A Framework for ID Fraud Prevention Policies in E-Tailing Sector

1. **Dr. Mahmood Hussain Shah**
   Associate Professor
   Newcastle Business School
   Northumbria University
   Newcastle-upon-Tyne, UK.
   Mahmood.shah@northumbria.ac.uk

2. **Dr. Zahoor Ahmed Soomro**

   Lecturer
   Teesside University Business School
   Teesside University
   Middlesbrough.
   z.soomro@tees.ac.uk

3. **Dr. Jason Thatcher**

   Professor
   Fox School of Business
   Temple University
   Philadelphia, PA USA.
   Jason.thatcher@temple.edu

Abstract

Identity fraud could lead to loss of revenue, causes operational problems to e-tailers and damages the firm's reputation. Most research in this domain focuses on the security technologies or system users' security compliance related issues.. In this research, we direct attention to understanding the content and breadth of identity fraud prevention policies. We conducted thirty-three semi-structured interviews with employees and management of three large UK based e-tailers. It was found that while e-tailers have policies and other related arrangements that address information security and data theft prevention, they often lack policies on identity fraud prevention. Additionally, we found that the design of security policy awareness strategies, approaches to updating security policies, and enforcement of security compliance/audits, do not help prevent identity fraud. Based on this analysis, we developed the Identity Fraud Prevention Policies Framework (IFPF) to help e-tailers develop and implement better identity fraud prevention practices.

Keywords: e-tailing; identity fraud; policymaking; interviews; holistic approach, case-study approach; UK organisations

1. Introduction

The advancement in information technology has changed shopping habits, enabling e-tailing to become a norm. E-tailing saves time and offers a better comparison of products and prices and, as a result, an increasing number of businesses are introducing e-tailing. The differences in shopping patterns are also causing changes to the nature and methods of fraud. Identity fraud has become a growing problem for e-tailers in developed countries; for example, in the USA, 15.1 million customers suffered identity fraud in 2016 (Javelin Strategy, 2018).

Although online shopping was already very popular, COVID-19 has taken it to new highs. Due to the pandemic, online shopping has significantly increased amongst all age groups and this trend is expected to continue in the years to come (Kim, 2020). This is significant increase in online retail has been accompanied by an increase in identity fraud challenges. According to a study by Buil-Gil et al. (2021), UK online shopping fraud has increased by 50% since May 2019. These figures are expected to increase as the pandemic unfolds. Most of the online shopping frauds involve identity (CIFAS, 2020).

Identity fraud as defined in the literature is the use of stolen, cloned or counterfeited identity to commit fraud (Onwubiko, 2020; Smadi et al., 2018). E-tailers are the first-line target for identity fraudsters as identity is verified through account credentials, which are easily stolen through various means. The policies and the practices of general fraud management may not be effective because of the distinct nature of online business operations. General fraud policies assume relatively rich information on the identity of victims, but the identity of the customer in an online business operation is limited to a username and password. That the information is lean, makes preventing the theft of these credentials more challenging for e-tailers, resulting in huge losses. The nature of identity fraud is different to that of traditional fraud in business, and involves technology, which is ever changing.

Identity fraud is a pervasive and global problem for e-tailers. Every two seconds, an American becomes a victim of identity fraud. Identity fraud accounts caused a total loss of US$ 16 billion in 2016 (Javelin Strategy, 2018). The situation in the UK is not much different as 364,643 fraud cases were reported by the National Fraud Database (NFD) in 2019. . CIFAS (2020) reports that identity fraud constitutes 61% of total frauds and 87% of these frauds occurred via online channels (CIFAS-2020) E-tailers share more than 35% of total frauds (CIFAS, 2019), which may be a result of a lack of effective policies, as most research studies argue that such issues are treated as technological rather than managerial (Soomro et al., 2019).

Because the majority of identity fraud studies direct attention to internal fraud in banking, insurance and other public sectors (e.g. Njenga and Osiemo, 2013; Coulson-Thomas, 2017; Bierstaker et al., 2006; Siponen et al., 2014)., they offer limited possibilities in terms of how to develop and manage identity fraud management policies among e-tailers. Consider the financial services; banks make significant investments in technology and human resources. Furthermore, banking and other public sectors have more legal enforcement, significant regulatory oversight and no physical product line. Therefore, personal identification procedures and policies in these sectors are definite and online services are precedent to personal and physical identification of their customers. In contrast, e-tail sector investments have very limited supporting arrangements and there is a lack of physical identity verification and an absence of policies to collect any evidence to prove customer identity (Amasiatu and Shah, 2018). Similarly, other private sectors may have less competition, availability of sufficient funds and more opportunities for business in comparison to e-tailers, who operate in tough competition with limited resources. In such a situation, the management of identity fraud becomes more challenging for e-tailers (Soomro et al., 2019.

Because e-tailers' operating environment differs to banking, public and other private sectors, it is important to develop a nuance understanding of identity fraud in the e-tailing environment, because losses caused by identity fraud can damage business reputations and discourage new or repeat customers. Without research, e-tailers may lack guidance on how to develop and implement effective responses to identity fraud.

Therefore, this paper investigates identity fraud among e-tailers in order to develop an Identity Fraud Prevention Policies Framework (IFPF) to guide future research and policy in practice. Based on a review of the relevant literature and a qualitative study, we will analyse the organisational practices related to the management of identity fraud policies in large e-tail organisations. Our focus is to investigate identity fraud prevention policy issues in the large e-tail sector in the UK. We will explore the significance of the development, updating, communication, awareness, and compliance of policies designed to prevent identity fraud. Grounded in a review of related literature and findings from the analysis of data collected in three large e-tail organisations, we suggest an identity fraud prevention policies framework (IFPF). Thus, this research encompasses every aspect of the policy mentioned in Table 1 within the scope of this study. Without touching on all the relevant policy issues i.e., policy development, communication, training, compliance and audit, policy implications may not be

evidenced. Therefore, our research develops a new insight into identity fraud prevention policies among the e-tailers to encompass all issues which make policy implications visible.

This study contributes to the literature by offering new insights into the prevention of identity fraud among e-tailers by (1) providing a rich, contextualized understanding of online identity fraud prevention practices in e-tailing; (2) offering IFPF to inform developing identity fraud policies; (3) providing an understanding of organisational practices in relation to policy management pertinent to e-tailers seeking to prevent identity fraud; and (4) offering suggestions for managers seeking to improve guidelines, and practices that minimise e-tailing losses due to identity fraud.

1.1 Previous research on fraud management

Policy has a significant impact on the practices and activities carried out in an organisation. Hence, organisations should create and maintain effective anti-fraud policies (Njenga and Osiemo, 2013; Bierstaker et al., 2006). Policies provide guidelines to adopt appropriate behaviour towards the attainment of the overall organisational goals. In the identity fraud prevention domain, a policy refers to the guidelines for actions to prevent frauds in a pre-determined way, supporting the overall objectives of the organisation. The extant literature addresses different aspects of policies in various contexts (Soomro et al., 2019). Most of the policy research is aimed at preventing internal and accounting frauds.

The organisational practices under the fraud prevention umbrella include the creation, evaluation, communication and compliance with policy (Wilhelm, 2004). Creating and maintaining an anti-fraud policy, that addresses all stages of fraud management is necessary to guide employees and to maintain organisational performance (Njenga and Osiemo, 2013). Because fraud prevention policies are a matter of survival for businesses (Coulson-Thomas, 2017), it is important for managers to encourage employees' participation in designing such policies (Chen et al., 2015; Bierstaker et al., 2006; Siponen et al., 2014; Soomro et al., 2016). First, employees input their initial information, gained through their personal experiences. Second, their involvement in policy development can be a motivating factor to ensure their compliance (Chen et al., 2015). Notably, the extant literature has examined employee engagement in designing fraud policy, but none of these studies focus on the e-tail sector, which operates in a different environment and has a varying nature of operations.

Fraud policies should include the technical, organisational and human aspects of fraud management, as an absence of any aspect would limit their effectiveness (Ji et al., 2007; Rhee et al., 2012). In addition, organisations that share their information with other parties, including contractors, should also ensure that the same information security protocols and anti-fraud policies are applied throughout (Liu et al., 2010; Jalali et al., 2019). These suggestions are critical but are limited to information and data security, while identity fraud prevention needs a comprehensive strategy on policies.

Organisations should have a mechanism to monitor and audit policy compliance (Chen et al., 2015; Parsons et al., 2014; Singh et al., 2013; Kolkowska et al., 2017; Maitlo et al., 2019; Syed, 2019). Monitoring is a continuous process carried out by supervisors to ensure that staff members are complying effectively with anti-fraud policies. Hence, senior staff members should be aware of the related policies (Njenga and Osiemo, 2013; Wright, 2007). Although these suggestions are worth implementing, they are focused on information security in banking and other sectors, implying that policy related issues in identity fraud prevention in the e-tail sector need atttention and merit specific investigation.

Monitoring and auditing are significant to ensure policy compliance. Previous studies have suggested that providing training can create awareness of online frauds and how they are prevented (Chen et al., 2015; Singh et al., 2013; Soomro et al., 2016). Such training and awareness influences employees' perceptions and assumptions on frauds which results in compliant behaviour. Our analysis suggests that most of the studies in policy domain are either focused on information security or other business operations. Thus, no significant study has been found in a related context.

Table 1 summarises the literature findings on the organisational practices regarding identity fraud management policies, their development, updates, communication, awareness, and compliance.

Table 1. A summary of the practices suggested for fraud prevention policies

Practices	Source
- Fraud management policies should be dealt with at the highest level in organisations.	(Coulson-Thomas, 2017)

- Organisations should have comprehensive policies on information security. - Organisations should create policy awareness. - Employees should be trained on policy compliance methods.	(Soomro et al., 2016)
- Encourage employees' participation in the design and development of information security policies. - Ensure policy compliance through close monitoring. - Ensure employees' awareness of existing information security policies. - Train the staff to develop a positive attitude towards policy compliance. - Organisations should have a policy compliance mechanism.	(Chen et al., 2015) (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 the 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. - Awareness and training programs should be implemented regarding the compliance of policies. - There should be an effective mechanism for policy compliance.	(Singh et al., 2013)
- Update the policies regularly. - The policies should be evaluated to ensure they are effective.	(Bechtsoudis and Sklavos, 2012)
- Anti-fraud policies should focus on the technical, organisational and human aspects of fraud management.	(Ji et al., 2007; Rhee et al., 2012)
- Regularly update the policies to ensure their effectiveness. - Organisations should ensure the same policy for a third party is applicable for contractors regarding information systems and fraud management.	(Liu et al., 2010)
- Involve employees in policy development. - Enhance employees' knowledge of policy and compliance methods.	(Albrechtsen and Hovden, 2010)
- Anti-fraud policies should also apply to the senior management. - Anti-fraud policies should establish the organisation's commitment to combating frauds and communicating the organisational stance against frauds.	(Wright, 2007)
- Organisations should develop and maintain anti-fraud policies. - Anti-fraud policies should be stand-alone and distinct from the firm's code of conduct and ethical policy. - A written acknowledgement should ensure that all staff members have received a copy and understand it.	(Bierstaker et al., 2006)

Anti-fraud policies have a significant impact on the management of information security and fraud Table 2 presents the organisational practices on anti-fraud policies and related issues suggested in previous studies in the context of information security in banking and accounting frauds. The extant literature suggests various organisational practices for developing, updating and communicating policies, in addition to building awareness and compliance, but none of these studies focus on identity fraud prevention in an online business context. Our analysis of the literature suggests opportunities for research focused on: the development of identity fraud prevention policies; policy updates, policy awareness; policy compliance; and the compliance audits. Addressing these dimensions of policy in the current context will help to suggest a comprehensive policy framework in identity fraud prevention in the online business context (Edquist, 2019).

The above discussion signifies that identity fraud prevention has not been investigated in the context of policy because it has been treated as a technological issue by e-tailers (Soomro et al., 2019; Shah, et al., 2016). To gain a policy understanding of the issues tied to identity fraud prevention in et-ailing, an in-depth qualitative study is required to obtain field interviews to gain missing insight. It is also important to use a comprehensive approach to develop a framework for managing policies effectively. Hence, this study examines managerial practices related to the management of identity fraud policies among e-tailers. Focusing on large scale e-tailers; because they offer credit to their customers, they are the firms that are most affected.

2. Method

To understand identity fraud and e-tailing, we employ a case study research to elicit insights based on the e-tailers real-life experiences of developing a management system for identity fraud prevention policies, as well as to identify opportunities for in-depth probes of that experience, based on iterative analysis and interviews (Yin, 2014). Consistent with Gibbert et al. (2008), our case study required close interaction with the practitioners who deal with security policy development issues.

The case study approach is widely used to investigate policy management. It is a comprehensive research process, which offers customised case design, a variety of data collection methods, data analysis approaches and presentation of results in an appropriate way (Yin, 2014). We used the case study approach to produce relevant knowledge from existing practices necessary to develop a framework for the prevention of identity fraud.

Regarding generalisability, the results of a single or a few cases are unlikely to be sufficiently comprehensive. However, similar to experimental outcomes, such results have value because they may expand and generalise theories (analytical generalisation), rather than infer probabilities (statistical generalisation) (Yin, 2014). Therefore, the present research represents a first step towards a generalised framework applicable to the e-tail sector. We acknowledge that our work draws data from large e-tail organisations within the UK, i.e. in a developed economy, so future work will be needed to check its applicability to small and medium organisations in developed economies; all other forms of business firms in different economies are not the object in focus.

In order to collect the data, we completed three case studies in large, UK online retailers. Conducting the work in the UK is important because it is a developed country where a significant amount of retail sales take place via online channels. Further, as a research context, conducting this research in the UK is timely because the number of identity frauds in the UK e-tail sector is rapidly increasing (CIFAS, 2020). In addition, by collecting data within one country, we ensured that our informants worked within a consistent regulatory context, enabling us to draw rich inferences across the experiences of informants from different organizations. A final reason for conducting our work in the UK was pragmatic, as qualitative research demands significant access to the participating organisations for interviews, and two of the authors are based in the UK with contacts in the UK retails sector. We used a theory-based approach, based on literal replication, to inform our selection of the research sites (Yin, 2014). The cases were selected by similarity (literal replication) (Yin, 2014). The selection criteria were that:

a) the organisation must be engaged in online retailing, because the study is focused on online business;

b) they must be large enough to have developed security policies;

c) they must be based in the UK, to guarantee similarty in culture and management styles so that they are comparable. This also supports data collection, as any other country's data collection may incur higher costs, extra time span, immigration issues and other data access problems;

d) they must be an independent organisation, not a marketplace (such as eBay); and

e) they must be organisations that offer credit to their customers and have an in-house identity fraud management system.

Thirty-three semi-structured interviews were conducted at three case organisations. All the case organisations are large retailers operating in similar industries in the UK. The reason for selecting the same industry is to identify similar patterns throughout the industry. The questions ased directed the participants' attention to identity fraud prevention policies. The questions were concerned with issues related to the development, updating, communication, awareness, compliance and audit of the policies. Semi-structured interviews were offered as the best method for such an in-depth inquiry on how, and the reasons why the organisational practices had been adopted.

The data was collected continually over a year because it took time to gain access and schedule interviews. We used purposive sampling to identify participants, seeking to interview the staff and managers responsible for identity fraud prevention. After obtaining the details of the responsibilities of staff engaged in online business management, a list of potential respondents was finalised in coordination with the person responsible for liaison. The interviewees included, but were not limited to, information security managers, business operation managers, database security managers, fraud managers, fraud advisors, fraud analysts, fraud investigations officers, compliance managers and auditors.

The respondents were approached through a liaison person in each firm. The potential participants were recommended by our main contact at each organisation and invited via e-mail to arrange a mutually convenient time for the interviews. This process resulted in securing access to a different number of participants in each organisation, totalling thirty-three participants. We conducted the interviews until we stopped finding new or further themes (inductive thematic saturation; Saunders et al., 2018), suggesting that we had reached a point of empirical and theoretical saturation. This technique is commonly used in thematic studies and is also used by Chowdhury et al. (2020).

A research questionnaire, mostly based on our literature review, was used to structure the interviews. The questions included; who is responsible for developing identity fraud prevention policies, how often do you update policies, how do you ensure the policy compliance etc. In order to make the most of the semi-structured interviews, further in-depth questions were asked, based on the answers of the respondents.

The computer-aided qualitative data analysis system (NVivo 11) was employed to assist with the coding and categorisation of the dataset. Based on the literature review, common themes had already been identified, including policy development, updates, communication and awareness, and compliance and audit. The software helped to classify the text in accordance with each theme. First, the primary nodes were developed in accordance with the themes prescribed through the literature findings, i.e. policy development, policy update, policy compliance etc. Second, sub-nodes were developed for individual organisational practices under each node for example frequency of policy update, policy communication, and compliance methods. The transcripts of the audio files were then imported to the word file and were read and re-read by the lead author, word-by-word, with a view to avoiding missing any theme. Thereafter, each piece of information was copied into NVivo and grouped into pre-set nodes and sub-nodes of the themes.

Using the inductive approach, additional nodes and themes were also developed. Thus, all the important pieces of data were transferred to NVivo. After that, the data were imported to word files and then reduced by eliminating any similar views within the same organisation only one or two statements were taken on one theme from each firm. Based on the imported data, a thematic analysis approach was adopted for the explanations, and arguments were developed, as given in the results section.

2.1 Background of the case study sites

The selected companies were leading e-tailers in the UK, selling well known brands, mainly clothing, makeup and home accessories. The total sales volume of these firms constitutes about 40% of the total UK online sales. These firms manage identity fraud internally without third party intervention, so first-hand information on the management of identity fraud policies among them was sought. The arrangements made by these firms in relation to identity fraud prevention policies may thus significantly influence industry practices, which also made these organisations ideal for this type of research. The characteristics of the selected organisations are presented below in Table 2.

Table 2. Case firms' staff, business channels, revenue and data sources

Firm	Staff	Methods of data collection	Business channels	Annual sales for 2016/17

C1	Over 5000	Semi-structured interviews, policy documents and informal discussions	Online, telephone	Over £1.5 bn.
C2	Over 25000	Semi-structured interviews and informal discussions	Online, telephone, stores	Over £4 bn.
C3	Over 25000	Semi-structured interviews and informal discussions	Online, telephone, stores	Over £3 bn.

The selected organisations sell their own brands as well as products made by many other brands. They all confirmed that they practice comprehensive fraud prevention activities. All three case organisations have separate fraud management teams. The following sub-sections provide a brief background on each of the three selected companies.[1]

Company A

Company A is one of the largest online retailers in the UK and is based on a merger of two large rival companies. It has a large customer network throughout the UK and Ireland. More than 90% of its business operations are conducted online, yet it has a few physical stores. It is a multi-brand online retailer, so in addition to selling its own brands, it also deals with hundreds of other famous brands. Company A is a credit-lending business which offers its customers an interest-free period when purchasing a product. Customers can hold an account with the firm by providing their personal information and can then obtain login credentials to access their account. The customer information is sensitive as it includes dates of birth, addresses, bank details and credit card details. The possession of customers' personal and financial information creates a risk of identity theft and fraud for the company and it forms a challenge in terms of effective policy development.

Company B

Company B is a large online retail organisation based in the UK. It also has a chain of stores throughout the UK and Ireland and has millions of online customers. The firm deals in a wide range of items from household goods to jewellery. Company B offers credit purchases to its customers for a limited period and charges a fixed interest rate after an initial interest-free period. To access and obtain such a facility, customers must have an account and hence they

[1] No detailed information about the case organisations is given to avoid their identification.

provide personal details and credit card information. The account holders set login credentials to access their accounts.

Company C

Company C is a large online retailer in the UK with a chain of stores and a website for online business. It sells its own brand and various other brands and sells a variety of clothing and other household items. Like the two other firms, this firm is also a credit lending company that allows its customers to have an account and purchase goods on credit. The credit is granted free of interest for a certain period of time and a fixed interest rate applies after the specified period. Although credit lending is an effective scheme to attract customers, it is prone to identity fraud as it requires the collection and processing of financial and personal information.

3. Results

Our results confirmed that the themes identified in our literature review were relevant to our three case study sites. They also identified new themes that we present in this section. The data collected from each firm is given below in accordance with the themes.

3.1 The presence of identity fraud prevention policies

Our participants described the presence of information security policies and suggested that they did not necessarily translate to identity fraud prevention policy.

When asked about IT security policies, Respondent CA-R05 stated:

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

In addition, respondent CA-R10 confirmed:

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

The statements show that Company A has some policies, but they are mostly related to information security. The company has developed policy documents which include information security mobile computing, information security email, acceptable use policy,

information security encryption policy, information security network policy, information security incident management policy, information security protecting employee and customer data policy, and information security internet acceptable use policy. The aim of these policies is to help secure the customer's information from theft and breaches. The absence of identity fraud prevention policies would result in lack of effective meaures against the ID frauds, and will make it difficult to control such frauds. Therefore the CA is suggested to have a comprehensive set of identity fraud prevention policies.

However, similar policies have not been developed or implemented for fraud prevention, which may be a reason for the occurrence of identity frauds. For example, in response to a question on the presence of identity fraud prevention policies, respondent CB-R14 from Company B explained:

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

Answering the same question, respondent CB-R02 mentioned:

> *"As for the initial fraud policies, we don't have".*

Furthermore, respondent CB-R13 stated:

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

These statements show that all the case organisations have some policies but are limited to the information security aspect only rather than the security of the entire e-commerce chain. Although these policies may help in identity theft prevention, the prevention of identity fraud is a broader field, for which the results from Company B suggest the firm lacked a policy. The absence of such policies is a serious deficiency. In the absence of fraud prevention policies, staff members may work in isolation and uncertain conditions to deal with fraud related issues, leading to ineffective practice and un-organised response to identity fraud prevention. This situation will lead to continued even increasing fraud attempts. Therefore CB is advised to focus on policy development to effectively prevent identity fraud.

The results show that Company C had some policies but these were limited to the security of information. When asked about identity fraud prevention policies, the participants stated:

> *"We have a security policy, so group security policy that covers every eventuality".* (CC-R04)

> *"So there is anti-money laundering policy, there is a fraud policy, and within those, there are certain elements that relate to frauds".* (CC-R01)

Our participants suggested that Company C has policies relating to IT infrastructure security, information and communication security and money laundering. Their responses imply that Company C is focused on policies linked to information security and internal frauds. However, these policies are limited to securing customers' identity information. It shows that the company has no appropriate policy arrangements to prevent identity frauds, which causes successful fraud attempts.

We did not find evidence that our case organisations possessed comprehensive sets of policies that address each aspect of identity fraud prevention. When asked about identity fraud prevention policies, all the respondents replied negatively. The absence of such policies may lead to inconsistencies within the organisations, resulting in poor arrangements for identity fraud prevention. The presence of antifraud policies is recommended by Soomro et al. (2019) and Njenga and Osiemo (2013) for effectiveness. Therefore, our framework provides a rubric for how to craft antifraud policies that give guidance on how managers and employees should think about how respond to and efficiently prevent identity fraud.

3.2 Data Access Management Policy

In addition to the arrangements for the prevention of external threats such as encryption, anti-malware and anti-virus, Company A has a policy in place to protect critical information from internal threats. Regarding the data access policy, CA-R09 said:

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

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

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

individual hold is still conformed to the role that they hold".

Our participants shared that Company A has a data access management policy through which staff is permitted limited access to organisational and customers' data, which is a good practice to prevent internal identity fraud.

These statements show that Company A operates a policy of least privilege on data access, which is intended to minimise internal information theft. The practice of regularly updating data access should comply with the data access management policy. Although Company A has a data access policy, it is revisited six monthly, which may leave some risks.

In response to a question on data access policy, respondent CB-R13 from Company B stated:

> *"Well, access to customer data is only permitted to people who are authorised and have demonstrated need in their job to have access to that customer data … People who have access to that data should acknowledge to abide by the Data Protection Act, et cetera, et cetera".*

Our participants indicated that access to data is linked to the nature of the job. If a job requires specific information, only the relevant data access is provided to staff to enable them to fulfil their jobs. This is a valid practice to prevent internal identity fraud attempts. The statement also shows that the firm is more concerned about the regulatory implications, which is mandatory, but for effective identity fraud preventions the firm is suggested to consider identity fraud prevention while developing the access management policies.

Respondent CC-R06 from Company C stated:

> *"We are given limited access to the customers' and other data in relation to our responsibilities".*

Our participants took care to note that the policy limited their access to customer and organisational information that went beyond the context of their duties and responsibilities and limited access to only the information necessary to accomplish their tasks. Notably, they expressed an awareness that data access is annually reviewed and managed in accordance with the access management policy. The annual review of the policy may leave some gaps in its effectiveness because of transfers and promotions within the firm. Therefore, it is recommended to review the access after relocation of every concerned staff.

The data show that the case organisations have access management system to limit staff access to critical customers' information. These arrangements help control internal fraud. Such recommendations are also made by Lim (2021) and Ramprasath and Seethalakshmi, (2021) on information security. Therefore, we included data access management policies to our framework to address concerns about internal identity fraud attempts.

3.3 Policy Awareness

When asked about policy awareness and ready access, respondent CA-R09 from Company A stated:

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

The results show that Company A has made the policies available to all staff members, which helps them to carry out their duties in accordance with the policy guidelines. Although the availability of policies is important, it does not guarantee that employees will read and comprehend them. Thus, no mechanism for confirmation of policy information was found. The absence of any mechanism to ensure that the staff is well aware of identity fraud prevention policies may be a major weakness in the policy awareness programme and such gap may lead to staff acting out of the policy guidelines. Hence, training programs should be arranged to enhance the employees' awareness and understanding of the policies and there should be mechanism to continuously monitoring the policy awareness among the staff.

Respondent CB-R01 from Company B stated:

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

Although it is good practice to ensure the availability of policies, it may not guarantee that all staff members understand them. In addition, regarding the awareness of policy updates, respondent CB-R12 stated:

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

Although email is an efficient way to communicate information, policy updates require that staff should fully understand the changes, which is lacking in Company B. Although the email information is received by the staff members but it does not guarantee that they read and understand the new policy or amendments, which may lead to lack of compliance. The awareness of policies is necessary for their compliance, so there should be a mechanism to ensure that the staff understand the policy and is trained to comply with.

Similar to the other firms, Company C also has a platform for policy awareness, as mentioned by respondent CC-R06 that:

> *"We have our internal database that offers access to available policies".*

In addition to accessing the existing policies regarding awareness of a new policy or any amendments, respondent CC-R02 told us that:

> *"New policies are circulated through emails".*

The statements show that Company C offers access on its policies (general information security) through its database, which is a passive form of policy awareness. It does not guarantee that the staff is well aware of the policies and is capable of complying with. As policy awareness has been found to be very important by various researchers (such as Soomro et al., 2019 and Parsons et al., 2014) in numerous different contexts which complement our findings. Consequently, we include policy awareness as an important part of our framework and suggest assurance of policy understanding.

Therefore, it should develop awareness training programmes to ensure policy awareness. The practice of sending staff e-mails on new policies is significant, but it should also develop a mechanism that ensures the staff read and understand new policies.

3.4 Policy Updates

Updating policies more frequently is critical in e-commerce, because the broader technological environment, particularly the online ecosystem, rapidly changes. The results show that our organisations had plans to systematically update their policies. When asked about the frequency of policy updates, CA-R05 from Company A stated:

> *"Any policy is reviewed every twelve months, and it can only be an active live policy".*

Respondent CB-R01 from Company B stated:

> *"I think it's every 12 months".*

While these statements show that Company A and Company B update and review their policies on an annual basis, and can help to enhance their effectiveness, such planned reviews may be problematic. The annual review of policies may result in some serious gaps, because the context of e-tailing rests on rapidly evolving technologies and rapidly evolving threats (Pymnts.com, 2021). So the current practice of annual policy review may cause ineffective policies in place. Reflecting on the rapid technological and emerging identity fraud trends, policies become absolete more frequently than ever, therefore, policy update practice may be revisited and a continuous process should be adopted. Because annual review cycles may be too long, we probed how e-tailers responded to emergent and dynamic threats of identify fraud. In this regards, Company C has a better standing, as explained by CC-R03 that:

> *"We have a laid down system of periodically updating our policies but sometimes we do it as soon as possible to mitigate risks".*

This statement shows that despite Company C's system of periodically updating its policies, it has the flexibility to update identity fraud policies anytime changes in the environment demands change. This flexibility is important, because more frequent update of policies should result in a more effective performance against perpetrators of identity fraud. Such practice is also significant to meet the challenges of ever-changing technological threats. This strategy of continued policy updating is also suggested by Bechtsoudis and Sklavos (2012) and Liu et al. (2010) and is part of the recommended framework.

3.5 Policy Compliance

Although the practice of having identity fraud prevention policies is important, compliance with these policies is even more important; such compliance is critical to fulfil their purpose. This statement provided by CA-R09 from Company A about compliance supports this:

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

In response to a question on how the firm ensures policy compliance, respondent CA-R10 stated:

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

This shows that Company A has a practice of ensuring the compliance of every policy, investigating any violations and taking corrective action. The results also show that Company A has a devoted team to monitor policy compliance. Although Company A monitor compliance with its policies, it does not provide any training on compliance methods and processes.

Regarding policy compliance at Company B, interviewee CB-R05 stated:

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

This reveals that in Company B, staff members are expected to comply with policies and adopt the best practices. However, the results show that Company B lacks a system for monitoring policy compliance, which may lead to non-compliance behaviour of some staff members. The gap for non-compliance behaviour may increase in absence of a monitoring system, so CB is advised to ensure that its policies are followed by all staff members.

Regarding the regular internal and external audits for policies compliance, respondent CC-R06 from Company C stated:

> *"Every department that is annually audited by the head of compliance ... each department has to succeed, and has to provide evidence of their compliance, so we internally audit the compliance and we externally audit".*

The statement shows that Company C lacked a system for continuous monitoring of policy compliance. Such gap in policy compliance monitoring is a significant threat to the organisation and my cause successful fraud attempts. In the absence of policies', compliance practices it would not add to their identity fraud prevention success, so Company C should be considering the development of policies at each step of fraud prevention and ensuring better practices, with continuous monitoring of compliance via supervising staff. Additionally, Company C may also develop a mechanism for policy compliance that would help to ensure positive staff behaviour towards compliance. The practices of continuous policy compliance

monitoring are also recommended by Siponen et al. (2014) and Chen et al. (2015), thus constituting a part of the recommended framework.

3.6 Compliance Audit

Auditing has a significant role in ensuring policy compliance as it helps to locate any non-compliance and those aspects of the procedure which make compliance easier to implement. In response to a question on compliance audit, respondents reported that:

CA-R06:

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

CB-R05 stated:

> *"It's internally audited and externally audited, and any issues are dealt* (with) *accordingly".*

CC-R05 told us that:

> *"We have a sound internal audit process to ensure that our policies are properly implemented".*

Further to this, the same respondent also mentioned that:

> *"We also invite external firms to carry out the compliance audit, especially related to the policies reflecting the external polices such as FCA and other regulating authorities".*

These statements show that all the case organisations have the appropriate infrastructure to promote policy compliance-that is waiting for identity fraud management policies to be put in place. The data shows that such compliance is mostly targeted to fulfil the requirements of financial and other regulatory authorities, and is thus less focused on identity fraud prevention. This gap in lack of focus on identity fraud prevention in policy compliance audit may result in significant losses due to the successful fraud attempts. The extant literature gives significant focus to the compliance audit (such as Soomro et al. 2019 and Singh et al. 2013. This study

forwards that policy compliance audit should be extended to include identity fraud prevention, which should also be made part of the recommended framework.

Thus, we found that there were no strong identity fraud prevention policies in play, though each organisation has a supporting structure for identity fraud prevention policies. These organisations should focus on including identity fraud prevention policies in the realm of their overall policy, as was supported by most of the participants. Finally, it has been emerged that no framework exists for preventing identity fraud in the e-tail sector.

4. Discussion

This research analysed organisational practices related to identity fraud prevention policies in the e-tail sector. While identity fraud is a fast-evolving problem, policy development and implementation is slow among e-tailers. Hence, this research provides new insights and suggests improvements in identity fraud policies. By doing so, our work is consistent with Giuliani's (2018) view of policy formulation, who suggests that any policy solutions should be comprehensive, because partial policies may not solve problems. So for the new theoretical framework, IFPF, was developed to offer a comprehensive approach to identity fraud policy management, through a case study approach of e-tailers.

In the absence of such a framework, e-tailers have no clear strategies on how to manage identity frauds, which has led to the absence of effective policies. In the absence of fraud prevention policies, staff dealing with business transactions do not know how to deal with suspicious transactions. This also leads to different actions on similar transactions, depending on who is dealing with such transactions. Due to this, e-tailers are losing a significant amount of their revenue in identity fraud losses. In the context of identity fraud prevention, policies play a critical role in determining the course of action against frauds. The results suggest that all three companies have information security policies in place that are limited to data protection and mainly focus on technological problems.

To study and implement policies that effectively prevent identity fraud in e-tailing, we turn to developing a holistic framework to manage policies focused on identity fraud prevention in e-tailing organizations. Figure 1 shows the IFPF developed in this research which integrates the main organisational practices that can affect identity fraud prevention in the e-tail sector. Our research goes one step ahead of the policy recommendations by Ling and Naughton, (2016) and adds one more component for compliance and audit to make it holistic to ensure that the

policies are implemented effectively. The four important themes (organisational practices) that emerged are:

- Presence of fraud prevention policies
- Policy on data access management;
- Policy awareness and updates; and
- Policy compliance and compliance audit.

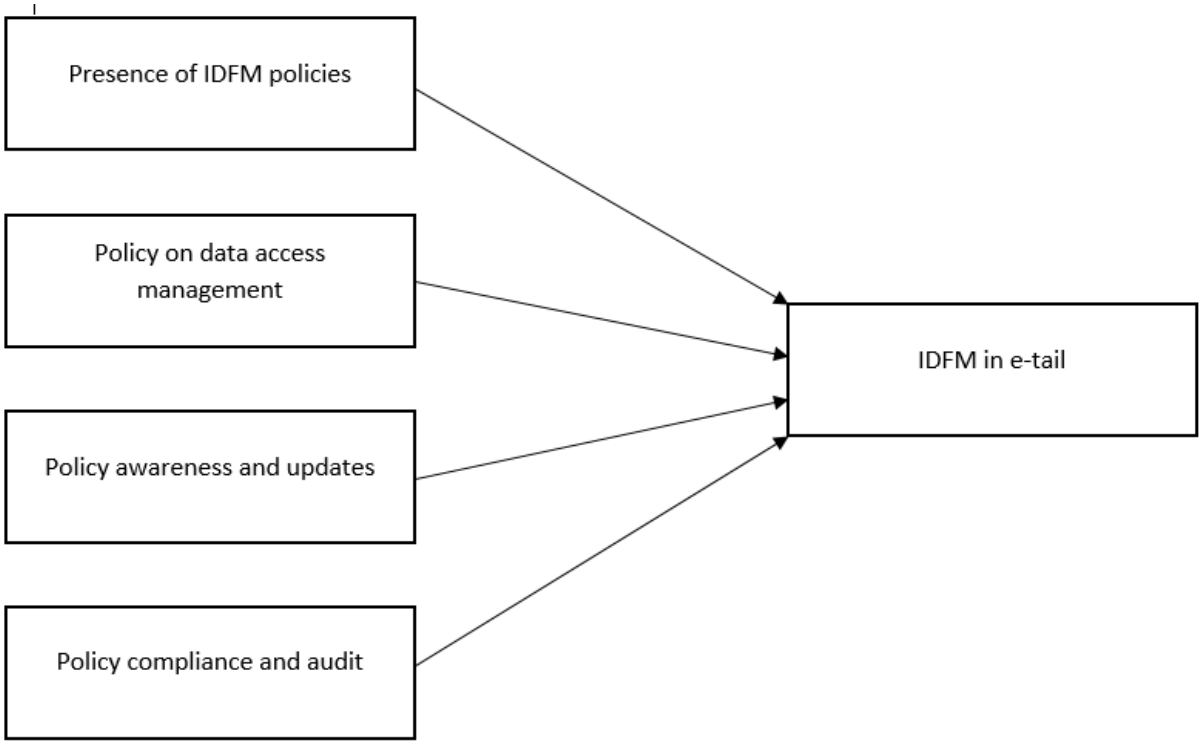

Figure 1: Identity Fraud Prevention Policies Framework (IFPF)

We found that all three e-tailers have policies in place to secure their information from theft and system hacking. These policies are mostly related to information security, communication security and infrastructure security. The findings indicate that all three companies have similar arrangements to secure their information. One of the major reasons for this consistency is that the firms are more focused on GDPR and privacy regulations compliance, so there is a lack of awareness on the difference between identity theft and identity fraud.

Although these policies are present to prevent identity theft, and could be used for identity fraud prevention, their main focus is preventing these incidents from taking place. For effective

identity fraud prevention, companies need policies at the subsequent stages of fraud prevention, including dealing with the incidents that take place, and monitoring.

Addressing this gap in understanding is important, because beyond the initial data breach, we were unable to identify prescriptive work that focused on identity fraud in e-tail firms. It appears that the literature has adopted a one-size-fits all approach, assuming that general identity fraud prescriptions are sufficient to prevent fraud across all organisations. The absence of policies causes weaknesses in the process of identity fraud prevention. It also shows that the firms studied are more focused on the prevention of information theft (to comply with GDPR requirements) Sultan, et al. (2020) which may be one of the valid reasons for a significant number of successful frauds. In the absence of a set of comprehensive policies at each stage of identity fraud prevention, there is a lack of strategic action against the fraud activities, which may allow some identity fraud incidents to take place.

In addition to the presence of appropriate policies, communicating and creating awareness of identity fraud policies will be important. While not within the domain of e-tailing, with regards to the importance of security policy, Puhamainen and Siponen (2010) and Siponen et al. (2014) argue that the visibility of an information security policy has a significant and positive impact on the policy compliance behaviour of employees. By creating visible, anti-identity fraud policies, Bierstaker et al. (2006) and Wright's (2007) work suggests e-tailers will become better at fraud prevention.

We found that our case study sites actively communicated with our participants about information security, and these communication practices could help increase awareness of identity fraud. Our studied companies have made their policies available to their staff members through an internal communication system. The readily available policy documents are helpful for staff to obtain guidance and obtain a clear set of guidelines to follow. In addition, the companies have a practice of sending policy updates via email in order to create employee awareness of the changes in existing policies, which helps employees to be updated with these changes.

As a result, to improve preventing identity fraud , we recommend studying the effectiveness of IT security, and building staff awareness of the policies as was recommended by Parsons et al. (2014) and determining whether they translate to the e-tailing context. The practice of creating policy awareness was highlighted in previous studies (Siponen et al., 2014; Soomro et al.,

2016). A summary of the organisational practices of each studied company in terms of identity fraud prevention and policy-making is provided in Table 3.

Table 3. A summary of the organisational practices of identity fraud prevention in the studied companies

Processes	Organisational Practices	CA	CB	CC
The presence of fraud prevention policies	- The presence of information and technology security policies.	Yes	Yes	Yes
	- The presence of identity fraud prevention related policies at each stage.	No	No	No
	- All policies are reviewed annually.	Yes	Yes	Yes
Data access management policies	- Staff should at least have access to personal information.	Yes	Yes	Yes
	- Only job-related information can be accessed.	Yes	Yes	Yes
	- Assessment of data access privilege.	Six monthly	Annual	Annual
Policy awareness	- E-learning packages are developed to help the staff learn about the contents of policies and understand them.	Yes	Yes	No
	- All policies are available in the internal communication system.	Yes	Yes	Yes
	- New and updated policies are communicated effectively.	Yes	Yes	Yes
	- Policy awareness and understanding is acknowledged.	No	No	No
Policy updates	- Policies are updated frequently	Annual	Annual	Annual
Policy compliance	- A mechanism for policy compliance.	Yes	No	No
	- Internally audit the policy compliance.	Yes	Yes	Yes
	- Invite external experts for compliance audit.	Yes	Yes	Yes
Compliance audit	- A practice of internal and external audit to ensure compliance with its policies	Yes	Yes	No

Notes: CA: Company A, CB: Company B, CC: Company C.

The findings in Table 3 show that Company A and Company B use an online learning system that helps the staff to gain access to any policy contents. This practice is essential to inform employees of the existing policies and interpret them in order to ensure compliance. Company C lacks such a learning system, which may result in policies not being readily available and

may lead to non-compliance. It is important to direct employees' responses in accordance with organisational objectives. In a theoretical perspective, it emphasises that policy communication should be active, and feedback oriented to ensure that concerned staff understand related policies and are capable of complying.

We found that a lack of employees' understanding of policies is one of the major obstacles to policy compliance. Therefore, e-tailers are recommended to arrange a feedback mechanism to ensure that employees read and understand the related policies. Additionally, these companies should develop a training program to create policy awareness, understanding and learning of the compliance process, and develop a positive attitude from staff which would result in improved compliance (Parsons et al., 2014; Singh et al., 2013; Soomro et al., 2016). To add to the theory, policy communication should be a two-way mechanism to ensure the appropriate understanding of the core of policies and commitment to compliance.

To ensure stewardship of customer data and privacy, e-tailers need to have stronger preventive measures for identity fraud. The studied companies hold sensitive information relating to a vast number of customers, which make these firms responsible for general data protection regulations (GDPR), and privacy regulations compliant. In addition to external challenges, these companies face internal threats, so to minimise these risks, companies allow their employees minimum access to sensitive information about their customers. Employees are only given access to information, which is essential to accomplish their duties, which helps to minimise the chances of internal data theft. It was also established that in Company B and Company C, data access privileges are assessed on an annual basis, which is not sufficiently frequent and may leave compromised data access privileges undetected for some time. Thus, Company B and Company C are recommended to assess privileges more frequently, which is a practice adopted in Company A. Additionally, e-tailers are also advised to review data access privileges when any change in the roles of staff members takes place (Alrashed, 2016; Wang et al., 2006).

The significance of related policies to effective management and development of policies on identity fraud has also been highlighted by Singh et al. (2013) and Soomro et al. (2016). Previous studies conducted by Jamieson et al. (2007), Kumar et al. (2007), Liu et al. (2010), Njenga and Osiemo (2013) and Wilhelm (2004) have emphasised the importance of the existence of related policies for the effective prevention of frauds. Therefore, e-tailers are

recommended to develop policies for effective identity fraud prevention. In addition, the significance of policy compliance is as important as the existence of the policy itself.

All three studied companies have a practice of internal and external audit for policy compliance, which helps top management ensure that the policies are complied with effectively to assist in achieving the organisational goals. However, to ensure policy compliance in real-time, Company A needs to develop a mechanism through which immediate supervisors ensure that the policies are being complied with, without waiting for an audit. Such practice would help to closely monitor the compliance process and correct any errors made by staff members about understanding policy and compliance procedures, enabling the enhancement of staff compliance performance through training and awareness.

It is recommended to extend the practices of closely monitoring the compliance processes and the presence of compliance mechanisms in an e-tail context that were highlighted by Chen et al. (2015) and Parsons et al. (2014) for IT security policy compliance.

Company C should develop a comprehensive set of identity fraud prevention policies at each stage of fraud prevention to provide proper guidelines to employees to ensure uniform and planned actions. The need for comprehensive fraud prevention policies is also emphasised by Bierstaker et al. (2006), and Njenga and Osiemo (2013). Identity fraud prevention policies should be dealt with at top management level, and input from operational staff should be sought to produce effective policies (Coulson-Thomas, 2017; Albrechtsen and Hovden, 2010).

Providing training helps employees to understand compliance methods and processes which leads to positive compliance behaviour (Soomro et al., 2016). Therefore, Company A should develop a training program to enhance policy compliance. The close monitoring of policy compliance was recommended in Chen et al.'s (2015) study. The company is also recommended to introduce compliance training, which would help employees to understand the policies and learn how to comply efficiently (Soomro et al., 2016). In addition, it is suggested that Company B and Company C implement a compliance monitoring system and train their staff members to comply with anti-fraud policies.

Our results show that while our e-tailers shared many similarities in their approaches to managing fraud, they also had substantial differences in their strategies across the firms, finding that these firms employ different strategies towards the revision of access management. Company A revise it twice a year while Companies B and C undertake this exercise annually.

We also found major differences among the case firms in the variation in policy compliance procedures. Results show that Company A has a continuous policy compliance procedure in place, while the others rely on a compliance audit which they conduct periodically. Furthermore, our results show that companies A and B get their policy compliance audited by internal and external parties for all of their policies, while Company C invites external auditors only to ensure compliance with the financial regulatory authority policies. Thus, our study finds some important differences in managerial practices in the prevention of identity frauds. In spite of these above-mentioned differences, our research found many similarities among the case organisations on prevention of identity frauds. These similarities may be because we theoretically sampled firms engaged in a shared industry (e-tailing), with similar organisational structures, similar size and similar operating environments.

4.1 Theoretical contributions

This study contributes to the identity fraud and e-tailing literature in several ways. First, the study develops a new theoretical framework (IFPF), integrating the organisational practices required for effective identity fraud prevention policies among e-tailers. This study is unique in its nature, as no previous research has investigated the management of identity fraud prevention policies.

E-tailing is a fast-growing market and a subject of financial conduct authority, so it is necessary to prevent identity fraud to avoid business and reputational damage. Hence, the novel contribution of this study is providing new insights into the identity fraud prevention policies through the IFPF proposed in this study. The research contributes to the existing knowledge by helping to bridge the gap in the literature, as it investigates the management of identity fraud prevention policies in the real world setting in large e-tail firms, as very limited prior research has focused on the e-tail sector. This study also offers insights into the significance of policy management in identity fraud prevention which, opens new avenues for future research. We have identified several gaps or opportunities for advancing our understanding of identity fraud in the context of e-tailing, and suggest research needs to go beyond identity theft in order to fully understand the implications of identity fraud for organizations.

This research also contributes to the current debate on identity fraud, given the dynamic nature of technological development and its effect on the e-tail sector. The findings of this study

advance the progress of managing online identity fraud and provide a foundation for future studies in this domain.

4.2 Practical implications

In addition to the theoretical contributions, this study also has practical implications for e-tailers seeking to solve issues related to identity fraud prevention policy management. As already mentioned in our work's motivation, identity fraud has significantly increased during the COVID-19 pandemic, so this study will help managers seeking to navigate the challenges associated with increased online shopping. First, this study helps e-tailers to understand what constitutes a comprehensive identity fraud prevention policy. Second, the analysis of identity fraud prevention policy management provides guidance to e-tailers on how to develop, implement and update policies on identity fraud prevention. This is an important contribution, since while identity fraud is a fast-evolving problem, policy development and implementation are slow among e-tailers. By providing a framework for evaluating the technology, processes and performance of relevant staff, our work helps e-tailers to identify any weaknesses in their identity fraud prevention, which could lead to the development of more effective policies.

Anti-fraud policies have a critical impact on the prevention of identity fraud. In addition, they help to direct employees' actions toward ideal actions. Hence, maintaining a detailed set of policies for identity fraud prevention is recommended. Detailed policies should also be established for the deployment of anti-fraud technologies. An accessible prevention policy should be designed to control internal fraud. It is suggested that identity fraud prevention policies be communicated effectively to facilitate and create awareness amongst all the employees so they can be successfully implemented. Furthermore, as ID theft is a fast evolving problem, identity fraud prevention policies should regularly be evaluated in response to emerging challenges in order for timely updates to take place. Table 4 provides detailed recommendations on organisational practices and policy-making in relation to identity fraud prevention among the three studied e-tailers.

Table 4. Suggestions for improvements of identity fraud prevention policies

Limitations of existing practices	Related to	Suggestions	Valid for
Policies are limited to information security.	CA, CB and CC	The case firms should develop policies specific to identity fraud prevention.	CA, CB and CC

Data access privilege is evaluated annually.	CB and CC	Data access privilege should be assessed more frequently.	CB and CC
Policy compliance is ensured only through an audit.	CB and CC	Develop a mechanism for policy compliance.	CB and CC
Policies are made available only on the firm's database	CC	Develop a learning package to make staff aware of policies.	CC
Policies are annually reviewed.	CA, CB and CC	Fraud related policies should be updated continuously to counter emerging challenges.	CA, CB and CC

Notes: CA: Company A, CB: Company B, CC: Company C.

Table 4 shows that e-tailers do not have a set of comprehensive policies on identity fraud prevention to direct employees' behaviour; additionally, the mechanisms for policy awareness and compliance have some critical limitations. Hence, suggestions to overcome these limitations are provided in Table 5. The findings also reveal that the three companies being studied review their policies on an annual basis. However, this may not be sufficient to overcome identity fraud challenges, particularly because cybercriminals actively create new tactics with great frequency, and e-tailers should adopt the practice of constantly updating their identity fraud prevention policies in order to ensure improved countermeasures against emerging fraud trends and methods (Soomro et al., 2019).

The suggested guidance of our framework would also help the e-tailers identify the mechanisms necessary to counter the increase in identity fraud attempts due to the pandemic related increase in online shopping trends. By directing attention, for example, to the frequency of policy updates, our recommended framework will help pandemic affected e-tailers know which mechanisms will help them fight identity fraud. E-tailers should also consider developing a policy learning system to help their employees to obtain access to policies for effective compliance. Although the concept of literal replication applies to this research, these results may be generalised to e-tailers of a similar nature, especially to credit lending firms.

4.3 Limitations and future research

Like all research, this study has some limitations that could be addressed in future research. First, data was collected from three e-tailers located in the UK; For wider focus, future studies may include a larger number of organisations to include wider population. Secondly, only large

firms were included, while small and medium firms may have different operational and management procedures, therefore future studies could collect data from small and medium size companies. Thirdly, our research was focused on the UK, which is a developed economy, so more studies are suggested focusing on developing countries and other developed economies to understand wider economic and cultural implications. Fourth, this study relied on the collection of qualitative data to develop the IFPF; qualitative data has some limitations, to overcome these limitations, future studies could collect quantitative data from a large number of respondents in order to generalise the findings. Finally, the lack of research on identity fraud prevention among e-tailers indicates a need for further studies in this and other areas, as this is an emerging and promising area on which future research could focus.

5. Conclusions

Identity fraud is a big challnge especially for online retailers, which causes them losing a significant amount of their revenues. To help e-tailers effectively preventing identity fraud, a qualitative data appraoch was adopted and the data was collected from three large online retailers, operating in the UK. Based on the results, this study has developed a new theoritical framework, IFPF, based on a comprehensive analysis of the organisational practices related to the management of identity fraud policies in large e-tail organisations.

Through the literature review, it was observed that identity fraud prevention in policy context is under researched. Although there have been significant number of studies in online fraud and information security prevention, but most of them are in technological context. Our findings suggest that identity fraud is one of the major challenges for e-tailers and these firms are losing a significant amount of their revenue due to fraud. Our study found that generally online issues are treated as technological challenges, so firms do not have a comprehensive set of policies regarding identity frauds and there are some weaknesses in creating policy awareness, updates and compliance, which may be a fundamental cause of such fraud losses. Hence, the study provides guidelines for improved management of identity fraud policies through IFPF.

In addition, the results showed that there are some important organisational practices that should be taken into consideration by e-tailers, namely: the availability of fraud prevention policies; a data access management policy; policy awareness and policy updates; and policy compliance and audit. New insights are offered into the theory of fraud prevention, and

guidelines are provided to e-tailers towards better prevention of identity frauds. This study investigates large e-tailers who are offering credit lending and operating in a developed economy which may limit generalisability, so it is suggested that future studies are undertaken with medium and small firms in varying economies. Additionally, for wider generalisability, future studies are suggested to be founded on quantitative data.

References

Albrechtsen, E. and Hovden, J. (2010) 'Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study', *Computers & Security,* 29(4), pp. 432-445.

Alrashed, F. (2016) 'Stealing More than Just Identity', *International Journal of Scientific & Engineering Research,* **7**(2), pp. 422-426.

Amasiatu, C. V., & Shah, M. H. (2018). First party fraud management: framework for the retail industry. International Journal of Retail & Distribution Management.

Bechtsoudis, A. and Sklavos, N. (2012) 'Aiming at higher network security through extensive penetration tests', *IEEE Latin America Transactions,* 10(3), pp. 1752-1756.

Bierstaker, J.L., Brody, R.G. and Pacini, C. (2006) 'Accountants' perceptions regarding fraud detection and prevention methods', *Managerial Auditing Journal,* 21(5), pp. 520-535.

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies*, 23(sup1), S47-S59.

Chen, Y., Ramamurthy, K. and Wen, K. (2015) 'Impacts of Comprehensive Information Security Programs on Information Security Culture', *The Journal of Computer Information Systems*, 55(3), pp. 11.

Chowdhury, N. H., Adam, M. T., & Teubner, T. (2020). Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures. Computers & Security, 97, 101931.

CIFAS. (2020) *Fraudscape 2020*. Retrieved from https://www.cifas.org.uk/insight/reports-trends/fraudscape-2020 [Accessed on 22-06-2020}.

CIFAS (2019) *Fraudscape 2019.* Available at: https://www.cifas.org.uk/secure/contentPORT/uploads/documents/Cifas%20Fraudscape%202019%20Full%20Digital%20Report%20.pdf (Accessed on 12-08-2019).

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

Edquist, C. (2019) Towards a holistic innovation policy: Can the Swedish National Innovation Council (NIC) be a role model? *Research Policy*, 48(4) pp 869-879.

Gibbert, M., Ruigrok, W. and Wicki, B. (2008) 'What passes as a rigorous case study?', *Strategic Management Journal*, 29(13), pp. 1465-1474.

Giuliani, E. (2018) Regulating global capitalism amid rampant corporate wrongdoing—Reply to "Three frames for innovation policy", *Research Policy*, 47(9) pp 1577-1582.

Jalali, M.S., Siegel, M. and Madnick, S. (2019) 'Decision-making and biases in cybersecurity capability development: evidence from a simulation game experiment', *The Journal of Strategic Information Systems*. 28 (1), pp. 66-82.

Jamieson, R., Winchester, D. and Smith, S. (2007) *Development of a conceptual framework for managing identity fraud.* 40th Annual Hawaii International Conference on System Sciences, (HICSS), Waikoloa, HI,. 3-6 January.

Javelin Strategy (2018) *Identity fraud hits record high, 154 million U.S. victims 2016, Up 16 percent according new Javelin Strategy and research study*. Available at: https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new (Accessed: 12 Jan, 2018).

Ji, S., Wang, J., Min, Q. and Smith-Chao, S. (2007) *Systems Plan for Combating Identity Theft - A Theoretical Framework.* International Conference on Wireless Communications, Networking and Mobile Computing, (WiCom), New York. 21-25 September.

Kim, R.Y.. (2020) The Impact of COVID-19 on Consumers: Preparing for Digital Sales, *IEEE Engineering Management Review*, 48(3), pp. 212-218. Doi: 10.1109/EMR.2020.2990115.

Kolkowska, E., Karlsson, F. and Hedström, K. (2017) Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. *The Journal of Strategic Information Systems*, 26(1), pp.39-57.

Kumar, V. and Kumar, D. and De Grosbois, D. (2007) *Collaboration in Combating Identity Fraud.* Annual Conference of the Administrative Sciences Association of Canada, Production and Operations Management Division, Ottawa, Canada.

Lim, H. I. (2021) An Approach to Improving Software Security Through Access Control for Data in Programs. In Advances in Computer Science and Ubiquitous Computing (pp. 413-419). Springer, Singapore.

Ling, C. and Naughton, B. (2016) An institutionalized policy-making mechanism: China's return to techno-industrial policy, *Research Policy*, 45(10), pp 2138-2152.

Liu, J., Xiao, Y., Chen, H., Ozdemir, S., Dodle, S. and Singh, V. (2010) 'A survey of payment card industry data security standard', *IEEE Communications Surveys & Tutorials,* 12(3), pp. 287-303.

Maitlo, A., Ameen, N., Peikari, H.R. and Shah, M. (2019) Preventing identity theft: Identifying major barriers to knowledge-sharing in online retail organisations. *Information Technology & People*. 32(5)1184-1214. https://doi.org/10.1108/ITP-05-2018-0255.

Njenga, N. and Osiemo (2013) 'Effect of fraud risk management on organization performance: A case of deposit-taking microfinance institutions in Kenya', *International Journal of Social Sciences and Entrepreneurship,* 1(7), pp. 490-507.

Onwubiko, C. (2020). Fraud matrix: A morphological and analysis-based classification and taxonomy of fraud. Computers & Security, 96, 101900.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014) 'Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)', *Computers & Security,* 42(May), pp. 165-176.

Puhakainen, P. and Siponen, M. (2010) 'Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study.', *MIS quarterly*, 34(4), pp. 757-778.

Pymnts.com (2021) Fraud Prevention. Available at: https://www.pymnts.com/fraud-prevention/2021/ecommerce-fraud-detection (accessed on 03/04/2021)

Ramprasath, J., & Seethalakshmi, V. (2021). Secure access of resources in software-defined networks using dynamic access control list. International Journal of Communication Systems, 34(1), e4607.

Rhee, H., Ryu, Y.U. and Kim, C. (2012) 'Unrealistic optimism on information security management', *Computers & Security,* 31(2), pp. 221-232.

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., ... & Jinks, C. (2018). Saturation in qualitative research: exploring its conceptualization and operationalization. Quality & quantity, 52(4), 1893-1907.

Shah, M. H., Ahmed, J., & Soomro, Z. A. (2016). Investigating the Identity Theft Prevention Strategies in M-Commerce. *International Association for Development of the Information Society*.

Singh, A.N., Picot, A., Kranz, J., Gupta, M.P. and Ojha, A. (2013) 'Information Security Management (ISM) Practices: Lessons from Select Cases from India and Germany', *Global Journal of Flexible Systems Management,* 14(4), pp. 225-239.

Siponen, M., Mahmood, M.A. and and Pahnila, S. (2014) 'Employees' adherence to information security policies: An exploratory field study', *Information & Management,* 51(2), pp. 217-224.

Smadi, S., Aslam, N., & Zhang, L. (2018). Detection of online phishing email using dynamic evolving neural network based on reinforcement learning. Decision Support Systems, 107, 88-102.

Soomro, Z.A., Ahmed, J., Shah, M.H. and Khoumbati, K. (2019), "Investigating identity fraud management practices in e-tail sector: a systematic review", *Journal of Enterprise Information Management,* 32 (2), pp. 301-324. https://doi.org/10.1108/JEIM-06-2018-0110

Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016) 'Information security management needs a more holistic approach: A literature review', *International Journal of Information Management,* 36(2), pp. 215-225.

Sultan AlGhamdi, Khin Than Win, Elena Vlahu-Gjorgievska, (2020) Information security governance challenges and critical success factors: Systematic review, Computers & Security, 99(December), pp 1-39, 102030, https://doi.org/10.1016/j.cose.2020.102030

Syed, R. (2019) Enterprise reputation threats on social media: A case of data breach framing. *The Journal of Strategic Information Systems*, 28(3), pp. 257-274. https://doi.org/10.1016/j.jsis.2018.12.001.

Wang, W., Yuan, Y. and Archer, N. (2006) 'A contextual framework for combating identity theft', *IEEE Security and Privacy*, 4(2), pp. 30-38.

Wilhelm, W.K. (2004) 'The fraud management lifecycle theory: a holistic approach to fraud management', *Journal of Economic Crime Management*, 2(2), pp. 1-38.

Wright, R. (2007) 'Developing effective tools to manage the risk of damage caused by economically motivated crime fraud', *Journal of Financial Crime*, 14(1), pp. 17-27.

Yin, R.K. (2014) *Case study research: design and methods.* 5th edn. London, Sagen Publications Ltd.