Investigating Identity Fraud Management Practices in E-tail sector: A Systematic Review

Journal:	*Journal of Enterprise Information Management*
Manuscript ID	JEIM-06-2018-0110.R2
Manuscript Type:	Research Article
Keywords:	identity fraud,, e-tailer, managerial practices, literature review, fraud management, identity theft

Investigating Identity Fraud Management Practices in E-tail sector: A Systematic Review

Abstract

Purpose: Identity fraud is a growing issue for online retail organisations. The literature on this issue is scattered, and none of the studies presents a holistic view of identity fraud management practices in online retail context. Therefore, this study aims at investigating the identity fraud management practices and presents a comprehensive set of practices for e-tail sector.

Methodology: A systematic literature review approach was adopted, and the articles were selected through pre-set inclusion criteria. We synthesised existing literature to investigate identity fraud management in e-tail sector.

Findings: The research finds that literature on practices for identity fraud management is scattered. Findings also reveal that firms assume identity fraud issues as a technological challenge, which is one of the major reasons for a gap in effective management of identity frauds. This research suggests e-tailers to deal this issue as a management challenge and counter strategies should be developed in technological, human and organisational aspects.

Research limitations: This study is limited to the published sources of data. Studies, based on empirical data, will be helpful to support the argument of this study, additionally future studies are recommended to include a wide number of databases.

Originality: This research makes unique contributions by synthesising existing literature at each stage of fraud management and encompasses social, organisational and technological aspects. It will also help academicians understanding a holistic view of available research and opens new lines for future research.

Practical implications: This research will help e-tail organisations to understand the whole of identity fraud management and help them develop and implement a comprehensive set of practices at each stage, for effective management identity frauds.

Keywords: identity fraud, e-tailer, identity theft, managerial practices, fraud management, literature review.

1. Introduction

E-commerce has changed the ways of doing business by offering unlimited opportunities to online retailers like reduction in operation costs, effective customer relationship, and boundary-less services. However, these opportunities also have created challenges for them especially related to identity frauds. Identity fraud occurs when a fraudster abuses personal information to impersonate someone else or creates a fictitious identity to make a purchase or open an account to defraud (CIFAS, 2018b).

The developed countries like USA and UK are adversely affected by this fraud. In 2016, 15.4 million American consumers were affected by identity frauds for an amount of US$ 16 billion; the victims were up by 16% as compared to previous year (Javelin Strategy, 2018). In the UK, the situation is almost the same as, 172,919 cases of identity frauds were reported by only credit industry fraud avoidance system (CIFAS) member organisations, in the year 2016, recording a continuous increase.

The extant literature has some studies exploring different aspects of identity fraud management. Some researchers also have suggested frameworks in the given context to present a full picture of the identity fraud management process, but these studies lack in-depth insights into the fraud management activities at each different process within the organisation. On the other hand, some studies are there which focus one or a few activities and processes of the fraud management. Thus, no study gives a comprehensive picture of identity fraud management practices at the different stages. In addition, still least is known about the nature of the issue, whether it is a technological or organisational problem. In the absence of such studies, organisations are unable to manage identity frauds effectively, so still, these frauds are on the rise. Therefore, the challenges of managing identity frauds in e-tail industry need to focus on a holistic approach to include the practices at each stage of fraud management and explore the grounds to counter it effectively. To attain the objectives of this research, it was necessary to synthesise the extant literature on practices at each stage of identity fraud management.

For literature search, five prominent databases were searched. Only peer-reviewed articles were included in this study. The results show that there has been no comprehensive study investing practices for effective identity fraud management in e-tail context. There was a number of articles focused on one or two aspects of the identity fraud management, but only a few researchers have focused on comprehensive fraud management by suggesting a framework. Therefore, synthesising the dispersed literature towards the development of a comprehensive set of practices is a unique contribution of this paper.

2. Background

The number of the identity frauds has movement trend with the increased use of online business opportunities. Table I represents the trend of identity-related frauds for the last five years for CIFAS member organisations only. These figures show only the frauds reported by CIFAS member organisations whereas the total number of identity-related frauds in the UK would be higher. Such an enormous number of identity frauds is a serious concern for online business firms in the UK, as they bear most of these losses (Brody *et al.*, 2007).

Insert table I here

The Table I represents the identity related frauds and their trends. The firms calculate application and account takeover frauds separately from other identity frauds, so for this study, these are added to give a comprehensive picture of IDFs. The table shows that IDFs are continuously at inclining trend. The Table I also reveal that the share of IDFs has significantly increased in last four years. The CIFAS reports on frauds show that fraud in e-tailers is growing on higher rate as compared to other sectors, as in 2015 it escalated at the rate of 19% and in 2016 it was up by 52% compared to the previous years (CIFAS, 2018b; CIFAS, 2018a).

According to a news released by CIFAS (2018c), IDFs (excluding the account takeover and application fraud) for first six months of 2017 have increased by 5%, from the corresponding period last year, adding to 56% of total frauds reported by its member organisations. The report also mentions that there is 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 table are limited to only the CIFAS member organisations, so the actual number of IDFs may be higher than these. Additionally, the CIFAS (2018b) mentions that these reports are based on the figures from large-scale organisations, while medium and small organisations are not included and mostly IDFs at these e-tailers are not reported at all.

E-tail business is one of the most affected sectors by online frauds. According to a news released by, Getsafeonline, (2017) the UK businesses have lost over one billion pounds for the period 03/2015 to 03/2016 in online frauds. It has also been confirmed that IDFs constitute more than half of the total online frauds (CIFAS, 2018b). 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 a significant adverse impact on business firms.

The data shows that the 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.

3. Identity fraud management: an overview

Fraud is an old activity, so the literature is rich focusing on various aspects of fraud management. Regarding the behavioural aspects of fraud management, it is a well-established argument that the potential fraudsters can be deterred by the fear of being caught and punished (Alanezi and Brooks, 2014). The concept of changing the behaviour of potential fraudsters is derived from the deterrence theory, which has widely been studied in various contexts and is proved to be significant to control the deviant behaviour.

The root of deterrence theory lies in the fear appeal theories. The fear appeals influence attitude, intention and behaviour of fraudsters and may prevent a fraud (Tannenbaum *et al.*, 2015). So far, the significance of this deterrence has been confirmed in various contexts mainly in accounting and audit (Dorminey *et al.*, 2012) and employee theft (Hollinger and Clark, 1983). Similarly, there are numerous studies focused on customer education and threat as measures of 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 presenting a comprehensive view of identity fraud deterrence practices in relation to the e-tail industry. Therefore, research is needed to present a holistic picture of managerial practices for identity fraud deterrence in e-tail organisations.

In spite of deterrent practices, frauds are still attempted. 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. What follows is that in addition to deterrence, organisations should also have systems to prevent and detect 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). A sound prevention system is an effective anti-fraud action (Prabowo, 2011). For preventing the identity theft 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; Geeta, 2011), but no significant research has been found to suggest a set of comprehensive practices in identity theft prevention.

Although measures are there to prevent identity fraud attacks, however, the literature findings reveal that fraudsters use genuine customers' information, as a result, some fraudulent transactions still pass through the security net. Therefore, organisations need to detect these transactions as the next stage after prevention (Chang and Chang, 2011). The extant literature suggests that fraud attempt is merely a result of an assumption of the lack of detection, so organisations should have an effective detection system that also helps to create the fear of being caught and punished (Cressey, 1950). The practices of having automated detection system and verification of suspicious transactions are recommended by various researchers (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. Thus far, no study has been found encompassing the whole of detection practices in the e-tail industry.

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). 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 used, and the reasons why it passed through the prevention system. In fraud management, this set of practices is called fraud analysis. Analysis of identity frauds is a critical stage that helps to develop policies and strategies for effective fraud management. 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 research has forwarded a comprehensive set of practices focused on identity fraud analysis in e-tail sector.

At each stage of fraud management, anti-fraud policies create layers of protection for the organisation and its employees (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). 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 presents a holistic view on identity fraud management policies in e-tail sector.

The above-mentioned fraud management stages focus on actions before and during the fraud attempt, but effective identity fraud management requires 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 however, businesses have a part to play (Cross and Blackshaw, 2014; Lewis *et al.*, 2014). Investigation and prosecution are critical stages of 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. Although, the extant literature has some studies (Amori, 2008; Brooks and Button, 2011; Cross and Blackshaw, 2014; Gogolin and Jones, 2010; Jamieson *et al.*, 2007; Lewis *et al.*, 2014; Rose *et al.*, 2015; Wilhelm, 2004) on investigation and prosecution of frauds however, comprehensive set of practices on identity fraud management in e-tail sector is unclear.

The above discussion shows that literature on identity fraud management is scattered. Articles in this domain are focused on limited aspects, thus management of identity fraud in e-tail sector is not properly understood. In the absence of a research encompassing a holistic view of identity fraud management practices, e-tailers are losing a significant portion of their revenues in such losses (Amasiatu, 2016). According to a report by CIFAS (2018b), 35% of total online frauds in the UK are related to retail firms, thus e-tailers share significant losses in online frauds. The Absence of such study is also a research challenge for academics. In the given situation, a single empirical study may not help in understanding identity fraud management properly. Also a single or a few articles may not encompass organisational, social and technological aspects at each of the eight stages of fraud management. To help bridging this gap, this study tries to review the extant literature in order to understand and forward a holistic view of identity fraud management and suggests practices at each stage of identity fraud management. This research will also open new avenues for research in current context and attract the attention of academics. This study may also help management of e-tailers to control such frauds, minimise business losses and establish favourable customer relationship.

~~1.~~4. Research m~~M~~ethodology

The practice of reviewing the literature systematically is advancing over the last few decades (Al-Kurdi *et al.*, 2018). Systematic literature review highlights significant contributions to specific domains (Jesson *et al.*, 2011). Encompassing a holistic view of identity fraud management and forwarding as set of comprehensive practices, ~~T~~this study used a systematic literature search approach to synthesise prior studies. Hence, the purpose of this study was to suggest a comprehensive set of practices for effective identity fraud management in e-tail sector~~ers~~, so the literature related any aspect of fraud management was searched.

Yang and Tate (2012), suggest four methods of literature review: narrative, descriptive, vote counting and meta-analysis. With a small number of empirical studies, the narrative reviews were used in this study, to extend the understanding of practices in underpinning context (Wang and Noe, 2010). However, a few researchers maintain that narrative reviews may lack methodological rigour (Jesson *et al.*, 2011). Therefore, a systematic literature review approach should be based on proper methods to find related studies and to be comprehensive (Ali and Miller, 2017; Williams *et al.*, 2015).

For presenting a comprehensive picture of identity fraud management and forwarding managerial practices at each stage, it was considered that limited number of research studies were present. Therefore, the approach suggested by Soomro, *et al*. (2016) was adopted that offered depth and breadth in searching the literature. ~~Keeping in view the aim of this study, the descriptive method seems to be the most appropriate one~~. This method of literature review has a systematic procedure of searching, filtering and classifying processes. The outcome of ~~the~~ such~~descriptive~~ review is often claimed to be representative of the current state of a research domain (Yang and Tate, 2012). ~~The procedure for conducting this descriptive review is detailed in the next section.~~

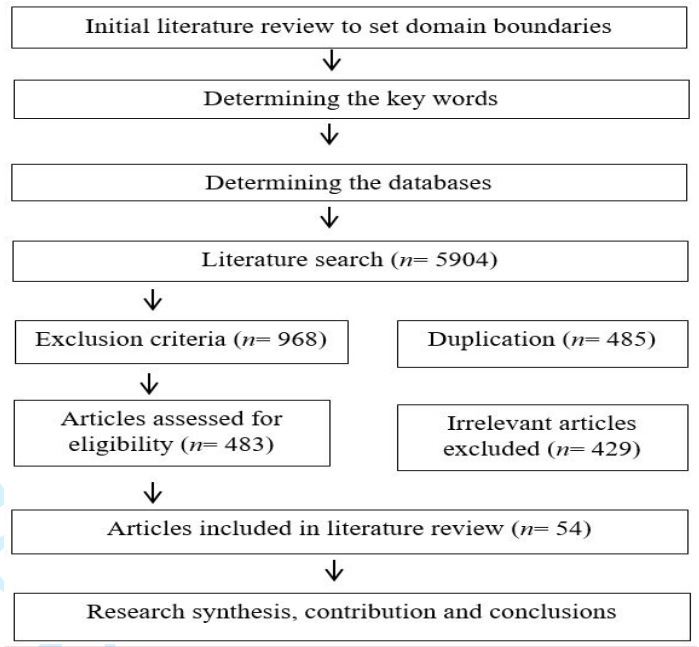

Figure 1. Research design

~~*1.1 2.1 Scope of the Literature Search*~~

~~The first step to literature analysis study is to locate relevant literature through a manual and computer searches. Traditionally the literature search is done through targeted journals and conferences, but this process is limited to focus on limited outlets which cannot be justified for literature on a much wider focus on identity fraud management process. Therefore, to search for literature on fraud management, it is appropriate and practical to focus on online databases (Yang and Tate, 2012).~~

~~For secondary data collection, the process used by~~Development of literature review method to attain the aim and objectives of this study, the process adopted by Soomro *et al.* (2016), was chosen~~adopted~~. The process offers step by step guidelines to conduct a systematic literature review in management domain. –A research plan was also developed to search key terms, inclusion and exclusion criteria and identification of related database. The figure 1 presents the detailed process of adopted research design.

At first, criteria has been set to select publications related to the context of this study. In this regard, the selection process covered research papers published between 2004 and 2017. Although, there may be some studies prior to the year 2004; however, no significant research was found presenting a comprehensive view of fraud management thus, fraud management lifecycle framework, proposed by Wilhelm (2004), has become an underpinning study to present a holistic view of fraud management. The framework suggests eight stages of fraud management i.e. deterrence, prevention, detection, mitigation, analysis, policy, investigation

and prosecution. Although the framework gives a comprehensive picture of fraud management but does not address the detailed practices of identity fraud management in e-tail sector. The other inclusion criteria were articles in English language only, peer reviewed journals papers, focused on either stage of fraud management. The exclusion criteria include; papers published before 2004, non-English articles, books, book chapters, personal reviews and non-academic research.

The first step to literature analysis study is to locate relevant literature through a manual and computer searches. Traditionally the literature search is done through targeted journals and conferences, but this process is limited to focus on limited outlets which cannot be justified for literature on a much wider focus on identity fraud management process. Therefore, to search for literature on fraud management, it is appropriate and practical to focus on online databases (Yang and Tate, 2012). To access the targeted literature, five prominent databases were included, which is a good number as some literature review studies, such as Yand and Tate (2012), used only four. These databases included IEEE Xplore, Science Direct (Elsevier), Emerald Insight, Business Source Complete and Computer and Applied Science Complete. The databases were selected based on their coverage of publications and focus on IT security and online business issues. Additionally, one search engine, Google Scholar was also used for searching purpose.

Initially literature review helped in setting up the boundaries of the research domain and setting up the keywords. Based on the literature review, some broad keywords such as; fraud, identity fraud, fraud management were identified. Additionally, the name of each stage of fraud management was set as a keyword. With the name of each stage, the word "fraud" has been added in order to retrieve the articles only focused on either some or all stages of fraud management. The list of keywords is given in Table 1.

~~To ensure the reliability of this research, a list of keywords was developed (see Table 1) to focus on the relevant studies. To access the targeted literature, five prominent databases were included, which is a good number as some literature review studies, such as Yand and Tate (2012), used only four. These databases included IEEE Xplore, Science Direct (Elsevier), Emerald Insight, Business Source Complete and Computer and Applied Science Complete. Additionally, one search engine, Google Scholar was also used for searching purpose.~~

Insert table II here

The key words mentioned in Table II~~I~~ were searched across all the five databases for the years 2004 onwards up to the end of 2017. The reason for the start of search period as 2004 is the

year of the publication of key article mentioning these stages of fraud management lifecycle as no significant study was found addressing organisational, social and technological aspects, within eight stages of fraud management, and ending period is the time of searching the literature. Our search was limited to peer-reviewed papers only.

~~To access the targeted literature, five prominent databases were included, which is a good number as some literature review studies, such as Yand and Tate (2012), used only four. These databases included IEEE Xplore, Science Direct (Elsevier), Emerald Insight, Business Source Complete and Computer and Applied Science Complete. Additionally, one search engine, Google Scholar was also used for searching purpose.~~

~~*2.2 Filtering Process*~~

In the first phase, the queries returned 5904 articles, and then the titles of each article were read. Only articles with relevant titles were selected for the next phase. Thus, 968 articles were selected for the next phase. These articles were then directly imported into RefWorks database; articles listed more than once were deleted manually. After the process of removing duplication, there remained 483 items for the next stage of reading the abstract and skimming the other parts of the articles to confirm the relevance of these articles in the present domain and to extract the themes related to any of the fraud management stages. Finally, 54 articles were found to be useful for this study.

~~2. BackgroundD~~

~~*1.2 3.1 Identity Fraud Scenario*~~

~~The number of the identity frauds has movement trend with the increased use of online business opportunities. Table I represents the trend of identity-related frauds for the last five years for CIFAS member organisations only. These figures show only the frauds reported by CIFAS member organisations whereas the total number of identity-related frauds in the UK would be higher. Such an enormous number of identity frauds is a serious concern for online business firms in the UK, as they bear most of these losses (Brody et al., 2007).~~

~~Table I showing number and percentage of identity-related frauds 2013-2017~~

~~Fraud type~~	~~2013~~	~~2014~~	~~2015~~	~~2016~~	~~2017~~

	% of total frauds	% of total frauds	% of total frauds	% of total frauds	% of total frauds (first six months)
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, 2018c; CIFAS, 2018b; CIFAS, 2018a))

The Table I represents the identity related frauds and their trends. The firms calculate application and account takeover frauds separately from other identity frauds, so for this study, these are added to give a comprehensive picture of IDFs. The table shows that IDFs are continuously at inclining trend. The Table I also reveal that the share of IDFs has significantly increased in last four years. The CIFAS reports on frauds show that fraud in e-tailers is growing on higher rate as compared to other sectors, as in 2015 it escalated at the rate of 19% and in 2016 it was up by 52% compared to the previous years (CIFAS, 2018b; CIFAS, 2018a).

According to a news released by CIFAS (2018c), IDFs (excluding the account takeover and application fraud) for first six months of 2017 have increased by 5%, from the corresponding period last year, adding to 56% of total frauds reported by its member organisations. The report also mentions that there is 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 table are limited to only the CIFAS member organisations, so the actual number of IDFs may be higher than these. Additionally, the CIFAS (2018b) reports mentions that these reports are based on the figures from large-scale organisations, while medium and small organisations are not included and mostly IDFs at these e-tailers are not reported at all.

E-tail business is one of the most affected sectors by online frauds. According to a news released by, Getsafeonline, (2017) the UK businesses have lost over one billion pounds for the period 03/2015 to 03/2016 in online frauds. It has also been confirmed that IDFs constitute

~~more than half of the total online frauds (CIFAS, 2018b). 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 a significant adverse impact on business firms.~~

~~The data shows that the 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. To some extent these frauds may be the result of the lack of internal control, which leads to negative impact on stock value (Kuhn and Morris, 2017). The extant literature has multiple studies on various aspects of fraud management, but no study presents a holistic view of on practices to manage identity frauds effectively. Also, none of the studies has focused on the whole of the problem. Therefore this study investigates IDFM practices, through a systematic literature review approach and presents a comprehensive set of practices for identity fraud management for e-tail sector. The present study also suggests that identity fraud management issue is a management challenge rather than a technological issue.~~

~~3.~~5. Research ~~s~~Synthesis

Results show that there are numerous studies on identity fraud management, focusing on one or more stages of fraud management but only a few focused on overall process. The following section is focused on understanding the identity fraud management process and activities at each stage.

~~1.3~~5.1 ~~4.1~~ Understanding Identity Fraud Management Process

The extant literature has numerous studies, focused on identity frauds, but only a few present a comprehensive picture of fraud management. These studies have presented fraud management concept in the form of frameworks. These include; fraud management lifecycle framework by Wilhelm (2004), identity fraud enterprise management framework by Jamieson, *et al.* (2007), Action-event identity theft management framework by Kumar *et al.* (2007) and role-based framework by Shah and Okeke (2011).

Fraud management lifecycle framework (Wilhelm, 2004) presents fraud lifecycle and suggest eight stages as a process of fraud management. The framework is focused on general fraud management in includes input from, telecommunication, insurance and banking sectors. These stages are deterrence, prevention, detection, mitigation, analysis, policy, investigation and

prosecution of frauds. The other frameworks as mentioned earlier are based on this framework, hence present a similar picture of fraud management.

~~1.4~~5.2 ~~4.2~~ Practices at each Stage of Identity Fraud Management Process

The fraud management lifecycle framework (Wilhelm, 2004) has eight stages, so each stage was separately searched for related literature. Many of the articles discussed more than one stage of the framework, but none of them gives a complete set of activities regarding identity fraud management process. To explore the practices at each stage in detail, and to understand the whole of identity fraud management these stages are discussed separately.

5.2.1 ~~4.2.1~~ Deterrence

Deterrence is to stop fraud or event before happening. Literary, deter means to inhibit or discourage through fear, hence to prevent action by fear of consequences. The extant literature has some studies on the deterrence of frauds and social crimes. Through effective deterrence, online, retailers can control the number of fraud attempts. The extant literature on deterrence is presented in the following table.

At the outset, Bishop (2004) argues that the trend in fraud-fighting strategy is changing and deterrence is getting 80% emphasis as compared to 20% previously. Deterrent activities are helpful in combating the potential fraud attempts, so it is a proactive way to deter the identity frauds. The deterrent practices for identity fraud management are given in the following table.

Insert table III here

Table III summarises the literature findings on deterrence. Deterrence has a critical role in managing identity frauds. Researchers such as Dorminey, *et al*. (2012), Leasure and Zhang (2017), Albrecht *et al.* (2011), Holt and Turner (2012), Arachchilage and Love (2013) and Sperdea, *et al.* (2011) have signified the role of deterrence in fraud management. The work of Albrecht *et al*. (2011), Arachchilage and Love (2013) and Holt and Turner (2012) is focused on the deterrence of identity theft at customer end. The study by Speradea, *et al.* (2011) investigates the ~~is focused on the~~ challenges of e-commerce. The research by Baer (2008) has investigated the significance of deterrence in corporate identity theft. All these studies have emphasised the role of deterrence and suggested some practices (summarised in Table III) to deter frauds effectively.

Although, these studies were conducted in various contexts but are uniformly focused on the role of deterrence in fraud management and present practices for effective fraud deterrence. These practices are limited only at the deterrence stage, however, for a holistic approach,

practices at other stages need to be investigated to present a comprehensive view of identity fraud management. Therefore, the literature on prevention stage and suggested managerial practices are presented in the next section.

~~1.4.1~~5.2.2 ~~4.2.2~~ Prevention

Prevention works at the boundary of interaction between organisation and customers to safeguard the interaction. In online business organisations, prevention activities are aimed at making the fraud more challenging to occur by implementing different measures such as information and communication security and strong authentication system. Furthermore, Table III gives a picture of the literature on prevention of identity frauds.

Insert table IV here

Table I~~V~~V~~H~~ presents the findings on prevention. Prevention is the most investigated approach for all types of frauds. For example, Amori (2008) has investigated the significance of prevention in identity theft in the health sector. Usman and Shah (2013) have investigated the significance of prevention in online banking. They suggest prevention as a significant stage in managing identity fraud, but in the banking sector. Dyer (2013) and Archer (2012) have studied the role of technology in effective prevention of frauds and found that training is a significant practice to improve employee performance in fraud and consumer identity theft prevention. Although they signified prevention as critical in fraud prevention, his research is limited to technological context. The research by Bang et al. (2012) and Lee and Yu (2012) are focused on the measures to prevent identity frauds. Although, these researchers have emphasised the role of prevention but are limited to the secure login of internet accounts. Thus, these studies do not present a full picture of identity fraud management.

Devos and Pipan (2009) have good insight into the role of prevention and suggest for technological and organisational arrangements for it, but their research is limited to payment card industry. Bierstaker et al. (2006) have suggested for organisational measures for better prevention, but their study is limited to internal frauds. Similarly, the study by Gerard et al. (2005) have focused on preventive measures and suggest for internal and external arrangements for identity theft prevention. Albeit, it signifies the importance of prevention and suggest practices to make it effective but is limited to the one aspect of identity fraud management. Wang et al. (2006) have given a framework for preventing identity theft and suggest the role of stakeholders in identity theft prevention, which is only a part of prevention stage. The studies by Boyer (2007) and Bose and Leung (2013) suggest the practice of sufficient investments for a better outcome of preventive technologies but are limited to the financial aspect of a single

stage. Hence no study presents a complete set of practices to manage identity frauds. Therefore, the present study explores practices at each stage of fraud management through scattered literature and presents a holistic view on managing identity frauds. Practices on detection stage are explained in the following section.

~~1.4.2~~5.2.3 ~~4.2.3~~ Detection

Any action or process intended to identify and locate the suspicious or fraudulent activity before, during or after completion of any fraudulent activity is referred as detection (Wilhelm, 2004). Detection works when prevention system fails to stop any suspicious attempt. The extant literature has some logical arguments regarding the importance of fraud detection in identity fraud management. For example, Kundu et al. (2009) and Devos and Pipan (2009) claim that for online merchants, the efficient fraud detection system is necessary to protect the legitimate customers and control the business costs through effectively managing the identity frauds. The following table represents the practices on fraud detection.

Insert table V here

Table ~~I~~V Presents the literature findings on the detection of online frauds. At the outset, all the studies confirm that detection is a critical stage for any online fraud management. The studies by Kundu *et al*. (2009), Xu *et al*. (2007) and Devos and Pipan (2009) emphasise for an effective detection system to control the frauds and to protect the customers from being victims of identity frauds. Although, these studies have signified the importance of fraud detection but are focused on financial industry. The research by Edge and Sampaio (2009), Ghosh (2010) and Xu *et al*. (2007) have focused on fraud detection and suggested fraud cues and behaviour monitoring for effective detection of online frauds, but these studies are limited to one aspect of fraud management.

The studies by Anderson (2010) and Nissan (2012) are focused on fraud detection and have suggested some practices, based on their investigations in the health sector and general crime detection contexts. Peotta *et al*. (2011) has suggested that device recognition system is helpful in identity fraud detection. Although it is a good practice in fraud detection these studies are focused on banking and technological contexts and have not been tested in e-tail. Cheng~~,~~ *et al*. (2015) and Tan~~,~~ *et al*. (2016) have also investigated the role of device recognition system in locating the customers' position to get help in identity fraud detection. Although, these studies present a good deal of practices but focus on the fraud detection only.

Allan and Zahn (2010) and Vahdati and Yasini (2015) have signified the importance of system updating and human skills, while Kahn and Roberds (2008), Amori (2008) and Albrecht *et al.*, (2011) have undertaken studies on prior verifications of customers' identities for detection of any identity fraud. Finally, the studies on significancet of detection by Behdad *et al.*, (2012), Kundu *et al*. (2009), Chang and Chang (2011) and Cavusoglu and Raghunathan (2004) have focused on various sectors and forwarded some notable practices.

The above discussion revealed that there have been many studies on fraud and forwarded some notable practices, but none of these studies has given a holistic view of fraud management. Therefore, present study tries to synthesise the extant literature on each stage of fraud management to give a holistic view of identity fraud management in e-tail sector. Managerial practices at the mitigation stage are given in the next section.

1.4.35.2.4 4.2.4 Mitigation

Mitigation starts once any suspicious activity is detected at an earlier stage of the fraud attempt. Wilhelm (2004), defines mitigation in fraud arena as "*to stop a fraudster from continuing or completing the fraudulent activity"*. Only efficient and timely mitigation system can guarantee a real-time termination of a fraud attempt, reduced number of successful frauds and minimised fraud losses (Wilhelm, 2004). Online organisations need a real-time mitigation system as the online transactions are completed within seconds.

Successful mitigation depends on the business process, so online organisations should develop an efficient business process to mitigate the identity fraud attempts in real time (Dyer, 2013). Dyer (2013), suggests that any changes in mitigation system or process should be aligned with existing policies and information technology systems. The following table refers the importance and process of mitigation in identity fraud management.

Insert table VI here

Table VI mentions the literature on the significance of mitigation and practices for its effeteness. Wilhelm (2004) has determined the mitigation as a significant part of identity fraud management and have explained two practice, i.e. minimising the fraud losses and recovery of customer account as normal. Furthermore, the studies by Cross and Blackshaw (2014) and Lewis *et al.* (2014) have signified the importance of information sharing in mitigation. Dyer (2013) argues that business process has a significant impact on fraud risk mitigation and suggests that changes in mitigation process should be aligned with policy, procedures and IT

systems. Additionally, Tan *et al.* (2016) suggest two critical practices, calling the customer for verification through asking identity related questions and checking the customer IP address to verify their location through a phone call. Another development in the verification of customer identities is documentary evidence. In this regard, Albrecht *et al.* (2011), Amori (2008) and Kahn and Linares-Zegarra (2016) suggest asking the customers for any documentary evidence in case of a suspicious transaction. However, collecting such evidence at the time of account opening would be more effective in identity fraud mitigation.

Furthermore, Becker *et al.* (2010) suggest the detection technologies should work as a complement to the human skills and provide feedback and training to mitigation staff to improve their performance. Finally, Hardouin (2009) advises~~suggests~~ organisations having complete information about their customers, update their personal information and monitor their account activities.

The studies mentioned above, have insights into the significance of mitigation and suggested some notable practices to improve the mitigation. Although, these studies have investigated in technical and non-technical aspects of various types of frauds but are limited to mitigation aspect of fraud management. None of these studies has holistically investigated fraud management. Managerial practices at the next stage of fraud management are presented in the following section.

~~*1.4.4*~~5.2.5 ~~4.2.5~~ Analysis

The analysis takes place to understand the fraud losses, patterns, methods and nature, once the identity fraud has been attempted. At this stage, managers analyse the causes and effects of fraud losses, fraud methods, patterns and performance of prevention and detection stages. At this point, analysts also suggest for supporting policy and improvements in activities at earlier stages of identity fraud management.

Identity fraud analysis has a significant impact on all other stages of fraud management lifecycle framework. It helps in designing an intelligent infrastructure to prevent, detect, mitigate and investigate the identity frauds and prosecute the fraudsters. Brody *et al.* (2007), suggest that analysis of vulnerability is a front line defence against online frauds and enhances the performance of prevention and detection activities. The following table discusses the arguments of the studies on fraud analysis.

Insert table VII here

Table VII mentions various studies on analysis stage of fraud management. At first, Brody *et al.* (2007) Rose *et al*. (2015) and Weisman and Brodsky (2011) have suggested for fraud risk assessment based on fraud types, trends, opportunities and occurrence. The studies by Phan and Vogel (2010) and Dorminey *et al*. (2012) investigated the significance of evaluation of the performance of employees, tools and techniques and process of fraud management. These studies suggest that analysis stage should suggest improvements through evaluation of elements of fraud management.

Furthermore, Phan and Vogel (2010) and Vahdati and Yasini (2015) have worked on technological perspectives while Tsaih *et al.* (2008) and Yelland (2013) have suggested the~~at~~ evaluation of tools and managerial practices, which are significant practices for effective fraud management. The research by Cross and Blackshaw (2014) has signified the importance of sharing fraud related data with other organisations as an effective practice in fraud management. On the top, Bierstaker *et al.* (2006) have studied the importance of vulnerability analysis and found that it has a significant impact on the performance of fraud detection and prevention. Finally, the research by Miri-Lavassani *et al*., (2009) presents a good insight into identity fraud and suggest to simplify the process of fraud analysis for better results.

The literature in Table VII covers a variety of industries and different contexts, and present many practices to manage identity frauds effectively. However, none of these studies has focused on other aspects of identity fraud management. Therefore, the present study investigates the extant literature to present a holistic picture of identity fraud management and suggest a comprehensive set of practices at each stage of fraud management.

~~*1.4.5*~~5.2.6 ~~4.2.6~~ Policy

The policy may be defined as "wisdom in the management of affairs". In practice, a policy is a guideline to perform activities aligned with overall business strategies. Many researchers ~~(Such as;~~ (Chang and Lin, 2007; Singh *et al.*, 2013; Siponen *et al.*, 2009) have emphasised the importance of policy in the management of various issues.

The extant literature discusses three aspects of policy, such as; policy development, updating and compliance. The following table depicts a picture of literature on policy in the fraud management and information security contexts.

Insert table VIII here

Table VIII shows that a number of studies have highlighted the significance of policies in the management of various operations. At the outset, many studies (Albrechtsen and Hovden, 2010;

Bechtsoudis and Sklavos, 2012; Chen *et al.*, 2015; Liu *et al.*, 2010; Parsons *et al.*, 2014; Rhee *et al.*, 2012; Singh *et al.*, 2013; Siponen *et al.*, 2014; Soomro *et al.*, 2016; Verdon, 2006;) have investigated the policies related issues and their significance in information security for prevention of identity theft, which is pre-requisite for identity fraud prevention. Their findings are related to the development, communication, awareness and compliance with policies but are limited to information security, which is only a part of fraud management. Hence, none of these studies offers a holistic view of fraud management.

On the other hand, studies by Calvasina~~,~~ *et al.* (2007) suggested the development of policies but limited to the prevention of internal staff information. Some researchers (Bierstaker *et al.*, 2006; Njenga and Osiemo, 2013; Wright, 2007) have forwarded notable suggestions for having comprehensive policies on frauds. These studies also highlight the significance of policy awareness and training and monitoring for effective compliance. However, these practices have been suggested on their own, which may not work effectively in isolation. Therefore, these practices are suggested as a stage or a part of comprehensive identity fraud management. Managerial practices regarding development, communication, awareness and compliance of policies would benefit more if made as a part of holistic identity fraud management. Therefore, this study suggests these practices as an integral part of identity fraud management for e-tail industry.

~~1.4.6~~5.2.7 ~~4.2.7~~ Investigation

Investigation in identity fraud context may be defined as the conduct of a systematic enquiry and collection of evidence to examine and observe the facts of identity frauds. Fraud investigations are usually carried out by state law enforcing agencies, but in the absence of more state intervention in fraud investigation, the fraud continues to grow (Lewis *et al.*, 2014). Therefore, business firms are suggested to initiate the investigations at their end, and after successful investigation, these firms should report fraud cases with related evidence to law enforcing agencies for further process, which leads to successful prosecution. The following table represents the studies on the investigation of frauds.

Insert table IX

Table ~~VII~~IX presents literature on fraud investigation and its practices. The studies by Wilhelm (2004), Furlan and Bajec (2008) and Rose et al. (2015) emphasise the significance of investigation for evidence collection and prosecution to recover the losses. Wilhelm (2004) and Cross and Blackshaw (2014) have suggested evidence management for effective investigations. Additionally, Brooks and Button (2011) suggest business firms carry out fraud

investigations at the business end and to be the part of law enforcing agencies for further investigations. Such practices would enhance the coordination between the organisations and will help to reduce dependency on police, which is critical to get their interest on business frauds (Cross and Blackshaw, 2014; Lewis *et al.*, 2014; Lewis *et al.*, 2014).

On the significance of investigators role, Wilhelm (2004) and Lewis et al. (2014) suggest that quality of investigations depends on the skills, knowledge and experience of investigators; how they collect, analyse and present the evidence. Lewis et al. (2014) also suggest online business organisations to involve in fraud investigations and prosecution. For online fraud investigations, Edge and Sampaio (2009) have suggested the collection of evidence through data mining to identify fraud trends, patterns and locations and social media.

Finally, on the organisational role in collecting and preserving the evidence of digital frauds, Gogolin and Jones (2010) suggest that business firms should involve in investigation process as they have more resources to perform it effectively. Although, these suggestions are noteworthy in identity fraud management but are limited to investigations and prosecution process, while practices at other stages are missing in these studies. Therefore, present research synthesises the extant literature to give a holistic view on identity fraud management.

~~1.4.7~~5.2.8 ~~4.2.8~~ Prosecution

Once the investigation has been completed with enough evidence and suspected fraudsters have been located, the next step is to recover the losses through a prosecution process. In fraud arena, prosecution serves three objectives first, to punish the fraudster to deter further frauds second, to enhance a firm's reputation for fraud deterrence and third, to recover the loss or possible restitution (Wilhelm, 2004). At this stage, organisations are suggested to work with law courts and other law enforcing agencies for legal proceedings. Wilhelm (2004), argues that consistent and visible coordination between supportive legislative and regulatory activities is unavoidable to stop fraudulent activities. The literature on prosecution is presented in the table below.

Insert table X here

Table ~~I~~X presents literature on fraud prosecution. In this regard, Lewis *et al.* (2014) suggest the business organisations to actively be involved in prosecution process because of less intervention from state agencies. The research by Gogolin and Jones (2010), is worth mentioning here because it is related to issues regarding investigation and prosecution identity fraud. At the outset, Gogolin and Joness (2010) suggest for an information security plan developed with the prosecution in mind, to make the system helping in the prosecution process.

Business organisations are also suggested to know legal system and requirements to make a fraud prosecutable. Furthermore, Wang~~,~~ *et al.* (2006) argue that business organisations avoid investing in prosecution activities, which leads to its ineffectiveness. These studies are focused on legal aspects of fraud management which cannot work in isolation, so a comprehensive set of practices is required for effective identity fraud management. Therefore, this study investigates the extant literature and presents a holistic view of identity fraud management and forwards a set of practices at each stage of fraud management.

To sum it up, this study presents extant literature on each stage of fraud management. At first, the literature was presented to draw a clear picture of what an identity fraud management is. The work of various authors was presented to coincide a complete set of identity fraud management. After that using the systematic literature review approach literature at each stage of identity fraud management was sought.

6. Discussions

In online business domain, identity fraud is generally treated as a technological issue. Therefore a large number of articles is limited to the technological arrangements. Only a few studies, (Amasiatu, 2016; Jamieson *et al.*, 2007; Kumar, *et al.*, 2007; Wilhelm, 2004) have addressed the issue comprehensively to include the eight stages of fraud management and suggest organisational, social and technological arrangements. While majority of the studies have focused on one or two stages of fraud management.

Extant literature has various studies on each stage of fraud management. On deterrence, there have been some studies (Dorminey *et al.*, 2012; Ijeoma and Aronu, 2013; Sperdea *et al.*, 2011) focusing on both aspects i.e. customer education and fear appeal. Whereas most of the studies are either focused on customer education or fear appeal (see Table III). Although, significant research has been found on different aspects of deterrence however, least has been done in identity fraud management in e-tail context. ~~most of the studies are based on fear appeal and general deterrence theories. Less literature has been found on identity fraud management in the online sector, and none of these studies focused on e-tail organisations.~~

At~~In~~ the prevention stage, majority~~most~~ of the literature is focused on information security and data breach, although these are parts of identity fraud prevention, yet more is needed in given context. The literature on identity fraud prevention is mainly focused on information security and authentication. Thus, studies by Amori, (2008), Bose and leung (2013), Boyer, (2007),

Devos and pipan, (2009), Gerard *et al.* (2005) and Wang (2006) are focused on information security measures to prevent online frauds. While Bang *et al.* (2012), Lee and yu, (2012) and Usman and Shah, (2013) have suggested to improve authentication system to prevent such frauds. Apart from these, Archer, (2012) and Dyer, (2013) have focused on staff training to prevent online frauds.

In fraud management, detection has a critical role, which attracted the attention of many researchers. A large number of articles on fraud detection is also an evidence for its importance (see Table V). For detection of fraud, extant literature is focused on behavioural aspects, bio-metric technologies, and cue based auto detection system (see Table V). ~~The existing studies on identity fraud prevention mostly focus on authentication. For identity fraud detection, significant work has been undertaken on technological aspects. Mostly, account analytic, and fraud cues with the automated flagging system have been suggested for identity fraud detection, but no study has been found to focus on e-tail organisation.~~

The extant literature suggests real-time mitigation to minimise the fraud losses and recovery of accounts. At this stage, majority of the studies suggest to keep and regularly update customers' records, which would help to verify genuine customer identities in case of any suspicious transaction. Additionally, some articles (Kahn and Liñares-Zegarra, 2016; Tan *et al.*, 2016) also suggest contacting customers for identity verification. For effective mitigation knowledge sharing is also recommended by some authors (Cross and Blackshaw, 2014; Lewis *et al.*, 2014).

~~It also suggests the business organisations dealing with identity fraud victims properly~~. Most of the studies on fraud analysis are focused on information security risks. More research is needed to explore the significance of identity fraud analysis and its related practices especially focused on e-tail sector. There is significant literature on policy and related issues but mostly in information security context. Some authors (Njenga and Osiemo, 2013), emphasise the significance of policy in identity fraud management, but no studies were found in e-tail context. Also, the detail of managerial practices in policy development, communication, awareness and compliance were presented by exploring the literature (see Table VIII). The studies on fraud investigations and prosecution, mostly emphasise business firms to get involved in private investigations and follow the prosecution process in order to get better results. This is a common view that law enforcing agencies are more involved in other critical issues, therefore, e-tailers are suggested for private investigations and development of close coordination with police. For effective prosecution, e-tailers are also advised to have knowledge on state laws regarding fraud prosecution. ~~were also presented, which suggest that business organisations come forward for private investigations and play an active role in the prosecution.~~

The findings show that extant literature has some studies on each stage of fraud management, but none of these studies has presented a comprehensive picture to understand the challenge and countermeasures. These individual studies are focused on three main aspects of identity fraud management, i.e. the technological, human and organisational. Hence it may be deduced that an effective fraud management is an association of technological, human and organisations practices.

Reflected on the extant literature, this study also found that identity fraud management~~IDFM~~ is not a technological but a managerial issue, which needs attention from all factors of business operations and focuses on top management. The accumulated practices at each stage would also need a contribution from top management to operational staff and from strategic planning to day to day business operations. Therefore, e-tailers are advised to revisit their instance of identity fraud management take~~s~~ it as a management challenge rather than a technological one.

~~This research makes two unique contributions towards the body of literature, first by synthesising the extant literature at each stage of the fraud management to give a holistic approach to identity fraud management. Second, suggesting a detailed list of practices of at each stage of fraud management for effective use in identity fraud management in e-tail sector. It will help academicians to forward this field of research by further research in given context. Suggestions forwarded by this research will also help the e-tailers to manage identity frauds effectively, to reduce their fraud losses and maintain their market share with better customer relationships. For real-world, the present study suggests e-tailers change their stance on fraud management and take it as a management challenge and reflect on the practices mentioned above to include technological, human and organisational measures for improved management of identity frauds.~~

~~4.~~7. Conclusions

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

presents a holistic view of identity fraud management and forwards a comprehensive set of related practices. We found that most of the studies are focused on one or some aspects, which may not cover the whole of fraud management. This research also found that most firms treat identity frauds as a technological issue.

We found that the eight stages of ~~identity~~ fraud management ~~consists of eight sets of practices,~~ named as; deterrence, prevention, detection, mitigation, analysis, policy, investigation and prosecution, suggested by Wilhelm ~~which are commonly termed as stages of fraud management.~~ (Wilhelm, 2004) are equally important to manage identity frauds in e-tail sector. ~~The related literature was reviewed, and practices at each stage were given.~~ This study found that identity fraud is generally treated as a technological issue, only a few studies have comprehensively focused to include organisational, social and technological aspects of fraud management. This study ~~We~~ suggests that identity fraud management is a managerial issue rather than a technological, so it should include technological, human and organisational arrangements. This research synthesise the extant literature on fraud management, presents a holistic view of identity fraud management and suggest managerial practices at each stage of identity fraud management. ~~Following are the key research findings.~~ Guidelines are also given for e-tail managers to effectively manage identity fraud, control losses and develop favourable customer relationship. This research will also help in building customers' trust on online shopping, which will lead to e-commerce development.

~~➢ Provided a holistic view of identity fraud management by synthesising the extant literature.~~

~~➢ Forwards details on practices at each stage of identity fraud management.~~

~~➢ Offers the practical world a comprehensive view of identity fraud management and practices at each stage for enhanced effectiveness.~~

~~➢ Coincide a comprehensive list of guidelines for online retailers to improve their position to combat identity frauds.~~

7.1 Theoretical contribution

This research draws a significant and representative portion of extant literature into a single, comprehensive study. It would help academics to understand the art of the state in identity fraud management and will open new avenues for future research. This study expended extant literature by delineating a set of comprehensive organisational, social and technological aspects

of identity fraud management, which presents a holistic view of identity fraud management. Such a broader view of identity fraud management will open new avenues for future research. The literature shows that much of the research is focused on the e-tailers role within the boundaries of their business. However, other stake holders such as customers, banks and identity issuing authorities, do have critical role to play, which are not much focused in management of these frauds. Therefore, this study also invites researchers to include other stakeholders in development of effective framework for identity fraud management. ~~This research makes two unique contributions towards the body of literature, first by synthesising the extant literature at each stage of the fraud management to give a holistic approach to identity fraud management. Second, suggesting a detailed list of practices of at each stage of fraud management for effective use in identity fraud management in e-tail sector. It will help academicians to forward this field of research by further research in given context.~~

7.2 Practical contribution

Management of identity fraud is a significant challenge for e-tailers throughout the globe. This study will help e-tail managers to understand a holistic view of identity fraud management. Generally, identity fraud management has been regarded as a technological issue. This study presents a comprehensive set of managerial practices to effectively manage identity frauds. Broader view of identity fraud management will also help managers to consider organisational, social and technological arrangements towards better performance in the management of identity frauds. E-tailers are the ultimate bearers of identity frauds and literature suggests that mostly identity information is stolen at customer side. Therefore, e-tailers should go beyond the boundaries to create awareness and educate customers to minimise the risk of such frauds. ~~Suggestions forwarded by this research will also help the e-tailers to manage identity frauds effectively, to reduce their fraud losses and maintain their market share with better customer relationships. For real-world, the present study suggests e-tailers change their stance on fraud management and take it as a management challenge and reflect on the practices mentioned above to include technological, human and organisational measures for improved management of identity frauds.~~

7.3 Limitations and future research

All of the academic studies have certain limitations, which also is the case with this study. This study used four databases i.e. IEEE Xplore, Science Direct (Elsevier), Emerald Insight, Business Source Complete and Computer and Applied Science Complete and google search engine to include a maximum number of related articles. However, there are still possibilities

of missing some articles. This study used Soomro *et al.* (2016) literature review process, which the authors found workable to include substantial portion of identity fraud management literature. This research suggest future studies to include other databases. This study used a rigorous approach for searching the related literature. However, there are still some limitations especially regarding the used search terms and identified articles. At the outset, only literature in the English language was targeted. Thus studies in other languages were not included. Furthermore, only predefined key terms were used, which may leave some literature unspotted. An alternate search process of gathering key terms during the literature analysis process is also suggested for future studies.

Finally, we suggest testing of our findings through empirical studies based on quantitative surveys and qualitative case studies, to enhance the understanding of a holistic view of identity fraud management highlighted in this study.

References

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. Available at: https://dblp.org/db/conf/amcis/amcis2014.html (accessed August 28, 2017).

Albrecht, C., Albrecht, C. and Tzafrir, S. (2011), "How to protect and minimize consumer risk to identity theft", *Journal of Financial Crime,* Vol. 18 No 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,* Vol. 29 No. 4, pp. 432-445.

Ali, M. and Miller, L. (2017), "ERP system implementation in large enterprises–a systematic literature review", *Journal of Enterprise Information Management,* Vol. 30 No. 4, pp. 666-692.

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. IEEE, 13-14 December.

Al-Kurdi, O., El-Haddadeh, R. and Eldabi, T. (2018), "Knowledge sharing in higher education institutions: a systematic review", *Journal of Enterprise Information Management,* Vol. 31 No. 2, pp. 226-246.

Allan, T. and Zhan, J. (2010), "Towards Fraud Detection Methodologies", *5th International Conference on Future Information Technology* (FutureTech), Busan, Korea (South). 21-23 May, available at https://dl.acm.org/citation.cfm?id=1853079&picked=prox. (accessed on 19 June 2017).

Alrashed, F. (2016), "Stealing More than Just Identity", *International Journal of Scientific & Engineering Research,* Vol. **7** No. 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 Thesis, available at www.clock.uclan.ac.uk (accessed on 12 February 2017)

Amori, G. (2008), "Preventing and responding to medical identity theft", *Journal of Healthcare Risk Management,* Vol. 28 No. 2, pp. 33-42.

Anderson, R.M. (2010), "A proposal for calculating reimbursed victims of financial identity theft under the federal sentencing guidelines", *Brooklyn Journal of Corporate, Financial & Commercial Law,* Vol. 5 No. 2, pp. 447.

Ann McGee, J. and Ralph Byington, J. (2015), "Corporate identity theft: A growing risk", *Journal of Corporate Accounting & Finance,* Vol. 26 No. 5, pp. 37-40.

Arachchilage, N.A.G. and Love, S. (2014), "Security awareness of computer users: A phishing threat avoidance perspective2, *Computers in Human Behavior,* Vol. 38 Issue September, pp. 304-312.

Arachchilage, N.A.G. and Love, S. (2013), "A game design framework for avoiding phishing attacks", *Computers in Human Behavior,* Vol. 29 No. 3, pp. 706-714.

Archer, N. (2012), "Consumer identity theft prevention and identity fraud detection behaviours", *Journal of Financial Crime,* Vol. 19 No. 1, pp. 20-36.

Baer, M.H. (2008), "Linkage and the Deterrence of Corporate Fraud", *Virginia Law Review,* Vol. 94 No. 6, pp. 1295-1365.

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,* Vol. 32 No. 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,* Vol. 3 No. 1, pp. 7-13.

Bechtsoudis, A. and Sklavos, N. (2012), "Aiming at higher network security through extensive penetration tests", *IEEE Latin America Transactions,* Vol. 10 No. 3, pp. 1752-1756.

Becker, R.A., Volinsky, C. and Wilks, A.R. (2010), "Fraud detection in telecommunications: History and lessons learned", *Technometrics,* Vol. 52 No. 1, pp. 20-33.

Behdad, M., Barone, L., Bennamoun, M. and French, T. (2012), "Nature-inspired techniques in the context of fraud detection", *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on,* Vol. 42 No. 6, pp. 1273-1290.

Bierstaker, J.L., Brody, R.G. and Pacini, C. (2006), "Accountants' perceptions regarding fraud detection and prevention methods", *Managerial Auditing Journal,* Vol. 21 No. 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),* Vol. 5 No. 2, pp. 120-127.

Bose, I. and Leung, A.C.M. (2013), "The impact of adoption of identity theft countermeasures on firm value", *Decision Support Systems,* Vol. 55 No. 3, pp. 753-763.

Boyer, M.M. (2007), "Resistance (to Fraud) Is Futile", *Journal of Risk & Insurance,* Vol. 74 No. 2, pp. 461-492.

Brody, R.G., Mulig, E. and Kimball, V. (2007), "Phishing, pharming and identity theft", *Academy of Accounting and Financial Studies Journal,* Vol. 11 No. 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,* Vol. 84 No. 4, pp. 305-319.

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,* Vol. 10 No. 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,* Vol. 95 No. 1, pp. pp. 91-101.

Cavusoglu, H. and Raghunathan, S. (2004), "Configuration of Detection Software: A Comparison of Decision and Game Theory Approaches", *Decision Analysis,* Vol. 1 No. 3, pp. 131-148.

Chang, S.E. and Lin, C. (2007), "Exploring organizational culture for information security management", *Industrial Management & Data Systems,* Vol. 107 No. 3, pp. 438-458.

Chang, W. and Chang, J. (2011), "A novel two-stage phased modeling framework for early fraud detection in online auctions", *Expert Systems with Applications,* Vol. 38 No 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,* Vol. 55 No. 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", paper presented at the Pacific Asia Conference on Information Systems (PACIS), July 5-9, Singapore available at: https://aisel.aisnet.org/pacis2015/ (accessed 8 August 2017).

CIFAS (2018a), "Fraudscape 2016", *a*vailable at: https://www.cifas.org.uk/insight/reports-trends (accessed 3 December 2017).

CIFAS (2018b), "Fraudscape 2017", *a*vailable at: https://www.cifas.org.uk/insight/reports-trends/fraudscape-report-2017 (Accessed 12 January 2018).

CIFAS (2018c), "Identity fraud soars to new levels", *a*vailable at https://www.cifas.org.uk/newsroom/identity-fraud-soars-to-new-levels (accessed: 23 February 2018).

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,* Vol. 38 No. 5, pp. 1045-1052.

Coulson-Thomas, C. (2017), "Fraud, security risks and corporate responses", in Ahluwalia J. S. (eds.) *"Corporate Ethics & Risk Management in an uncertain world",* IOD Publishing, Mumbai, pp. 67-76.

Cressey, D.R. (1950), "The criminal violation of financial trust", *American Sociological Review,* Vol. 15 No. 6, pp. 738-743.

Cross, C. and Blackshaw, D. (2014), "Improving the police response to online fraud", *Policing: A Journal of Policy and Practice,* Vol. 9 No. 2, pp. 119-128.

Devos, J. and Pipan, I. (2009), "The Role of IT/IS in Combating Fraud in the Payment Card Industry", *Journal of Internet Banking & Commerce,* Vol. 14 No. 3, pp. 1-17.

Dorfleitner, G. and Jahnes, H. (2014), "What factors drive personal loan fraud? Evidence from Germany", *Review of Managerial Science,* Vol. 8 No. 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,* Vol. 27 No. 2, pp. 555-579.

Dyer, R. (2013), "External reactive detection v. internal proactive prevention: The holistic approach to integrate change", *Journal of Financial Crime,* Vol. 20 No. 3, pp. 287-292.

Edge, M.E. and Falcone Sampaio, P.R. (2009), "A survey of signature based methods for financial fraud detection", *Computers & Security,* Vol. 28 No. 6, pp. 381-394.

Furlan, S. and Bajec, M. (2008), "Holistic approach to fraud management in health insurance", *Journal of Information and Organizational Sciences,* Vol. 32 No. 2, pp. 99-114.

Gerard, G.J., Hillison, W. and Pacini, C. (2005), "Identity theft: the US legal environment and organisations' related responsibilities", *Journal of Financial Crime,* Vol. 12 No. 1, pp. 33-43.

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 March 2018).

Ghosh, M. (2010), "Mobile ID fraud: the downside of mobile growth", *Computer Fraud & Security,* Vol. 2010 No. 12, pp. 8-13.

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,* Vol. 19 No. 3, pp. 109-117.

Hardouin, P. (2009), "Banks governance and public-private partnership in preventing and confronting organized crime, corruption and terrorism financing", *Journal of financial crime,* Vol. 16 No. 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,* Vol. 41 No. 5, pp. 2345-2352.

Hollinger, R.C. and Clark, J.P. (1983), "*Theft by employees",* Lexington Books, Lexington, MA.

Holt, T.J. and Turner, M.G. (2012), "Examining risks and protective factors of on-line identity theft", *Deviant Behavior,* Vol. 33 No. 4, pp. 308-323.

Ijeoma, N. and Aronu, C. (2013), "The Impact of Fraud Management on Organizational Survival in Nigeria", *American Journal of Economics,* Vol. 3 No. 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), January 3-6, Waikoloa, Hawaii, available at https://www.computer.org/csdl/proceedings/hicss/2007/2755/00/27550157c-abs.html. (accessed 2 March 2017)

Javelin Strategy (2018), "Identity fraud hits record high 154 million U.S. victims 2016, Up 16 percent according new Javelin Strategy and research study", *a*vailable at:

https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new (accessed 12 January 2018).

Jesson, J., Matheson, L. and Lacey, F.M. (2011), "*Doing your literature review: Traditional and systematic techniques", Sage* Publications, London.

Kahn, C.M. and Liñares-Zegarra, J.M. (2016), "Identity Theft and Consumer Payment Choice: Does Security Really Matter?", *Journal of Financial Services Research,* Vol. 50 No 1, pp. 121-159.

Kahn, C.M. and Roberds, W. (2008), "Credit and identity theft", *Journal of Monetary Economics,* Vol. 55 No 2, pp. 251-264.

Kolb, N. and Abdullah, F. (2009), "Developing an information security awareness program for a non-profit organization", *International Management Review,* Vol. 5 No 2, pp. 103.

Kuhn, J.R. and Morris, B. (2017), "IT internal control weaknesses and the market value of firms", *Journal of Enterprise Information Management,* Vol. 30 No. 6, pp. 964-986.

Kumar, V. and Kumar, D. and De Grosbois, D. (2007), "Collaboration in Combating Identity Fraud", working paper, [SL 2007-034] Carleton University Sprott School of Business, Carleton University, Ottawa, November.

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,* Vol. 6 No. 4, pp. 309-315.

Leasure, P. and Zhang, G. (2017), "That how they taught us to do it: Learned Deviance and Inadequate Deterrents in Retail Banking", *Deviant Behaviour,* Vol. 33 No. 1, pp. 1-14.

Lee, S. and Yu, J. (2012), "Success model of project management information system in construction", *Automation in Construction,* Vol. 25 Issue 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,* Vol. 42 No. 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,* Vol. 12 No. 3, pp. 287-303.

Meinert, M.C. (2016), "In the Fight Against Fraud, Strong Leadership is KEY", *ABA Banking Journal,* Vol. 108 No. 2, pp. 55-56.

Miri-Lavassani, K., Kumar, V., Movahedi, B. and Kumar, U. (2009), "Developing an identity fraud measurement model: a factor analysis approach", *Journal of Financial Crime,* Vol. 16 No. 4, pp. 364-386.

Narain Singh, A., Gupta, M. and Ojha, A. (2014), "Identifying factors of organizational information security management", *Journal of Enterprise Information Management,* Vol. 27 No. 5, pp. 644-667.

Nissan, E. (2012), "An Overview of Data Mining for Combating Crime", *Applied Artificial Intelligence,* Vol. 26 No. 8, pp. 760-786.

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,* Vol. 1 No. 7, pp. 490-507.

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,* Vol. 42 Issue 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,* Vol. 3 No. 1, pp. 186-197.

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,* Vol. 47 No. 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,* .

Prabowo, H.Y. (2011), "Building our defence against credit card fraud: a strategic view", *Journal of Money Laundering Control,* Vol. 14 No. 4, pp. 371-386.

Prosch, M. (2009), "Preventing Identity Theft Throughout the Data Life Cycle", *Journal of Accountancy,* Vol. 207 No. 1, pp. 58-62.

Rhee, H., Ryu, Y.U. and Kim, C. (2012), "Unrealistic optimism on information security management", *Computers & Security,* Vol. 31 No. 2, pp. 221-232.

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,* Vol. 72 No. 3, pp. 22-24.

Seda, L. (2014), "Identity theft and university students: do they know, do they care?", *Journal of Financial Crime,* Vol. 21 No. 4, pp. 461-483.

Shah, M. and Okeke, R.I. (2011), "A Framework for Internal Identity Theft Prevention in Retail Industry", *in* European Intelligence and Security Informatics 2011 proceedings of the Conference in Athens, Greece. IEEE Xplore pp. 366-371

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,* Vol. 14 No. 4, pp. 225-239.

Siponen, M., Mahmood, M.A. and Pahnila, S. (2009), "Are Employees Putting Your Company At Risk By Not Following Information Security Policies?", *Communications of the ACM,* Vol. 52 No. 12, pp. 145-147.

Siponen, M., Mahmood, M.A. and and Pahnila, S. (2014), "Employees' adherence to information security policies: An exploratory field study", *Information & Management,* Vol. 51 No. 2, pp. 217-224.

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,* Vol. 36 No. 2, pp. 215-225.

Sperdea, N.M., Enescu, M. and Enescu, M. (2011), "Challenges of managing e-commerce", *Economics, Management and Financial Markets,* Vol. 6 No. 2, pp. 194.

Swathi, M. and Kalpana, K. (2013), "Spirit of Identity Fraud And Counterfeit Detection", *International Journal of Computer Trends and Technology,* Vol. 4 No. 6, pp. 1891-1895.

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,* Vol. 53 No. 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,* Vol. 141 No. 6, pp. 1178-1204.

Taylor, E. (2016), "Mobile payment technologies in retail: a review of potential benefits and risks", *International Journal of Retail & Distribution Management,* Vol. 44 No. 2, pp. 159-177.

Tsaih, R., Lin, W. and Chen, A. (2008), "Safeguard gaps and their managerial issues", *Industrial Management & Data Systems,* Vol. 108 No. 5, pp. 669-676.

Tsavli, M., Efraimidis, P.S., Katos, V. and Mitrou, L. (2015), "Reengineering the user: privacy concerns about personal data on smartphones", *Information & Computer Security,* Vol. 23 No. 4, pp. 394-405.

Usman, A.K. and Shah, M.H. (2013), "Strengthening e-banking security using keystroke dynamics", *The Journal of Internet Banking and Commerce,* Vol. 18 No. 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,* Vol. 51 No. A, pp. 180-187.

Verdon, D. (2006), "Security policies and the software developer", *IEEE Security & Privacy,* Vol. 4 No. 4, pp. 42-49.

Vidalis, S. and Angelopoulou, O. (2014), "Assessing identity theft in the Internet of Things", *Journal of IT Governance Practice,* Vol. 2 No. 1, pp. 15-21.

Vijaya Geeta, D. (2011), "Online identity theft–an Indian perspective", *Journal of Financial Crime,* Vol. 18 No. 3, pp. 235-246.

Wang, S. and Noe, R.A. (2010), "Knowledge sharing: A review and directions for future research", *Human resource management review,* Vol. 20 No. 2, pp. 115-131.

Wang, W., Yuan, Y. and Archer, N. (2006), "A contextual framework for combating identity theft", *IEEE Security and Privacy,* Vol. 4 No. 2, pp. 30-38.

Weisman, A. and Brodsky, M. (2011), "Fighting fraud with both fists", *The CPA Journal,* Vol. 81 No. 1, pp. 11.

Wilhelm, W.K. (2004), "The fraud management lifecycle theory: a holistic approach to fraud management", *Journal of Economic Crime Management,* Vol. 2 No. 2, pp. 1-38.

Williams, M.D., Rana, N.P. and Dwivedi, Y.K. (2015), "The unified theory of acceptance and use of technology (UTAUT): a literature review", *Journal of Enterprise Information Management,* Vol. 28 No. 3, pp. 443-488.

Wright, R. (2007), "Developing effective tools to manage the risk of damage caused by economically motivated crime fraud", *Journal of Financial Crime,* Vol. 14 No. 1, pp. 17-27.

Xu, J., Sung, A.H. and Liu, Q. (2007), "Behaviour Mining for Fraud Detection", *Journal of Research & Practice in Information Technology,* Vol. 39 No. 1, pp. 3-18.

Yang, H. and Tate, M. (2012), "A descriptive literature review and classification of cloud computing research", *Communications of the Association for Information Systems,* Vol. 31 No. 2, pp. 35-60.

Yelland, M. (2013), "Fraud in mobile networks", *Computer Fraud & Security,* Vol. 2013 No. 3, pp. 5-9.

Table I. Showing number and percentage of 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 (first six months)
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, 2018c; CIFAS, 2018b; CIFAS, 2018a)

Table II. List of keywords

S. No	Keywords	S. No	Keywords
1	Fraud	2	Identity fraud
3	Fraud management	4	Identity fraud management
5	Fraud deterrence	6	Fraud prevention
7	Fraud detection	8	Fraud mitigation
9	Fraud analysis	10	Fraud policy
11	Fraud investigation	12	Fraud prosecution

Table III. The articles discussing the importance of and practices at deterrence stage

Findings	References
Organisations need to take two significant actions for effective fraud deterrence; 1 educate their customers, 2 send fear messages to the society for fraudsters being caught and punished.	(Sperdea *et al.*, 2011; Dorminey *et al.*, 2012; Ijeoma and Aronu, 2013)
Educating the customers on identity theft risk, its methods and precautionary measures have a significant impact on fraud deterrence. For effective deterrence, organisations should advise their customers to check their credit file, bank statements and other business accounts regularly and not to share personal information on social media.	(Seda, 2014; Arachchilage and Love, 2013; Kolb and Abdullah, 2009)
Awareness of the risk of identity theft and self-efficacy of customers has a critical impact on identity theft deterrence.	(Holt and Turner, 2012; Arachchilage and Love, 2013)
Customers' knowledge and awareness of identity frauds have a significant impact on the fraud deterrence.	(Albrecht *et al.*, 2011; Brody *et al.*, 2007; Copes *et al.*, 2010)
Impact of fraud deterrence can be increased by creating the fear of being caught and punished. Similarly, the certainty of punishment on frauds has a significant impact on deterrence.	(Dorminey *et al.*, 2012; Leasure and Zhang, 2017)
Deterrence depends on the fraudsters' evaluation of risk, so societies should increase the expected penalties and punishments for fraudsters	(Baer, 2008)

Table IV. The articles discussing the importance of and practices at prevention stage.

Findings	References
Organisations should implement strong authentication system to prevent identity frauds in online organisations.	(Bang *et al.*, 2012; Lee and Yu, 2012; Usman and Shah, 2013).
Prevention is an effective tool against predicted frauds, and it is mostly based on IT/IS solutions combined with organisational arrangements.	(Devos and Pipan, 2009).
Organisations should implement effective measures to prevent internal frauds.	(Bierstaker *et al.*, 2006).
Organisations should regularly manage the risk of online identity theft.	(Amori, 2008; Tsavli *et al.*, 2015; Taylor, 2016).
Regular monitoring and updating of internal and external security systems are critical to prevent identity theft.	(Amori, 2008; Gerard *et al.*, 2005)
Prevent identity theft through screening and management mechanisms involving all stakeholders.	(Wang *et al.*, 2006)
Efficient prevention technologies yield more incentives for investments.	(Boyer, 2007; Bose and Leung, 2013).
Training is a significant practice to improve the employee performance in fraud prevention.	(Dyer, 2013; Archer, 2012).

Table V. The articles discussing the importance of and practices at the detection stage

Findings	References
A combination of both fraud cues and behavioural detection technologies could help to detect these frauds.	(Edge and Falcone Sampaio, 2009; Ghosh, 2010; Xu *et al.*, 2007)
Behavioural technologies proactively detectidentity fraud through aggressively considering factors and patterns based on identity, demographic information, shopping history, product types, devices used and addresses.	(Nissan, 2012; Anderson, 2010; Ghosh, 2010)
The organisations also use the device recognition to detect identity frauds through linking customer devices with accounts, which to identify the suspicious activities on the account.	(Peotta *et al.*, 2011; Ghosh, 2010)
The device recognition also used with IP (internet protocol) to detect the location of customers, this approach enhances the performance of account analytics in detection.	(Cheng *et al.*, 2015; Tan *et al.*, 2016)
Fraud detection systems rely on knowledge, skills and expertise of fraud managers or domain experts.	(Vahdati and Yasini, 2015)
Detection cues require regular upgrading, maintenance and require accuracy in threshold and parameter definition according to identity fraud trends.	(Allan and Zhan, 2010)
The organisations should monitor individual identities and ask for identity document as a proof of identity for early identity fraud detection.	(Kahn and Roberds, 2008; Amori, 2008; Albrecht *et al.*, 2011)
Online fraud detection is difficult without automation of the transaction systems.	(Behdad *et al.*, 2012; Cavusoglu and Raghunathan, 2004)
For online organisations, it is impractical to control frauds without efficient fraud detection system	(Kundu *et al.*, 2009)
For effective online fraud management, an efficient fraud detection mechanism is necessary.	(Chang and Chang, 2011).

Table VI. The articles discussing the importance of and practices at mitigation stage

Findings	References
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.	(Tan *et al.*, 2016)
Organisations should monitor the customers' identities and ask for documentary proof for earlier detection of identity frauds.	(Albrecht *et al.*, 2011; Amori, 2008; Kahn and Liñares-Zegarra, 2016)
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.	(Becker *et al.*, 2010)
Know your customers. Update the customers' data. Monitor the customers' activities.	(Hardouin, 2009)
Identity fraud mitigation activity can be explained as efforts to minimise the fraud losses and correct the customer credit record in the minimum time.	(Wilhelm, 2004).
Sharing of identity fraud management knowledge with other organisations has a positive impact on mitigation and reduction of fraud losses.	(Cross and Blackshaw, 2014; Lewis *et al.*, 2014).
The business process has a significant impact on fraud risk mitigation	(Dyer, 2013).

Table VII. The articles discussing the importance of and practices at the analysis stage

Findings	References
The fraud analysis initiated with potential risk assessment, which includes identifying fraud trends, schemes, incentives (fraud losses), opportunities for fraud occurrence and loopholes in technological systems.	(Brody *et al.*, 2007; Rose *et al.*, 2015; Weisman and Brodsky, 2011)
Effective identity fraud management depends upon the performance of tools, techniques, strategies, processes and employees' who works at different stages of fraud management	(Dorminey *et al.*, 2012; Phan and Vogel, 2010; Vahdati and Yasini, 2015)
The evaluation activity helps to analyse employees' strengths, weaknesses, behaviour, quality of work and their issues.	(Vahdati and Yasini, 2015)
The evaluation is a process that helps the organisation to identify and understand the weakness and loopholes in tools and practices of identity fraud management.	(Tsaih *et al.*, 2008; Yelland, 2013)
The organisations share the fraudulent information with other companies and law enforcement agencies to reduce the risk of identity fraud.	(Cross and Blackshaw, 2014).
Vulnerability analysis helps to direct internal audit plan to spot the most vulnerable assets. It is a proactive step in fraud prevention and detection.	(Bierstaker *et al.*, 2006).
The use of complex analysing tools is an obstacle for assessment of identity fraud	(Miri-Lavassani *et al.*, 2009)

Table VIII. The articles discussing the importance of and practices at policy stage

Findings	References
Organisations should have comprehensive policies on information security. Organizations should create policy awareness. Train the employees on policy compliance methods and processes.	(Soomro *et al.*, 2016)
Let employees participate in the formulation, design and development of information security policies. Monitoring the compliance of security policy indeed influence the employees' perceptions and assumptions on security.	(Chen *et al.*, 2015)
Employees should regularly be trained on information security policies. Information security policies should periodically be reviewed with changing environment.	(Singh *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.	(Parsons *et al.*, 2014)
Create awareness, as it is a useful mechanism for policy compliance.	(Siponen *et al.*, 2014)
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.	(Njenga and Osiemo, 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.	(Singh *et al.*, 2013)
The policy should meet its purpose, be proactive to meet the challenges of known and unknown vulnerabilities and regular updates of policy are necessary	(Bechtsoudis and Sklavos, 2012).
The policies should focus on technical, organisational and human aspects of fraud management.	(Rhee *et al.*, 2012)
Involve the employees in policy development. Enhance the employees' knowledge of policy and compliance methods.	(Albrechtsen and Hovden, 2010)
Regularly update the policies for their effectiveness. Organisations should ensure the same policy for third party contractors regarding the information security and fraud management.	(Liu *et al.*, 2010)
Anti-fraud policies should also apply to the senior management.	(Wright, 2007)

Anti-fraud policies should establish the organisation's commitment to combating frauds and communicate organisational stance against frauds.	
Organisations should develop and maintain anti-fraud policies. Anti-fraud policies should be stand-alone and distinct from firm's code of conduct and ethical policy. A written acknowledgement should be ensured that all the staff have received a copy and understood it.	(Bierstaker *et al.*, 2006)
The policy is a layer to protect the organisation and employees, so not having a policy on fraud is bad, and having a policy without compliance is the same.	(Verdon, 2006).
Organisations should develop a policy to protect personal information which can be used in identity frauds.	(Calvasina *et al.*, 2007).

Table IX. The articles discussing the importance of and practices at the investigation stage

Findings	References
The evidence and facts collected through the investigation will support the successful prosecution or recovery of goods.	(Wilhelm, 2004; Furlan and Bajec, 2008; Rose *et al.*, 2015; Furlan and Bajec, 2008; Rose *et al.*, 2015).
For successful prosecution and recovery, the coordination with law enforcement agency (local police) is very important.	(Cross and Blackshaw, 2014; Wilhelm, 2004; Lewis *et al.*, 2014; Wilhelm, 2004; Lewis *et al.*, 2014).
The evidence management has a significant impact on identity fraud investigation, which requires exact information and intelligence to achieve the goal of prosecution and recovery.	(Cross and Blackshaw, 2014; Wilhelm, 2004)
Investigation depends upon skills, knowledge and experience of the investigator to collect, analyse and present the evidence.	(Wilhelm, 2004; Lewis *et al.*, 2014; Lewis *et al.*, 2014)
Investigators can collect evidence through data mining (using big data and knowledge discovery), identify and update most hits of frauds by trends, patterns and methods at a particular location and on social media.	(Edge and Falcone Sampaio, 2009)
The organisation should consider the private agencies or appoint a dedicated team of loss prevention managers to perform such for investigation, prosecution and recovery.	(Cross and Blackshaw, 2014; Lewis *et al.*, 2014; Lewis *et al.*, 2014)
Conduct investigations at the business end. Be involved in further investigations conducted by law enforcement agencies.	(Brooks and Button, 2011)
Online organisations should follow authentic electronic evidence preservation and integrity practices.	(Gogolin and Jones, 2010)

Table X. The articles discussing the importance of and practices at prosecution stage

Findings	References
Business organisations should involve in prosecution on account of less intervention from state agencies.	(Lewis *et al.*, 2014).
Low level of resources is invested in identity theft crime prosecutions.	(Wang *et al.*, 2006).
Information security plan should be developed with prosecution as a possible outcome; otherwise, it will not be helpful in managing identity frauds. Business organisations should be aware of legal requirements to make a fraud prosecutable.	(Gogolin and Jones, 2010).

List of changes corresponding to the reviewers' comments

Responses list reviewer 1.

Reviewer 1	Responses
1. Originality: Does the paper contain new and significant information adequate to justify publication?: Having read the paper, it is unclear to me where the research challenge lies and why it is a research challenge. This, should not be mistaken for a further question which is where is the scholarship; around which disciplinary domain, around the methodological approach etc.	The research gap has been defined in the section 3 especially last paragraph.
The paper is very interesting and comprehensive but it needs to fill a gap and the gap need identifying	The research gap has been defined in the section 3 especially last paragraph.
2. Relationship to Literature: Does the paper demonstrate an adequate understanding of the relevant literature in the field and cite an appropriate range of literature sources? Is any significant work ignored?: The literature review is very comprehensive with detailed emerged taxonomies that do make a contribution.	Thanks a lot for your comments No action needed
3. Methodology: Is the paper's argument built on an appropriate base of theory, concepts, or other ideas? Has the research or equivalent intellectual work on which the paper is based been well designed? Are the methods employed appropriate?: The SLR methodological approach is adapted. But more description is needed and also to justify it as an appropriate approach to address the gap identified in point 1.	The whole methodology section has been revised to include detailed description and justification of the approach to address the gap.
4. Results: Are results presented clearly and analysed appropriately? Do the conclusions adequately tie together the other elements of the paper?: The results are comprehensive and well-articulated.	Thanks a lot for your comments. No action required.
5. Practicality and/or Research implications: Does the paper identify clearly any implications for practice and/or further research? Are these implications consistent with the findings and conclusions of the paper?:	

The conclusion should also be an extrapolation of the key findings from the research and not a summary. So, there should be conclusions around the background theory, data theory/analysis and, key outcomes.	The conclusion section has been revised to discuss background theory, data analysis and key outcomes (see section 7).
6. Quality of Communication: Does the paper clearly express its case, measured against the technical language of the field and the expected knowledge of the journal's readership? Has attention been paid to the clarity of expression and readability, such as sentence structure, jargon use, acronyms, etc.: Finally, there needs to be a dedicated implications section; implications to theory and implications to practice/management.	Sections 7.1 and 7.2 has been added to address the theoretical and practical contributions.
This is a good paper with a slightly fine-tuned positioning needed to justify the need for this work.	A paragraph has been added to support the evidences for the need of this study (see details paragraph 10 section 3)

Responses list reviewer 2.

Reviewer 2	Responses
1. Originality: Does the paper contain new and significant information adequate to justify publication?: It is still not clear, the gap is not well addressed The author/s claimed that "none of the studies presents a holistic view of identity fraud management practices in online retail context" This cannot be enough to conduct a systematic literature review	The research gap has been defined in the section 3 especially last paragraph.
2. Relationship to Literature: Does the paper demonstrate an adequate understanding of the relevant literature in the field and cite an appropriate range of literature sources? Is any significant work ignored?: Yes, it is a systematic literature review presenting comprehensive research done in this domain	Thanks a lot for your comments No action needed
3. Methodology: Is the paper's argument built on an appropriate base of theory, concepts, or other ideas? Has the research or equivalent intellectual work on which the paper is based been well designed? Are the methods employed appropriate?: Yes, appropriate methodology, but the author/s need to explain how they reached to these combinations of keywords used for the search. The also need to justify based on what the assign the period of articles collected starts from 2004, why not before/after	The details on the selection and combination of keywords has been given. Justifications has been given on the period of included articles.
4. Results: Are results presented clearly and analysed appropriately? Do the conclusions adequately tie together the other elements of the paper?: Yes, but it was mixed with the findings	Findings have been separated as las two paragraphs of discussions section.
5. Practicality and/or Research implications: Does the paper identify clearly any implications for practice and/or further research? Are these implications consistent with the findings and conclusions of the paper?: Yes it identifies but the author did not address these implications	Sections 7.1 and 7.2 added to address the theoretical and practical contributions.

6. Quality of Communication: Does the paper clearly express its case, measured against the technical language of the field and the expected knowledge of the journal's readership? Has attention been paid to the clarity of expression and readability, such as sentence structure, jargon use, acronyms, etc.: yes	Thanks a lot for your comments. No action required
It is interesting and worth considering. Although I believe that it can be very much improved. Some of my comments as follow. The gap is not well addressed.	The research gap has been defined in the section 3 especially last paragraph.
I was not properly convinced of the need for such study, the author needs to support this need with evidences. e.g the author/s claimed that "none of the studies presents a holistic view of identity fraud management practices in online retail context" This cannot be enough to conduct a systematic literature review.	A paragraph has been added to support the evidences for the need of this study (see details paragraph 10 section 3)
The author/s need to explain how they reached to these combinations of keywords used for the search. The author/s jumped straight to the methodology. There should be some sections introducing the knowledge in this field.	Explanation about keywords and their combinations is given in the paragraph just before the table 2. A section has been added to introduce the knowledge in the field (see section 3).
They also need to justify based on what the assign the period of articles collected starts from 2004, why not before/after. Do you think the 5 sources of the data are covering the field? Please justify it	Justifications has been provided for the start period of collected articles (see paragraph 5 of section 4). Inclusion of five sources of data has been justified in paragraph 6 of section 4.
The analysis part is good, I recommend having another section before the conclusion summarising findings and discussion rather than including them in the conclusion. Also the contribution needs to be addressed	Thank you. No action required Discussions (section 6) has been added to before the conclusion. It summarises the findings and discussing the results. Sections 7.1 and 7.2 added to address the theoretical and practical contributions.