery process.

However, the results also reveal that in some instances the police force is reluctant to take action on the grounds, such as the involvement of smaller amount the loss was small and it was possibe to stop the delivery, thus incurring no loss. In this regard, the firms should improve its controlled delivery system to minimise the police role and saving the resources of the police force, which may enhance their motivation to be involved in such process.

5.3.8 Prosecution of IDFs

In IDFM prosecution plays an important role. To begin with, it helps with the recovery of losses. In addition, a successful prosecution gives a warning to potential fraudsters. The results demonstrate that all the case firms are involved in the prosecution of IDFs, which confirms that the prosecution stage is also observed as a part of IDFM. Therefore, these firms investigate at their end, collect evidence and prepare the case to submit to the police for prosecution. The police do not always accept and process fraud cases for prosecution. According to the respondents, this happens when the monetary value involved is small or when the police lack technology or resources to investigate.

The results also reveal that the police forces are more focused on other critical issues, so small fraud cases are of less interest to them. To resolve these problems, the e-tailers should be more involved in investigations and prepare the cases that need the least efforts from the police while developing close coordination with them in dealing with the cases of fraud as is also advised by Gogolin and Jones (2010).

For effective prosecution, it was found that these firms have the practice of following the fraud case in the courts of law. These firms send their representatives to the courts to pursue the cases and help the courts by responding to the queries and providing additional information and evidence if required, which is in line with the recommendations of Lewis *et al*. (2014) and Monaghan (2010).

Furthermore, these authors also advise private firms to be involved in prosecution process and initiate the prosecution privately, which may reduce the dependency on the police. In this case e-tailers would be able to prosecute any fraud case irrespective of the amount involved or resources required to process it. This practice would enhance the rate of prosecutions, which in results would improve the position of e-tailers against IDFs.

The results reveal that the C1 publicises the arrests and successful prosecutions in the media, which may have a deterrent effect on identity fraudsters, but the C2 and C3 do not do this. The respondents from C2 and C3 expressed the opinion that publicising such information may put a scare off their potential customers.

This contradicts the view held by authors suchas Dorminey *et al*. (2012), Ijeoma and Aronu (2013) and Sperdea *et al*. (2011) who recommend to publicise such cases to send a clear message to criminals as a deterrent that the firms are determined to have them caught and punished. In this regard, the C2 and C3 may be advised to focus on the contents of the text and tone of message to make it more favourable showing e-tailers strategic standing against fraudsters and a sense of security for their customers.

Therefore, tactical information on arrests and prosecutions would put a positive impact on their customers for being secure while dealing with these firms, and simultaneously a threat to the potential fraudsters. Based on the above discussion the conceptual framework is presented below.

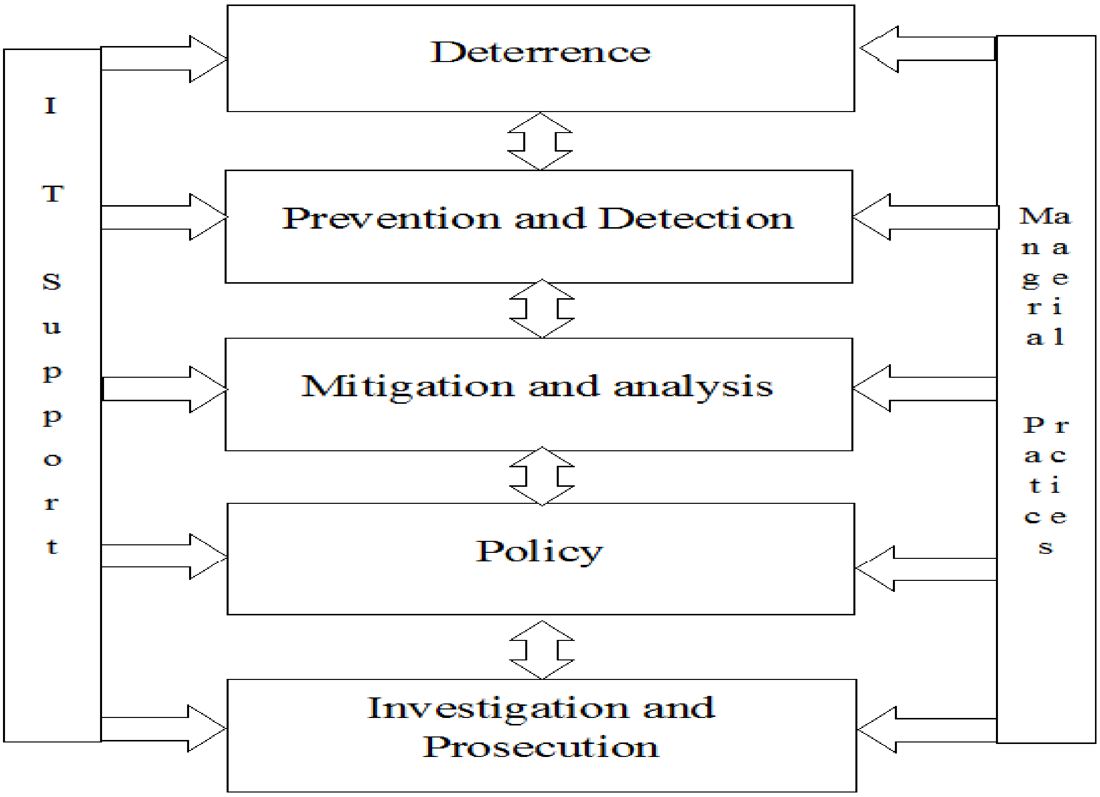

Figure 5. 1 A Conceptual Framework for Management of Identity Fraud.

The conceptual framework represents the significance of managerial practices and IT support for the management of identity fraud in e-tail sector. The framework contains eight stages for effective identity fraud management encompassing organisational, social and technological aspects. Some of these stages are kept in same box because of the similar nature of managerial practices and close inter-connections between them. The arrows show the connections and flow of support and communication between the stages of framework and support elements.

Summary of the Chapter

This chapter presented a cross-case analysis of the results from three e-tailers and discussed the effectiveness of existing practices and suggested improvements and some additional practices to improve IDFM. At first, the types and methods of prevailing identity frauds at e-tail firms were presented, and was confirmed that similar types of identity frauds are faced by the large e-tailers based in the UK.

In the next section, the framework extension is detailed and managerial practices at each stage of the framework were compared across the three e-tailers and the extant literature.

Starting from the first stage, managerial practices at each stage were discussed in details for their effectiveness. The weaknesses of existing managerial practices were discussed, and guidelines are recommended to improve these practices. This study also found that the e-tailers are not giving appropriate and balanced focus on the stages of fraud management, so practices were suggested to enhance e-tailers focus on some stages to improve the impact of IDFM.

CHAPTER 6
CONTRIBUTION TO PRACTICE AND KNOWLEDGE AND CONCLUSIONS

6.1 Contribution of this Study

The literature shows that online frauds have become a significant challenge for e-tailers. IDFs make more than 60% of total online frauds (CIFAS, 2018b). The literature reveals that e-tailers fall victim of the greatest share of these identity frauds. Although, the extant literature has some studies on online frauds, previous studies are mostly focused on banking and non-banking financial institutions, and public sector organisations. In the absence of any significant research on IDFM in e-tail sector, these business firms are facing various financial and reputational challenges.

At the outset, present study contributes to the literature by investigating the types of IDFs faced by large e-tailers. This study confirmed that the types of IDFs faced by e-tailers in the UK are similar to those, found in other industries through the literature. Additionally a novel type of IDF was found, which was termed as delivery fraud. In this type of fraud the delivery driver does not handover the parcel but fraudulently sign as delivered.

This study is unique in its nature as no previous research has investigated managerial practices in IDFM. Hence it’s the novel contribution of this study that it provides new insights into IDFM practices. This research also contributes by exploring IDFM practices in real world setting at large e-tail firms and offers suggestions for improvements. This research tried to understand IDFM, its process and explored practices adopted by large e-tail firms and identified the limitations and weaknesses based on the reflections from literature findings. The suggestions forwarded by this study advance the state of the art in managing IDFs a step ahead, which provides foundation for future studies in current domain. Synthesising the empirical data, additional managerial practices are also added to the body of knowledge.

The fraud management lifecycle framework (Wilhelm, (2004), has also been extended in IDFM in e-tailing. The framework was used as underpinning to base the research and get help in data collection. The framework was also helpful in developing the research instrument as the questions were based on each stage of the framework. Observing the flexibility of the framework, this study forwards that it may also be used and extended in various contexts. Finally, a conceptual framework has been suggested in IDFM domain in e-tail industry, such extension is detailed in the next section.

Furthermore, present research offers suggestions for improvements in IDFM. E-tailers are also advised to put IDFs as the top management priority to gain their attention and focus in the management of frauds. Additionally, this study contributed to the real world by forwarding e-tail firms guidelines to improve the existing managerial practices. Reflecting on the theoretical and empirical data e-tailers are suggested a comprehensive set of managerial practices at each stage of fraud management, which are briefed in section 6.1.3.

6.1.1 The Theoretical Contribution - Explanation of Conceptual Framework and Design Method

The major frameworks discussed in the literature have been studied in the context of e-tailing and reviewed for their suitability as discussed in section 2.7 of this thesis. The fraud management lifecycle framework, suggested by Wilhelm (2004) was selected to as under-pinning framework to design a conceptual framework for improvements in IDFM in the e-tail sector. Originally, the framework was developed for the management of various types of frauds in communication, mortgage and credit card industries. The framework consists of eight stages: deterrence, prevention, detection, mitigation, analysis, policy, investigation and prosecution. These are described in detail in chapter two, section 2.7.5.

This fruad management lifecycle framework (Wilhelm, 2004) has already been adopted and extended by various researchers, such as Amasiatu (2016), Jamieson et al. (2007), Kumar et al. (2007) and Njenga and Osiemo (2013) in relation to first-party fraud, enterprise IDT, organisational collaboration and risk performance respectively. The characteristics of the framework and the criteria for their selection have already been explained in detail in chapter two. Furthermore, the framework has never been extended to an e-tail context, so its extension adds value to the literature and practice.

This study has suggested a conceptual framework for managing identity frauds in e-tail sector. The framework is based on empirical findings of this research. It is given a new shape based on its functionality. As per the confirmation of the significance of each stage of the framework, no stage has been removed, but some stages are put together based on similar practices and close interactions. The framework is designed to its functions. It suggests managerial practices for each stage, while IT support is set as support for each stage. Therefore, stages of fraud management are put in-between two horizons i.e. IT support and managerial practices.

The deterrence stage is put on the top, because it comes before any other IDFM activity. At the next down, prevention and detection stages are put together on the bases of similar nature of managerial practices at both the stages. At this point, the purpose of managerial practices is to stop any fraud attempt prior to occurrence, or to detect any attempted fraud. After that, flow down the mitigation and analysis stages. The objectives at this stage are to minimise the extent of fraud and know the causes and consequences of such frauds in order to prevent these in future. The policy stage comes below them, as the analysis stage provides grounds to design effective IDFM policies. The exploration of the limitations of the systems, managerial practices and risk analysis gives a sound base for the development of effective policies. Finally, investigation and prosecution stages are put together confirming their relevance. Both the stages are linked together, as without investigations, effective prosecution in not possible and standalone investigations may not worth doing.

The stages of fraud management, IT support and managerial practices are linked together with the help of arrows. Such linkages enable the flow of information from one to another stage and also facilitates sequential as well as simultaneous functioning of the stages. The links among the stages also facilitate the design of IDFM policies; as an outcome of analysis process and the flow of policy guidelines is further communicated through IT support and managerial practices. The detailed managerial practices at each stage are explained in chapter five. These stages are also interconnected for better performance. This study also farwarded that each stage at IDFM may be given an appropriate focus in all aspects of fraud management.

This research investigated the applicability of the processes and practices at each stage of the framework to e-tailing, relying on the synthesis of the original empirical data and the analysis of the extant literature. The conceptual framework creates a foundation for recommendation on how to evaluate the success of various aspects of fraud management. This will also help to improve managerial practices, so that they meet the emerging challenges related to the management of IDFs. The framework also focuses on the human aspects of IDFM not adequately addressed in previous studies. The empirical results point at a lack of focus on staff training and awareness, and on customer education among e-tailers.

Finally, the framework helped to analyse the managerial practices of e-tailers at each stage of IDFM. The collected evidence made it possible to highlight the limitations of existing practices and suggest improvements, as well as recommend some additional practices in the conceptual framework (see section 5.3). Recommendations regarding managerial practices at each stage of IDFM and conceptual framework in e-tail context constitute the novelty element of this research, which contributes to the existing body of knowledge and opens many avenues for future research.

6.1.2 Contribution to the Practice of E-tailing

In addition to the literature, this study also contributes significantly to the real world of e-tailing. Three large e-tailers have been investigated for the management of IDFs, which have never been done before. These investigations have helped to understand the identity fraud issues and analysing managerial practices in detail. The managerial practices and organisational actions and strategies were analysed, their limitations were exposed, and suggestions were given to improve IDFM**.**

To reflect the existing practices, the fraud management framework by Wilhelm (2004) has been extended. The modified framework offers detailed procedures and managerial practices at each stage of IDFM. Firstly, the extended framework helps e-tailers to understand what constitutes IDFM. Secondly, analysis of managerial practices at each stage of the framework provides guidance to e-tailers on how to adopt better practices and improve the existing ones. E-tailers are also suggested to evaluate the performance of each stage. The practice of evaluating the technology, process and performance of related staff would help e-tailers to understand the weaknesses in IDFM. Based on these evaluations and the recommendations of this study, the businesses may improve their response to IDFs.

The case organisations were given feedback reports based on individual results. In these reports, each firm was given a detailed understanding of their existing practices, their weaknesses and suggestions and guidelines were forwarded on how to improve their management of IDFs. In addition, these firms were also provided with an anonymised cross-case report to help them expand their understandings of IDFM and to adopt better managerial practices. Finally, the outcomes of the present research will assist the e-tail sector in controlling IDF losses and retaining better customer relationship. Summarised recommendations and guidelines for each stage of IDFM are given below.

6.1.3 Recommendations to E-tailers for Better IDFM

This study helps e-tailers to confront successfully the challenge of IDF through better management of IDF. It was established that these firms are losing significant amount of financial resources every year. These losses may be curtailed at each stage of the extended framework if e-tailers implement the recommendations that follow.

For a better deterrence, e-tailers should educate their customers and create fear among potential fraudsters. For customer education, active means of communication should be adopted. Customer education should focus on creating awareness of IDFs. Customers should be educated about possible countermeasures to IDFs. In order to create the fear of being caught and punished in fraudsters, e-tailers should make public organisational arrangements employed to catch fraudsters.

Arrests and successful prosecution should be publicised in such a way that such publicity should not make any negative impression on potential customers. To achieve this firms should check the contents and the tone of the messages they send out. E-tailers should also inform the public about their actions and standing against the fraudsters. Additionally, e-tailers should assure their customers that their personal information is safe with them, to enhance their trust.

The prevention of information theft is a critical aspect of IDFM. In this regard, most organisations employ the services of third party firms. Although, outsourcing may be beneficial, e-tailers should ensure the proper application of prevention technologies in the IDT prevention domain. The e-tailers should also evaluate the performance of prevention systems. Third parties may be hired to do the checking. Information sharing on effective measures of IDT prevention will also enhance the effectiveness of the preventive measures. Human aspects should be prioritised, as the majority of information breaches are the results of human mistake or ignorance.

Accordingly, e-tailers should have a comprehensive programme to promote IDT prevention awareness. The IT professionals should be trained continuously to stay abreast with emerging technologies and to ensure that third party provide up to date services that meet the firm's objectives. For effective authentication of customers' accounts, firms should either adopt the practice of sending login alerts or send a one-time password to the customers.

Identity fraud detection has a significant impact on stopping the frauds and enhancing the firm's resistance against fraudsters. In this regards, e-tailers should implement a fraud screening system that is not limited to the reflections on past frauds, but is capable of detecting new types of frauds and emerging fraudulent trends. For that, e-tailer should actively seek knowledge on new IDF trends through media and from other firms. Additionally, the performance of fraud screening should be evaluated regularly in the context of the emerging fraud trends.

Mitigation is a critical stage in the verification of identity information and locating identity frauds. It follows from this research that for effective mitigation e-tailers may use various sources of identity verification. These businesses may collect any documentary proof of identification at the time of account opening that would be helpful in ID verification in future transactions. The mitigation staff should be given feedback training on their decisions to improve the quality of their decisions. Thus, it would help to increase the chances of IDF detection, and releasing the genuine purchase orders. Additionally, customers may also be advised to regularly check their credit card and bank transactions to detect any IDF at an earlier stage.

Fraud analysis should not be limited to calculating the financial impact of these frauds. Managerial practices at this stage should be aimed at diagnosing the weaknesses of technologies, processes and procedures and human aspects of failure. A detailed report on each fraud should be circulated among the related staff and arrangements should be made to overcome those weaknesses. The analysis process should also evaluate the performance of other stages of fraud management and feedback should be given to enhancing their effectiveness.

The anti-fraud policies have a critical impact on the management of IDFs; these may help to direct the staff actions toward the ideal manners, so maintaining a detailed set of policies for each stage of IDFM may be advised. Detailed policies should also be established for the deployment of anti-fraud technologies and especially access management policy should be designed to control internal fraud. IDFM policies should be communicated effectively to ensure that each member of staff is familiar with these policies and can comply with. A sound compliance procedure should be executed by immediate supervisors. Furthermore, IDFM policies should be evaluated regularly and frequently in response to emerging challenges so that timely updates take place.

Investigation and prosecution are essential stages in IDFM. In this regards, e-tailers should ensure appropriate investigations at their end, as police force may not necessarily show interest in such frauds. To enhance cooperation with the police, e-tailers should privately investigate the frauds, collect and preserve evidence and prepare the case for prosecution in accordance with the laws of the state. The firms may also be suggested to pursue the prosecution process in the courts of law to defend their position and to recover the damages and getting the fraudsters punished.

6.2 Conclusions

Online frauds have been a big challenge for e-tailers. The dominant share in these scams is contributed by manipulations with the identity of customers. These frauds result in substantial financial losses and reputational damages to e-tailers thus creating a significant obstacle to e-commerce. With advancements in technology, the means and methods of online fraud are also evolving. Although, online identity frauds have been investigated by scholars, most of the studies are limited in scope. So far no study has offered a comprehensive picture of identity fraud management in e-tail context. The absence of such studies resulted in continuous growth in the instances of fraud and associated losses. This research has set itself the objective of helping e-tailers to improve IDFM through empirical investigation.

This study has provided a comprehemsive understanding of managerial practices in IDFM in large e-tail organisations and used analysis to suggest improvements and guidelines for better IDFM. The starting point for the investigation was a thorough review of the extant literature in order to set the boundaries of this research and explore the depth and breadth of the literature addressing the current issue. The review has revealed that most of research in identity frauds addresses financial businesses and public sector organisations, and mostly focuses on the technological aspects of identity fraud. The position of this researcher, however, is that better management of IDFs needs a comprehensive approach incorporating the human, organisational and technological aspects of IDFM.

For a comprehensive study on IDFM the literature was examined to find an appropriate framework, comprehensively addressing various aspects of fraud management. A number of frameworks were evaluated (see section 2.7), based on the selection criteria established in section 2.7.1. The fraud management lifecycle framework proposed by Wilhelm (2004) was found to be the most appropriate one to attain the objectives of this study.

This study used a qualitative method involving a multiple case study. The data was collected from three large UK based e-tailers. For data collection, semi-structured interview were used. In all, 33 face-to-face interviews were conducted with respondents representing various fields and levels of management. The interview recordings were transcribed, and Nvivo software was used to organise the data. The results from the cases were analysed individually, followed by a cross-case analysis for lateral replication. These results were analysed and suggestions were provided in reflections with the extant literature.

The findings revealed that IDFs is one of the biggest challenges for the case e-tailers and these firms are losing a significant amount of their revenues due to fraud. Various types and methods of IDFs were explored at each retailer and were comparatively analysed. It was also known that the e-tailers were less interested in identifying the types and methods of frauds, especially IDFs, which may lead to some weaknesses in fraud management.

All the case firms had the process of managing identity frauds, and all the stages of fraud management, suggested by Wilhelm (2004) were prevalent. The results also revealed that these firms had nearly similar managerial practices for IDFM. It was also found that similar to cases described in the extant literature, these companies prioritised the technological aspects of IDFM at the expense of developing the skills and awareness of their staff, which may be one of the possible reasons for the existing deficiencies of fraud management. In fact, this study has found that the human factor is a critical aspect of IDFM. Also it has been established that customer education was not carried out efficiently and IDT mostly occurs at the customer side. However, the e-tailers are to deal with customers in a highly competitive environment, so there is a trade-off between putting extra security layers and the ease of purchasing. Such a trade-off makes the identity fraud management more challenging for the e-tailers.

On this basis, the study recommends the e-tailers to adopt a strategy that focuses on human, organisational and technological aspects to faciltate better managerial practices in IDFM. An appropriate emphasis should be given to each stage of the framework and a comprehensive set of IDFM policies should be developed, updated regularly and compliance should be ensured. Customer education may be improved to build trust between clients and e-tailers helping them to cooperate in preventing any IDT. The breadth and depth of information sharing, with customers, other business firms, law enforcing agencies and related organisations may be increased to include sharing the best practices at each stage of IDFM. It would help the whole industry and the customers to minimise the risks of online shopping.

The managerial practices for the evaluation of each stage of IDFM are also suggested in this study to diagnose the weaknesses of existing processes and practices and to improve the overall IDFM. Finally, this research extended the fraud management framework in identity fraud management and managerial practices at each stage were suggested, and guidelines were given to make the framework effective for IDFM. Thus, the outlined objectives of this study were achieved.

6.2.1 Research Objective 1. To explore identity fraud types and methods facing the e-tail sector.

To achieve the aim of this study, various types of identity fraud faced by e-tailers were described and analysed. It was found that not all types of IDFs mentioned in the literature were present in the case firms. The particular types of frauds faced by each company are specified in the results section dedicated to each case and are further discussed in section 5.2. The data reveal that the e-tailers do not pay sufficient attention to the identification of the types and methods of IDFs, which may result in the lack of proper countermeasures for certain categories of fraud.

6.2.2 Research Objective 2. To investigate the existing managerial practices of IDFM in e-tail sector.

The managerial practices at each stage of the IDFM were investigated in detail through semi-structured interviews conducted at three large UK e-tailers. These practices were discussed in sections 4.3, 4.4 and 4.5. Furthermore, they have also been cross-compared in section 5.3. The data show that the three e-tailers have IDFM comprised of eight stages. It was also revealed that the e-tailers do not always treat these stages with necessary attention, which provides for some weaknesses in IDFM. It has been found that all three e-tailers do not have in place a set of comprehensive policies for IDFM.

Furthermore, the data reveal that the human factor is not given due attention which may also add to the ineffectiveness of fraud management. Finally, customer education has a certain weakness, as only passive channels are used for communication and advice is limited to the recommendation of the continual change of the password. However, customers are not educated on possible other methods of IDFs and available counter measures to minimise the account takeover frauds, the leading form of IDF.

6.2.3 Research Objective 3. To extend the fraud management lifecycle framework (Wilhelm, 2004) for improving managerial practices in IDFM in e-tail sector.

In this dissertation the fraud management framework, suggested by Wilhelm (2004) was adopted to IDFM in the e-tail sector. Various managerial practices have been suggested at each stage of the framework as well as guidelines aimed at improving the existing practices. The framework is extended on the basis of the results obtained, and some novel practices are developed. The conceptual framework is summarised in the next section.

6.2.4 The Extended Framework

The conceptual framework comprises the same eight stages, namely deterrence, prevention, detection, mitigation, analysis, policy, investigation and prosecution. These stages can work both in linear and network forms as already suggested by Wilhelm (2004). The framework has been suggested based on the empirical results. It has been designed to illustrate its functionality. Stages with similar nature of managerial practices and close interactions have been kept together. IT support throughout the stages has also been illustrated to signify its importance. The detailed design process has been explained in section 6.1.1 and the picture of the framework is given as figure 5.1. A summary of managerial practices at each stage of IDFM is given below.

a) Deterrence

For effective deterrence, customer education and creating of fear among fraudsters are critical. To advance customer education e-tailers should use active channels of communication and make them aware of countermeasures to IDT. For creating the fear of being caught and punished, e-tailers should use mass media. However, to avoid any negative impact on the public opinioin, especially the potential customers, the tone and context of the message should be designed in such a way that it presented the firm's strategy against fraudsters in a positive way and ensured confidence in business dealings.

b) Prevention

Prevention is a crucial stage in securing the integrity of critical information related to the customers and the firm. It is related more to the technological arrangements, but attention should be given to the appropriate deployments of these technologies in reflections of the challenges of IDT. The human factor should not be neglected either as the performance of any technology depends on the expertise of the people who use it. The authentication system should be made more effective by the use of advanced technologies. Information security should be enhanced, and data access policy should be implemented and log of who accessed what information should be maintained.

c) Detection

Earlier detection of IDFs is necessary to limit fraud losses. For IDF detection e-tailers should have a fraud screening system based on fraud cues and data mining. Intelligent fraud cues should be implemented and information from various sources ought to be utilised for designing useful fraud cues. These fraud cues should also reflect the IDF methods and types. The extent of the information sharing may be extended to get help developing more effective fraud cues.

d) Mitigation

Real-time mitigation is necessary for e-tailers as online transactions ought to be processed very quickly. At this stage, the identity of suspicious transactions need to be verified through various databases. These databases may include the electoral roll, credit history and mortality register.

The social media can be used as well. A telephone conversation is the most useful mode of quizing the identity of the customer. The human aspect here is critical as the decisions of whether it is a fraud or not lies with staff dealing with them. To increase staff competence a comprehensive training program should be designed. Additionally, feedback training should be organised to improve the performance of mitigation staff**.**

e) Analysis

This stage helps to determine fraud types and methods detected after the occurrence. The analysis process also helps to identify the weakness of the managerial practices performed at the detection and mitigation stages. Such feedback on the shortcomings in managerial practices helps to enhance fraud detection and mitigation and suggests improvements in managerial practices. At this stage, the financial impact of these frauds is calculated, and foundations for further investigations and prosecution are provided. The fraud analysis process may also help in designing better IDFM policies.

f) Policy

Policies provide guidelines to carry out day to day business operations. For an efficient IDFM, e-tailers should have a comprehensive set of policies at each stage of fraud management. Effective channels should be used for policy communication, and it should be ensured that each staff member reads and understands related policy documents. The policies should be reviewed and regularly updated to meet the emerging challenges of IDFs. Finally, there should be a compliance mechanism to ensure that each member of staff performs her duties in accordance with the policy guidelines. Additionally, internal and external audits should be conducted to evaluate the policy compliance**.**

g) Investigations

For effective investigations, e-tailers should have a team of experts to conduct inquiries at the business end. Investigators should have sound knowledge of related state laws. The law enforcing agencies are focused on critical issues. They show little or no interest in IDF investigations. Private investigations reduce the role of the police and also help to develop close coordination with them thus, better investigations of IDFs are achieved. The e-tailers should collect and preserve all the traditional and digital evidence in accordance with the state laws. The investigators should also prepare the fraud cases that are complete and ready to be filed for prosecution**.**

h) Prosecution

The prosecution is a critical stage in IDFM. It offers multiple advantages to e-tailers. The benefits are not limited to the recovery of losses but can also be used as a deterrent. Therefore, e-tailers should try to prosecute every fraudster, for which,enough evidence is collected. E-tailers should also follow-up the prosecution process and investigational staff should represent the firm in the courts of law. The successful prosecutions should be publicised as deterrence strategy.

6.2.5 A summary of the Key Findings of this Research

This research was carried out to understand IDFM and analyse the managerial practices in IDFM at large UK e-tail organisations. The study has produced some significant results that would help to improve IDFM in e-tailing. At the outset, it was found that the e-tailers are less focused on identifying the types and methods of IDFs. In the absence of such information, managerial practices in IDFM remain less effective. Therefore, the e-tailers should take steps to identify the types and methods of IDFs, which will help them to adopt better practices to manage these frauds.

This research established that the stages of fraud management framework proposed by Wilhelm (2004) were prevalent in the e-tail firms but were not linked in a holistic way for IDFM. Additionally, it was found that these stages of fraud management are not given proper attention, resulting in weaker arrangements at some stages, which may be one of the reasons for the weaknesses in IDFM.

At the deterrence stage, it was found that the e-tailers have the process of customer education but is limited, which is not significantly contributing to the effectiveness of IDFM. On the issue of creating fear among the potential fraudsters, contrary results were found as two firms had that practice of creating fear, while one business was reluctant, for the reasons of negative impact of the firm on the society.

This research also found that e-tailers are more focused on the technological aspects of IDFM and less on the organisational and human factors, which may be contributing to the persistence of frauds occurrence. The prevention system also has some limitations as the authentication process allows the access customer account with stolen information, which was a big challenge for these firms. To counter this challenge, better managerial practices can be adopted to introduce an additional layer of security. Practices at the fraud detection stage are reactionary, which may be improved by considering various sources of information on the types and methods of IDFs.

Similar to customer education, the e-tailers also have the practice of sharing information with other firms. However, such information is limited to data on incurred frauds, which limits the benefits of learning from the experiences of others.

It was also established that none of the three e-tailers has policies on IDFM, which weakened fraud management significantly. The few existing policies, which every e-tailers had, were limited to information security at the prevention stage. The absence of policies at other stages may be seen as a major limitation of an effective IDFM. Furthermore, weaknesses were also found in policy communication, awareness and the compliance methods.

Finally, some flaws were also found in IDF investigation and prosecution procedures. The investigations carried out at the business end had some limitations, which resulted in lack of coordination from the police. In such a situation resources spent on analysis and investigations were wasted, thus multiplying the fraud losses.

Last but not least, it was found that all the e-tailers have sound IT security systems and have invested generously in the technology. Therefore, no significant data breach or any other incident has been reported. However, the organisational and human aspects of IDFM require more focus.

6.2.6 Research Limitations and Suggestions for Future Work

Like every other research, this study has certain limitations.

This study is based on only three online retailers and based on replication logic. So these results may not be generalizable to the whole e-tail sector. Therefore, research based on wider number of e-tailers is required to verify the generalisability of this research.

A qualitative research approach was adopted, with 33 interviews from three e-tailers. To overcome the limitations of this approach, more studies based on quantitative survey approach and covering a greater number of respondents is needed.

This study was based on examples from a developed country; Business norms, organisational culture, buying behaviour of customer and economic conditions in developing countries may vary. Therefore additional research is suggested to cover diverse aspects of emerging economies. Additionally, the data regulations and cyber laws may also vary from country to country. It is therefore proposed to conduct more research, encompassing the mentioned aspects.

In this study, the data were collected from large e-tailers, however, there may be some variations based on the size of the business. Therefore, more research is needed to include medium and small e-tailers, to understand differences related to the firm size in the effective management of IDFs.

All the e-tailers under study are credit lending firms that allow customers open accounts and use credit for a specified period. It is possible that non-credit lending e-tailers may have a different situation. Therefore, more research is needed to study the impacts of advance payment methods on the challenges of IDFM.

This research was more focused on the managerial aspects; further studies may be initiated analysing the technological and human aspects in depth.

Appendices

Appendix 1. The Research Questionnaire

Evaluating the managerial practices in identity fraud management in e-tail organisations UK

Case study research questionnaire

Block 01: Introduction

Questions	Related Questions
1. What is area of your responsibility?	i. Job title ii. Length of service
2. What is your role in identity (ID) fraud management domain?	i. Level of management.

Block 02: Deterrence

Questions	Related Questions
1. What do you do to deter ID frauds in your organisation?	i. What managerial practices (i.e customer education, security awareness, threat etc.) are helpful to deter ID related frauds?
2. What other practices you think will help in developing effective deterrence?	

Block 03: Prevention

Questions	Related Questions
1. How do you prevent ID frauds?	i. How is it effective?
2. How do you support the IT professionals to develop an effective ID fraud prevention system?	ii.
3. Do you audit to ensure effectiveness of control systems for ID fraud prevention?	i. How can ID fraud prevention system be improved?

Block 04: Detection

Questions	Related Questions
1. What system do you have to detect the ID frauds?	i. How effective is the detection system? ii. How do you measure the effectiveness of detection system?
2. How do you deal with any suspicious ID fraud attempt?	iii. Does everyone know about his/her responsibility and reporting line regarding ID fraud detection?

Block 05: Mitigation

Questions	Related Questions
1. How do you mitigate the fraudulent transactions?	i. How effective is the process?

2. Do you think that you are given enough authority to deal with mitigation matters?	ii. Do you believe that delegation of more powers will be helpful in this regard?
3. How can the mitigation system be improved?	

Block 06: Analysis

Questions	Related Questions
1. How do you analyse the ID related frauds?	
2. What managerial practices (like, hiring of special professionals, provision of resources, technological tools, etc.) do you use in ID fraud analysis?	i. How are these practices helpful?
3. How do you use analysts' report/recommendations for effective ID fraud management?	i. How does the management support to implement the analysts' suggestions?
4. How can the analysis process be improved?	i. What the management can do to support the analysts?

Block 07: Policy

Questions	Related Questions
1. Do you have a ID fraud management policy?	i. If yes, how effective is it? ii. If no, do you think such a policy would be helpful? How?
2. How do you communicate the policy?	i. How do you ensure the policy compliance?
3. What managerial practices (such as supervisory support, training, awareness, communication etc.) are helpful in policy compliance?	i. How do you promote a policy compliance culture in your organisation?
4. How do you ensure coordination and cooperation among various departments for effective policy development and compliance?	i. What other factors you believe would be helpful for a successful policy?

Block 08: Investigation & Prosecution

Questions	Related Questions
1. What process you have to investigate and prosecute an ID fraud?	i. How effective is the process to recover the losses and deter the ID frauds?
2. How do you work with the law enforcing agencies regarding ID fraud investigation and prosecution?	ii. How are these links helpful? iii. How can the working relationship be improved in ID fraud management dimension?
3. How can investigation system be improved?	i. What do you suggest to improve the prosecution system on your part?

Block 09: General

Questions	Related Questions
1. How do you do the online business?	i. How is it effective in ID fraud management?
2. Are there trainings for ID fraud awareness and policy compliance in your organisation?	i. Do you need more trainings and awareness to manage ID frauds?
3. What special rewards are there for effective ID fraud management?	i. How can the reward system be improved?
4. What channels do you use for communication within and outside the organisation?	
5. Whether centralised or decentralised decision system you have in ID fraud management?	i. How is it effective than the other one?
6. What other practices you think will be helpful in ID fraud management?	i. At what level ID fraud issues are dealt in your organisation?
7. Do you share any information about ID fraud management with colleagues and other teams?	i. How is the information sharing helpful in ID fraud management?

Appendix 2. Research Publications

Soomro, Z.A., Ahmed, J., Muhammad, R., Hayes, D. and Shah, M.H. (2017) 'Critical success factors in implementing an e-rostering system in a healthcare organisation', *Health services management research*, pp. 0951484817745695. doi: (Available online at: http://journals.sagepub.com/doi/abs/10.1177/0951484817745695).

Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016) 'Information security management needs more holistic approach: A literature review', *International Journal of Information Management*, **36**(2), pp. 215-225.

Shah, M.H., Ahmed, J. and **Soomro, Z.A**. (2016). 'Investigating the Identity Theft Prevention Strategies in M-Commerce.'. International Conferences on Internet Technologies & Society (ITS), Melbourne, Australia, 59-66.

References

Ahamad, S.S., Sastry, V., Udgata, S.K. and Nair, M. (2014) *A Secure and Reliable Mobile Banking Framework.* ICT and Critical Infrastructure: Proceedings of the 48th Annual Convention of Computer Society of India, Andhra Pradesh, India. 13-15 December.

Akers, R.L. (2013) *Criminological theories: Introduction and evaluation.* Abingdon Oxan, Routledge, Taylor & Francis Group.

Alanezi, F. and Brooks, L. (2014) *Combatting Online Fraud in Saudi Arabia Using General Deterrence Theory (GDT), .* 20th Americas conference on information systems, Savannah, Georgia, USA,. August 7-9.

Albrecht, C., Albrecht, C. and Tzafrir, S. (2011) 'How to protect and minimize consumer risk to identity theft', *Journal of Financial Crime,* **18**(4), pp. 405-414.

Albrechtsen, E. and Hovden, J. (2010) 'Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study', *Computers & Security,* **29**(4), pp. 432-445.

Al-Jumeily, D., Hussain, A., MacDermott, Á, Tawfik, H., Seeckts, G. and Lunn, J. (2015) *The Development of Fraud Detection Systems for Detection of Potentially Fraudulent Applications.* International Conference on Developments of E-Systems Engineering (DeSE), Dubai, UAE. 13-14 December.

Allan, T. and Zhan, J. (2010) *Towards Fraud Detection Methodologies.* 5th International Conference on Future Information Technology (FutureTech), Busan, Korea (South). 21-23 May.

Alonso-Paulí, E. and Pérez-Castrillo, D. (2012) 'Codes of Best Practice in competitive markets for managers', *Economic Theory,* **49**(1), pp. 113-141.

Alrashed, F. (2016) 'Stealing More than Just Identity', *International Journal of Scientific & Engineering Research,* **7**(2), pp. 422-426.

Amasiatu, C.V. (2016) *Framework for managing first party fraud in e-tailing: a case stuty of the UK retail sector.* PhD. University of Central Lancashire, UK.

Amasiatu, C.V. and Shah, M.H. (2018) 'First party fraud management: framework for the retail industry', *International Journal of Retail & Distribution Management,* **46**(4), pp. 350-363.

Amori, G. (2008) 'Preventing and responding to medical identity theft', *Journal of Healthcare Risk Management,* **28**(2), pp. 33-42.

Ann McGee, J. and Ralph Byington, J. (2015) 'Corporate identity theft: A growing risk', *Journal of Corporate Accounting & Finance,* **26**(5), pp. 37-40.

Apel, R. and Nagin, D. S. (2017) *Perceptual Deterrence.* New York, USA, Oxford University Press.

Arachchilage, N.A.G. and Love, S. (2014) 'Security awareness of computer users: A phishing threat avoidance perspective', *Computers in Human Behavior,* **38**(September), pp. 304-312.

Ates, A., Garengo, P., Cocca, P. and Bititci, U. (2013) 'The development of SME managerial practice for effective performance management', *Journal of Small Business and Enterprise Development,* **20**(1), pp. 28-54.

Atkinson, P. (2015) *For ethnography.* London, UK, Sage publications ltd.

Baer, M.H. (2008) 'Linkage and the Deterrence of Corporate Fraud', *Virginia Law Review,* **94**(6), pp. 1295-1365.

Bai, F. and Chen, X. (2013) 'Analysis on the new types and countermeasures of credit card fraud in mainland China', *Journal of Financial Crime,* **20**(3), pp. 267-271.

Bang, Y., Lee, D., Bae, Y. and Ahn, J. (2012) 'Improving information security management: An analysis of ID–password usage and a new login vulnerability measure', *International Journal of Information Management,* **32**(5), pp. 409-418.

Baz, R., Samsudin, R.S. and Che-Ahmad, A. (2017) 'The Role of Internal Control and Information Sharing in Preventing Fraud in the Saudi Banks', *Journal of Accounting and Financial Management,* **3**(1), pp. 7-13.

Bechtsoudis, A. and Sklavos, N. (2012) 'Aiming at higher network security through extensive penetration tests', *IEEE Latin America Transactions,* **10**(3), pp. 1752-1756.

Becker, R.A., Volinsky, C. and Wilks, A.R. (2010) 'Fraud detection in telecommunications: History and lessons learned', *Technometrics,* **52**(1), pp. 20-33.

Benbasat, I. and Zmud, R.W. (1999) 'Empirical research in information systems: the practice of relevance', *MIS quarterly,* **23**(1), pp. 3-16.

Bierstaker, J.L., Brody, R.G. and Pacini, C. (2006) 'Accountants' perceptions regarding fraud detection and prevention methods', *Managerial Auditing Journal,* **21**(5), pp. 520-535.

Bishop, T.J.,F. (2004) 'Preventing, Deterring, and Detecting Fraud: What Works and What Doesn't', *Journal of Investment Compliance (Euromoney),* **5**(2), pp. 120-127.

Blaikie, N. (2007) *Approaches to social enquiry: Advancing knowledge.* 2nd edn. Cambridge, UK, Polity Press.

Bloom, N. and Van Reenen, J. (2007) 'Measuring and Explaining Management Practices Across Firms and Countries', *Quarterly Journal of Economics,* **122**(4), pp. 1351-1408.

Bloor, M. and Wood, F. (2006) *Keywords in qualitative methods: A vocabulary of research concepts.* London, Sage.

Boss, S.R., Galletta, D.F., Lowry, P.B., Moody, G.D. and Polak, P. (2015) 'What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors', *MIS Quarterly (MISQ),* **39**((4)), pp. 837-864.

Bourgeon, J., Picard, P. and Pouyet, J. (2008) 'Providers' affiliation, insurance and collusion', *Journal of Banking & Finance,* **32**(1), pp. 170-186.

Boyer, M.M. (2007) 'Resistance (to Fraud) Is Futile', *Journal of Risk & Insurance,* **74**(2), pp. 461-492.

Braun, V. & Clarke, V. (2006) 'Using thematic analysis in psychology', *Qualitative Research in Psychology,* **3**(2), pp. 77-101.

Brody, R.G., Mulig, E. and Kimball, V. (2007) 'Phishing, pharming and identity theft', *Academy of Accounting and Financial Studies Journal,* **11**(3), pp. 43-56.

Brooks, G. and Button, M. (2011) 'The police and fraud investigation and the case for a nationalised solution in the United Kingdom', *The Police Journal,* **84**(4), pp. 305-319.

Bryman, A. (2015) *Social research methods.* 5th edn. New York, Oxford university press.

Bryman, A. (2013) *Doing research in organizations.* Oxon, Routledge.

Bryman, A. and Bell, E. (2015) *Business research methods.* 4th edn. New York, Oxford University Press.

Button, M. (2011) 'Editorial: Fraud, corruption and the financial crisis', *International Journal of Law, Crime and Justice,* **39**(3), pp. 137-139.

Calvasina, G.E., Calvasina, R.V. and Calvasina, E.J. (2007) 'Preventing Employee Identity Fraud: Policy and Practice Issues for Employers', *Journal of Legal, Ethical & Regulatory Issues,* **10**(2), pp. 69-80.

Carneiro, N., Figueira, G. and Costa, M. (2017) 'A data mining based system for credit-card fraud detection in e-tail', *Decision Support Systems,* **95**(1), pp. pp. 91-101.

Cavaye, A.L. (1996) 'Case study research: a multi- faceted research approach for IS', *Information systems journal,* **6**(3), pp. 227-242.

Chang, W. and Chang, J. (2011) 'A novel two-stage phased modeling framework for early fraud detection in online auctions', *Expert Systems with Applications,* **38**(9), pp. 11244-11260.

Chen, Y., Ramamurthy, K. and Wen, K. (2015) 'Impacts of Comprehensive Information Security Programs on Information Security Culture', *The Journal of Computer Information Systems,* **55**(3), pp. 11.

Cheng, D., Ter Chian Felix Tan, Guo, Z. and Cahalane, M. (2015) *Developing ICT-Enabled Information Processing Capabilities for Combatting E-Commerce Identity Fraud: A Case Study of Trustev's Social Fingerprinting Solution.* Pacific Asia Conference on Information Systems (PACIS), Singapore. 5-9 July.

Chohan, R., Shah, M., Larson, M. and Welch, M. (2014) *Overcoming Trust Barriers: Evaluating Inter-Organisational Knowledge Sharing in UK Online Retail Sector'*. European Conference on Knowledge Management, Santarem, Portugal. 4-5 Spetember.

Christie, M., Rowe, P., Perry, C. and Chamard, J. (2000) *Implementation of realism in case study research methodology*. International Council for Small Business, Annual Conference, Brisbane, Australia. 7-10 June.

CIFAS (2018a) *Fraudscape 2016*. Available at: https://www.cifas.org.uk/insight/reports-trends (Accessed: 3 December 2017).

CIFAS (2018b) *Fraudscape 2017*. Available at: https://www.cifas.org.uk/insight/reports-trends/fraudscape-report-2017 (Accessed: 12 January 2018).

CIFAS (2018c) *Identity fraud soars to new levles*. Available at: https://www.cifas.org.uk/newsroom/identity-fraud-soars-to-new-levels (Accessed: 23 February 2018).

CIFAS (2015) *Fraudscape: UK fraud trends*. Available at: http://www.cifas.org.uk/secure/contentPORT/uploads/documents/External%20-%20Fraudscape%20main%20report%20for%20website.pdf (Accessed: 20 November 2016).

Colton, D. and Covert, R.W. (2007) *Designing and constructing instruments for social research and evaluation*. John Wiley & Sons.

Copes, H., Kerley, K.R., Huff, R. and Kane, J. (2010) 'Differentiating identity theft: An exploratory study of victims using a national victimization survey', *Journal of Criminal Justice*, **38**(5), pp. 1045-1052.

Corbin, J. and Strauss, A. (2008) *Basics of qualitative research 3e*. 3rd edn. London, Sage Publications.

Coulson-Thomas, C. (2017) 'Fraud, security risks and corporate responses', in Ahluwalia J. S. (eds.) *"Corporate Ethics & Risk Management in an uncertain world"* Mumbai, IOD Publishing, pp. 67-76.

Cressey, D.R. (1950) 'The criminal violation of financial trust', *American Sociological Review*, **15**(6), pp. 738-743.

Creswell, J.W. and Poth, C.N. (2017) *Qualitative Inquiry & Research Design*. 4th edn. California, USA, SAGE Publications, Inc.

Cross, C. and Blackshaw, D. (2014) 'Improving the police response to online fraud', *Policing: A Journal of Policy and Practice*, **9**(2), pp. 119-128.

Cunliffe, A.L. (2010) 'Retelling tales of the field: In search of organizational ethnography 20 years on', *Organisational Research Methods*, **13**(2), pp. 224-239.

Da Veiga, A. and Martins, N. (2015) 'Information security culture and information protection culture: A validated assessment instrument', *Computer Law & Security Review*, **31**(2), pp. 243-256.

D'Arcy, J., Hovav, A. and Galletta, D. (2009) 'User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach', *Information Systems Research*, **20**(1), pp. 79-98.

DeAngelo, G. and Charness, G. (2012) 'Deterrence, expected cost, uncertainty and voting: Experimental evidence', *Journal of Risk and Uncertainty*, **44**(1), pp. 73-100.

Delanty, G. (2005) *Social science: Philosophical and methodological foundations.* 2nd edn. Berkshire, UK, Open University Press.

Denzin, N.K. and Lincoln, Y.S. (2011) *The Sage handbook of qualitative research.* California, Sage Publications Inc.

Devos, J. and Pipan, I. (2009) 'The Role of IT/IS in Combating Fraud in the Payment Card Industry', *Journal of Internet Banking & Commerce*, **14**(3), pp. 1-17.

Dorfleitner, G. and Jahnes, H. (2014) 'What factors drive personal loan fraud? Evidence from Germany', *Review of Managerial Science*, **8**(1), pp. 89-119.

Dorminey, J., Fleming, A.S., Kranacher, M. and Riley Jr, R.A. (2012) 'The evolution of fraud theory', *Issues in Accounting Education*, **27**(2), pp. 555-579.

Easterby-Smith, M., Thorpe, R. and Jackson, P.R. (2015) *Management and business research.* 5th edn. London, Sage Publications Ltd.

Easterby-Smith, M.P.V. and Thorpe, R. and Lowe, A. (2013) *Qualitative research in business and management.* London, Sage Publications Ltd.

Eriksson, P. and Kovalainen, A. (2015) *Qualitative Methods in Business Research: A Practical Guide to Social Research.* 2nd edn. London, Sage Publications Ltd.

Feledi, D. and Fenz, S. (2012) *Challenges of web-based information security knowledge sharing.* 7th International conference on availability, reliability and security (ARES), Prague, Czech Republic. 20- 24 August.

Furlan, S. and Bajec, M. (2008) 'Holistic approach to fraud management in health insurance', *Journal of Information and Organizational Sciences*, **32**(2), pp. 99-114.

getsafeonline (2017) *Over £1 billion lost by businesses to online crime in the last year.* Available at: https://www.getsafeonline.org/press/over-1-billion-lost-by-businesses-to-online-crime-in-the-last-year/ (Accessed: 24-01-2018).

Ghosh, M. (2010) 'Mobile ID fraud: the downside of mobile growth', *Computer Fraud & Security*, **2010**(12), pp. 8-13.

Gibbert, M., Ruigrok, W. and Wicki, B. (2008) 'What passes as a rigorous case study?', *Strategic Management Journal*, **29**(13), pp. 1465-1474.

Gogolin, G. and Jones, J. (2010) 'Law Enforcement's Ability to Deal with Digital Crime and the Implications for Business', *Information Security Journal: A Global Perspective,* **19**(3), pp. 109-117.

Gonzalez, S.M. and Tacorante, D.V. (2004) 'A new approach to the best practices debate: are best practices applied to all employees in the same way?', *International Journal of Human Resource Management,* **15**(1), pp. 56-75.

Goyal, V., Pandey, U. and Batra, S. (2012) 'Mobile banking in India: Practices, challenges and security issues', *International Journal of Advanced Trends in Computer Science and Engineering,* **1**(2), pp. 55-66.

Gray, D.E. (2013) *Doing research in the real world.* 3rd edn. London, Sage Publications Ltd.

Grbich, C. (2013) *Qualitative data analysis: An introduction.* 2nd edn. London, Sage Publications Ltd.

Guitton, C. (2012) 'Criminals and cyber attacks: The missing link between attribution and deterrence', *International Journal of Cyber Criminology,* **6**(2), pp. 1030.

Hannagan, T. and Bennett, R. (2008) *Management: concepts & practices.* 5th edn. Harlow, Pearson Education.

Hardouin, P. (2009) 'Banks governance and public-private partnership in preventing and confronting organized crime, corruption and terrorism financing', *Journal of financial crime,* **16**(3), pp. 199-209.

He, B., Chen, C., Su, Y. and Sun, H. (2014) 'A defence scheme against identity theft attack based on multiple social networks', *Expert Systems with Applications,* **41**(5), pp. 2345-2352.

Hille, P., Walsh, G. and Cleveland, M. (2015) 'Consumer fear of online identity theft: Scale development and validation', *Journal of Interactive Marketing,* **30**, pp. 1-19.

Hollinger, R.C. and Clark, J.P. (1983) *Theft by employees.* Lexington, MA, Lexington Books.

Holt, T.J. and Turner, M.G. (2012) 'Examining risks and protective factors of on-line identity theft', *Deviant Behavior,* **33**(4), pp. 308-323.

Ijeoma, N. and Aronu, C. (2013) 'The Impact of Fraud Management on Organizational Survival in Nigeria', *American Journal of Economics,* **3**(6), pp. 268-272.

Jamieson, R., Winchester, D. and Smith, S. (2007) *Development of a conceptual framework for managing identity fraud.* 40th Annual Hawaii International Conference on System Sciences, (HICSS), Waikoloa, HI,. 3-6 January.

Javelin Strategy (2018) *Identity fraud hits record high 154 million U.S. victims 2016, Up 16 percent according new Javelin Strategy and research study.* Available at:

https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new (Accessed: 12 Jan, 2018).

Ji, S., Wang, J., Min, Q. and Smith-Chao, S. (2007) *Systems Plan for Combating Identity Theft-A Theoretical Framework.* International Conference on Wireless Communications, Networking and Mobile Computing, (WiCom), New York. 21-25 September.

Kahn, C.M. and Liñares-Zegarra, J.M. (2016) 'Identity Theft and Consumer Payment Choice: Does Security Really Matter?', *Journal of Financial Services Research*, **50**(1), pp. 121-159.

Koskosas, I. (2013) 'A Short Literature Review in Information Systems Security Approaches', *Academic Research,* **1**(1), pp. 1-7.

Kumar, D. and Goyal, N. (2016) *Security issues in M-commerce for online transaction.* 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO), 2016, Noida, India.

Kumar, R. (2014) *Research Methodology.* 4th edn. India, Sage Publications Ltd.

Kumar, V. and Kumar, D. and De Grosbois, D. (2007) *Collaboration in Combating Identity Fraud.* Annual Conference of the Administrative Sciences Association of Canada, Production and Operations Management Division, Ottawa, Canada.

Kundu, A., Panigrahi, S., Sural, S. and Majumdar, A.K. (2009) 'Blast-ssaha hybridization for credit card fraud detection', *IEEE Transactions on Dependable and Secure Computing*, **6**(4), pp. 309-315.

Latham, J.R. (2012) 'Management System Design for Sustainable Excellence: Framework, Practices and Considerations', *Quality Management Journal,* **19**(2), pp. 7-21.

Leasure, P. and Zhang, G. (2017) 'That how they taught us to do it: Learned Deviance and Inadequate Deterrents in Retail Banking', *Deviant Behavior*, **33**(1), pp. 1-14.

Lee, S. and Yu, J. (2012) 'Success model of project management information system in construction', *Automation in Construction*, **25**(August), pp. 82-93.

Lewis, C., Brooks, G., Button, M., Shepherd, D. and Wakefield, A. (2014) 'Evaluating the case for greater use of private prosecutions in England and Wales for fraud offences', *International Journal of Law, Crime and Justice*, **42**(1), pp. 3-15.

Liu, J., Xiao, Y., Chen, H., Ozdemir, S., Dodle, S. and Singh, V. (2010) 'A survey of payment card industry data security standard', *IEEE Communications Surveys & Tutorials,* **12**(3), pp. 287-303.

Mansfield-Devine, S. (2013) 'Biometrics in retail', *Biometric Technology Today*, **2013**(9), pp. 5-8.

Mason, M. (2010) 'Sample size and saturation in PhD studies using qualitative interviews', *Forum: qualitative social research*, **11**(3), pp. 1-19.

Matthew A. Cordell (2013) *Beware of red flags: What must your business do to protect customers from identity theft.* Available at: http://www.wardandsmith.com/articles/what-must-your-business-do-to-protect-customers-from-identity-theft#.VSqxQPD7L4Z (Accessed: 12 Nov, 2017).

Meinert, M.C. (2016) 'In the Fight Against Fraud, Strong Leadership is KEY', *ABA Banking Journal*, **108**(2), pp. 55-56.

Merriam Webster (2018) *Merriam Webster Dictionary.* Available at: https://www.merriam-webster.com/dictionary/stage (Accessed: 3 January 2018).

Merriam, S.B. and Tisdell, E.J. (2015) *Qualitative research: A guide to design and implementation.* 4th edn. San Francisco, John Wiley & Sons.

Metwally, E. (2013) 'Using the case research approach in understanding the effect of managing change through technology to achieving strategic competitiveness in private banks: Gains and perils.', *Journal of International Finance & Economics,* **13**(2), pp. 5-20.

Mithas, S. and Rust, R.T. (2016) 'How Information Technology Strategy and Investments Influence Firm Performance: Conjecture and Empirical Evidence.', *MIS quarterly,* **40**(1), pp. 223-245.

Monaghan, C. (2010) 'To Prosecute or Not to Prosecute? A Reconsideration of the Over-Zealous Prosecution of Parents under the Fraud Act 2006', *The Journal of Criminal Law,* **74**(3), pp. 259-278.

Myers, M.D. (2013) *Qualitative research in business and management.* 2nd edn. London, Sage Publications Ltd.

Myers, M.D. and Avison, D. (1997) 'Qualitative research in information systems', *Management Information Systems Quarterly,* **21**(2), pp. 241-242.

Nairn, A., Berthon, P. and Money, A. (2007) 'Learning from giants-Exploring, classifying and analysing existing knowledge on market research', *International Journal of Market Research,* **49**(2), pp. 257-274.

Njenga, N. and Osiemo (2013) 'Effect of fraud risk management on organization performance: A case of deposit-taking microfinance institutions in Kenya', *International Journal of Social Sciences and Entrepreneurship,* **1**(7), pp. 490-507.

Orlikowski, W.J. and Baroudi, J.J. (1991) 'Studying information technology in organizations: Research approaches and assumptions', *Information systems research,* **2**(1), pp. 1-28.

Palmberg, K. (2010) 'Experiences of implementing process management: a multiple-case study', *Business Process Management Journal,* **16**(1), pp. 93-113.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014) 'Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)', *Computers & Security,* **42**(May), pp. 165-176.

Peotta, L., Holtz, M.D., David, B.M., Deus, F.G. and De Sousa, R. (2011) 'A formal classification of internet banking attacks and vulnerabilities', *International Journal of Computer Science & Information Technology,* **3**(1), pp. 186-197.

Pergola, C.W. and Sprung, P.C. (2005) 'Developing a genuine anti-fraud environment', *Risk Management,* **52**(3), pp. 43-44.

Petraşcu, D. and Tieanu, A. (2014) 'The Role of Internal Audit in Fraud Prevention and Detection', *Procedia Economics and Finance,* **16**, pp. 489-497.

Phan, D.D. and Vogel, D.R. (2010) 'A model of customer relationship management and business intelligence systems for catalogue and online retailers', *Information & management,* **47**(2), pp. 69-77.

Phua, C., Lee, V., Smith, K. and Gayler, R. (2010) 'A comprehensive survey of data mining-based fraud detection research', *arXiv preprint arXiv:1009.6119,* .

Pope, C., Ziebland, S. and Mays, N. (2006) 'Analysing qualitative data', in Pope, C. and Mays, N. (eds.) *Qualitative research in health care*. 3rd edn. Oxford, Blackwell Publishing, pp. 63-81.

Porter, D. (2004) 'Identity fraud: the stealth threat to UK plc', *Computer Fraud & Security,* **2004**(7), pp. 4-6.

Power, D.J. and Power, M.L. (2015) *Sharing and Analyzing Data to Reduce Insurance Fraud.* Proceedings of the 10th Annual MWAIS Conference, Pittsburg, KS, USA. 14-15 May.

Prabowo, H.Y. (2012) 'A better credit card fraud prevention strategy for Indonesia', *Journal of Money Laundering Control,* **15**(3), pp. 267-293.

Prabowo, H.Y. (2011) 'Building our defence against credit card fraud: a strategic view', *Journal of Money Laundering Control,* **14**(4), pp. 371-386.

Prakash, R.A., Mehata, K. and Chellappan, C. (2015) 'A Robust Biometric Authentication and PIN Distribution Technique for Secure Mobile Commerce Applications', *Research Journal of Applied Sciences, Engineering and Technology,* **9**(6), pp. 409-418.

Prosch, M. (2009) 'Preventing Identity Theft Throughout the Data Life Cycle', *Journal of Accountancy,* **207**(1), pp. 58-62.

Puhakainen, P. and Siponen, M. (2010) 'Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study.', *MIS quarterly,* **34**(4), pp. 757-778.

Rhee, H., Ryu, Y.U. and Kim, C. (2012) 'Unrealistic optimism on information security management', *Computers & Security,* **31**(2), pp. 221-232.

Ritchie, J., Lewis, J., Nicholls, C.M. and Ormston, R. (2014) *Qualitative research practice: A guide for social science students and researchers.* 2nd edn. London, Sage Publications Ltd.

Roberts, L.D., Indermaur, D. and Spiranovic, C. (2013) 'Fear of cyber-identity theft and related fraudulent activity', *Psychiatry, Psychology and Law,* **20**(3), pp. 315-328.

Robinson, C. (2002) *Real world research: a resource for social scientists and practitioner-researchers.* Oxford, UK, Blackwell.

Rogers, R.W. (1975) 'A protection motivation theory of fear appeals and attitude change1', *The Journal of psychology,* **91**(1), pp. 93-114.

Rose, M., Sarjoo, P. and Bennett, K. (2015) 'A boost to fraud risk assessments: reviews based on the updated COSO Internal Control-Integrated Framework may help prevent fraud', *Internal Auditor,* **72**(3), pp. 22-24.

Sanchez, M. (2012) 'The Role of the Forensic Accountant in a Medicare Fraud Identity Theft Case', *Global Journal of Business Research (GJBR),* **6**(3), pp. 85-92.

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H. and Jinks, C. (2018) 'Saturation in qualitative research: exploring its conceptualization and operationalization', *Quality & Quantity,* **52**(4), pp. 1893-1907.

Savirimuthu, A. and Savirimuthu, J. (2007) 'Identity theft and systems theory: the Fraud Act 2006 in perspective', *SCRIPTed,* **4**(4), pp. 436-461.

Schafermeyer, M., Grgecic, D. and Rosenkranz, C. (2010) *Factors influencing business process standardization: A multiple case study.* 43rd Hawaii International Conference on System Sciences (HICSS), Honolulu, HI, USA. 5-8 January.

Seda, L. (2014) 'Identity theft and university students: do they know, do they care?', *Journal of Financial Crime,* **21**(4), pp. 461-483.

Shah, M. and Okeke, R.I. (2011) *A Framework for Internal Identity Theft Prevention in Retail Industry.* European Intelligence and Security Informatics Conference (EISIC), Athens, Greece. 12-14 September.

Shamsi, J.A., Zeadally, S., Sheikh, F. and Flowers, A. (2016) 'Attribution in cyberspace: techniques and legal implications', *Security and Communication Networks,* **9**(15), pp. 2886-2900.

Sharma, A., Kansal, V. and Tomar, R. (2015) 'Location Based Services in M-Commerce: Customer Trust and Transaction Security Issues', *International Journal of Computer Science and Security (IJCSS),* **9**(2), pp. 11.

Silverman, D. (2016) *Qualitative research.* 4th edn. London, Sage Publications Ltd.

Singh, A.N., Picot, A., Kranz, J., Gupta, M.P. and Ojha, A. (2013) 'Information Security Management (ISM) Practices: Lessons from Select Cases from India and Germany', *Global Journal of Flexible Systems Management,* **14**(4), pp. 225-239.

Siponen, M., Mahmood, M.A. and and Pahnila, S. (2014) 'Employees’ adherence to information security policies: An exploratory field study', *Information & Management,* **51**(2), pp. 217-224.

Soomro, Z.A., Ahmed, J., Muhammad, R., Hayes, D. and Shah, M.H. (2017) 'Critical success factors in implementing an e-rostering system in a healthcare organisation', *Health services management research,* , pp. 0951484817745695.

Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016) 'Information security management needs more holistic approach: A literature review', *International Journal of Information Management,* **36**(2), pp. 215-225.

Sperdea, N.M., Enescu, M. and Enescu, M. (2011) 'Challenges of managing e-commerce', *Economics, Management and Financial Markets,* **6**(2), pp. 194.

Stake, R.E. (2013) *Multiple case study analysis.* New York, Guilford Press.

Stake, R.E. (2005) *Qualitative case studies.* London, Sage publications.

Strauss, A. and Corbin, J. (1990) *Basics of qualitative research.* California, Sage.

Subramony, M. (2006) 'Why organizations adopt some human resource management practices and reject others: An exploration of rationales', *Human resource management,* **45**(2), pp. 195-210.

Swathi, M. and Kalpana, K. (2013) 'Spirit of Identity Fraud And Counterfeit Detection', *International Journal of Computer Trends and Technology (IJCTT),* **4**(6), pp. 1891-1895.

Taitsman, J.K., Grimm, C.M. and Agrawal, S. (2013) 'Protecting patient privacy and data security', *New England Journal of Medicine,* **368**(11), pp. 977-979.

Tajpour, A., Ibrahim, S. and Zamani, M. (2013) 'Identity theft methods and fraud types', *International Journal of Information Processing and Management, IJIPM,* **4**(7), pp. 51-58.

Tan, F.T.C., Guo, Z., Cahalane, M. and Cheng, D. (2016) 'Developing business analytic capabilities for combating e-commerce identity fraud: A study of Trustev's digital verification solution', *Information & Management,* **53**(7), pp. 878-891.

Tannenbaum, M.B., Hepler, J., Zimmerman, R.S., Saul, L., Jacobs, S., Wilson, K. and Albarracín, D. (2015) 'Appealing to fear: A meta-analysis of fear appeal effectiveness and theories.', *Psychological Bulletin,* **141**(6), pp. 1178-1204.

Teh, P.S., Zhang, N., Teoh, A.B.J. and Chen, K. (2016) 'A survey on touch dynamics authentication in mobile devices', *Computers & Security,* **59**, pp. 210-235.

Tøndel, I.A., Line, M.B. and Jaatun, M.G. (2014) 'Information security incident management: Current practice as reported in the literature', *Computers & Security,* **45**(1), pp. 42-57.

Usman, A.K. and Shah, M.H. (2013) 'Strengthening e-banking security using keystroke dynamics', *The Journal of Internet Banking and Commerce,* **18**(3), pp. 1-11.

Vahdati, S. and Yasini, N. (2015) 'Factors affecting internet frauds in private sector: A case study in cyberspace surveillance and scam monitoring agency of Iran', *Computers in Human Behavior,* **51**(A), pp. 180-187.

Vaismoradi, M., Turunen, H. and Bondas, T. (2013) 'Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study', *Nursing & health sciences,* **15**(3), pp. 398-405.

Verdon, D. (2006) 'Security policies and the software developer', *IEEE Security & Privacy,* **4**(4), pp. 42-49.

Vidalis, S. and Angelopoulou, O. (2014) 'Assessing identity theft in the Internet of Things', *Journal of IT Governance Practice,* **2**(1), pp. 15-21.

Vijaya Geeta, D. (2011) 'Online identity theft–an Indian perspective', *Journal of Financial Crime,* **18**(3), pp. 235-246.

Von Glinow, M.A., Drost, E.A. and Teagarden, M.B. (2002) 'Converging on Ihrm Best Practices: Lessons Learned from a Globally Distributed Consortium on Theory and Practice', *Human resource management,* **41**(1), pp. 123.

Wang, E.K., Cao, Z., Wu, T. and Chen, C. (2015) 'A mutual authentication protocol for mobile payment (MAPMP)', *Journal of Information Hiding and Multimedia Signal Processing,* **6**(4), pp. 697-707.

Wang, W., Yuan, Y. and Archer, N. (2006) 'A contextual framework for combating identity theft', *IEEE Security and Privacy,* **4**(2), pp. 30-38.

Weisman, A. and Brodsky, M. (2011) 'Fighting fraud with both fists', *The CPA Journal,* **81**(1), pp. 11.

Whitman, M.E. and Mattord, H.J. (2011) *Principles of information security.* USA, Cengage Learning.

Wilhelm, W.K. (2004) 'The fraud management lifecycle theory: a holistic approach to fraud management', *Journal of Economic Crime Management,* **2**(2), pp. 1-38.

Wilson, J. (2014) *Essentials of business research: A guide to doing your research project.* 2nd edn. London, Sage Publications Ltd.

Workman, M. and Gathegi, J. (2007) 'Punishment and ethics deterrents: A study of insider security contravention', *Journal of the American Society for Information Science and Technology,* **58**(2), pp. 212-222.

Wright, R. (2007) 'Developing effective tools to manage the risk of damage caused by economically motivated crime fraud', *Journal of Financial Crime,* **14**(1), pp. 17-27.

Xiao, Z. (2017) *The Development of E-Commerce in Europe.* Master thesis. Centria University of Applied Sciences.

Yelland, M. (2013) 'Fraud in mobile networks', *Computer Fraud & Security,* **2013**(3), pp. 5-9.

Yin, R.K. (2014) *Case study research: design and methods.* 5th edn. London, Sagen Publications Ltd.

Yin, R.K. (2011) *Applications of case study research.* 3rd edn. California, Sage Publications Inc.

Zadig, S.M. and Tejay, G. (2010) *Securing IS assets through hacker deterrence: A case study.* eCrime Researchers Summit (eCrime), Dallas, USA. 18-20 October.