www.revistageintec.net
ISSN: 2237-0722
revista GEINTEC Gestão, Inovação e Tecnologias

Overcoming Trusting Barriers in Inter-organizational Identity Theft Prevention in Knowledge Sharing: A Case of UK Retailing Industry

Dr. Rozina Chohan[1]; Engr. Murk Chohan[2*]; Irfan Mir Chohan[3]; Farhana Mir Chohan[4]
[1]Shah Abdul Latif University, Khairpur Mir's, Sindh, Pakistan.
[2*] The Begum Nusrat Bhutto Women University, Sukkur, Sindh, Pakistan.
[2*]Murk.chohan@bnbwu.edu.pk
[3]Jiangsu University, China.
[4]Shah Abdul Latif University, Khairpur Mir's, Sindh, Pakistan.

Abstract
Inter-organizational knowledge sharing basically connects two or more firms with one another in exchange relationship for skills, expertise and knowledgeable personnel. Knowledge plays a key role in organizational performance but it is given a very little attention in terms of information security and requires addressing security concerns due to following reasons: First, because retailing is the most victimized channel due to online trade. Second, if organizational criminal wings can compromise the information system of one firm, they can attack other firms too. Hence, identity theft is a collective problem. A security breach is among the top three business stories and identity theft is the key reason why it occurs in online retailing. Identity theft is a serious issue of society at a large and its prevention requires knowledge sharing by several actors. Through different case studies, interviews and theoretical and empirical analysis, this study highlights some unknown side of prevention collaboration in the retail industry in the United Kingdom (UK) which is of theoretical and practical importance. This paper theoretically furthers our understanding of how communication of organizations with comparable goals is handled differently in information security management. Practically, it evaluates relationships of retailing firms, online fraud forums and law enforcement departments in the fraud prevention process. Our research outlines how retailers' partnerships with different stakeholders will help them solve and reduce identity theft by presenting a structure for inter-organizational fraud prevention in retailing organizations.

Key-words: Digital Identities, Personal Identity, Authentic Identity.

1. Introduction

The need to protect a person's identity is due to its link with the individuality and consciousness of self. Personal identity and the ability of an external party to prove it, is the key to

various commercial transactions, especially in this technological age. Rannenberg, Royer and Deuker (2009, p. 1) emphasized that "*the personal appearance at the counter, is now as virtual as a user account at a web portal, an email address or a mobile phone number*". Supplementary digital identities are being created to help business in daily activities. Consumers do not need to visit shops to buy products and services, and businesses do not need to spend on high street stores. Businesses are now exploring the idea of personal identity and utilize personal information to bring shopping to the doorsteps of customers (Rabolt and Miler, 2009).

The growing need for social distancing will also increase the demand for shopping to the doorsteps of customers. This, however, will also increase the challenge for firms to prove authentic identity, because there is a deliberate and illegal use of names or numbers to commit identity fraud (Newman and McNally, 2005, p. 1).

Identity fraud is a serious problem for society. It has posed a challenge to firms since various internal measures outlines have been ineffective. Shaw (2016) argued that the frontline security officers in the UK police department need to be equipped with the skills to tackle identity theft. On the other hand, Flores, Antonsesn and Ekstedt (2014, p. 92) suggested that reliance on security services may be enough when dealing with identify theft challenges. The authors highlighted that "*there might be a lack of specific expert knowledge among the personnel providing security services, and as a consequence provided security services are neither relevant to a firm's current context nor implemented effectively*". While there is an immense need for social distancing, there is also a need for knowledge sharing among different actors to combat identity theft.

This qualitative paper based from online shopping organisations in the United Kingdom discusses how various actors can share knowledge of identity theft prevention while maintaining social distancing. In this paper, we have evaluated the influence of knowledge flow on the retailing industry by exploring retailers' three major knowledge networks: dyad, virtual and forum based. Dyad is a one-to-one relationship of organizations with comparable goals. Mitchel et al., (2014, p. 2198) argued that "*Clusters of related firms may increase potential for the sharing of tacit knowledge between firms*". Similarly, the importance of the virtual relationships cannot be denied, because retailers can access technical knowledge on the web and can maintain social distancing (see e.g., Tamjidyamcholo, et al, 2014). We believe that forum based relationship is also necessary. It can act like a hub for knowledge gatekeeping. Knowledge gatekeepers acquire information from various sources and communicate them to the relevant audience (Mitchel et al., 2014). Through this important relationship, we have examined how inter-organizational identity theft prevention knowledge can help retailers to address and mitigate identity theft.

The empirical study is designed for UK firms because they were in better position to provide useful insights. UK retailing is Europe's biggest online economy and is the most prone in identity theft related crimes. Nearly 82 percent of identity crimes were committed in the UK via online mechanism (Cifas, 2015). Approximatly, six million identity frauds happened only in England and Wales (Office for the National Statistics, 2016). This paper espouses some unknown side of prevention collaboration in the UK retailing industry, which is of theoretical and practical importance. Theoretically, this paper enhances our understanding for how communication of organizations with comparable goals is handled differently in information security management. Practically, this study has evaluated the relationship of retailing firms with online fraud forums and law enforcement agencies. The barrier to their communication and solutions are discussed. Previously, identity theft prevention strategies failed to consider the impact of inter-organizational knowledge sharing on security services. The novel contribution of this study is that considers the relationship of retailing firms, online fraud forums and law enforcement agencies.

The rest of this paper is designed as follows. Firstly, the literature evaluates what is knowledge and how it is helpful in identity theft prevention practice. It also attempts to establish the relationship between inter-organizational communication practice and its relationship with the online fraud prevention process. Thus, it highlights the research gap and study questions. The case study is designed which covers these aspects. Finally, results and discussion highlights communicational gaps of various stakeholders in the fraud prevention process, and whether retailers were able to reduce fraud with the help of inter-organizational knowledge sharing. The study concludes by identifying research implications and future research suggestions.

2. Literature Review

Identity theft is one of the most common crimes in this millennium and leads to devastating consequences for the victim. This type of crime involves compromising personal information such as individuals names, date of birth, social security details and other personal information. This type of crime has posed a challenge to firms since various internal measures outlines have been ineffective. Shaw (2016) argued that the frontline security officers in the police department need to be equipped with the skills to tackle identity theft. However, Flores, Antonsen and Ekstedt (2014, p. 92) suggested that reliance on security services may be enough when dealing with identify theft challenges. The authors highlighted that "*there might be a lack of specific expert knowledge among the personnel providing security services, and as a consequence provided security services are neither relevant to a*

firm's current context nor implemented effectively". This suggests the need for knowledge sharing among different actors to combat this crime.

Like these authors, Wang, Yuan and Archer (2006) showed that identity theft prevention requires communication and collaboration from identity owners (registered members of the public), identity issuers (government and private organizations that issue identity certificates), identity checkers (the custom or traffic police officers) and identity protectors (the government and legislation authorities or law enforcement agencies). This collaboration starts when a victim of identity theft reports violation of identity information to identity issuing authority such as a retailer or a banker. The retailer then performs its assessment and then forwards the case to the law enforcement agency for legal actions. Thus, information flows from one stakeholder to another in identity theft prevention.

In this context, information, however, is merely an awareness that something has happened, whereas knowledge implies the application of information to produce tangible results (Sanchez, 2005). Nonaka (1994) suggests that information is a flow of messages; until we anchor that very flow into actions then it becomes knowledge. Tsoukas (2011, p. 454) maintains that a mind needs to exercise and participate in a larger collective so that it does not only focus on the values but also in the abstraction, general principals and ability to produce tangible results. Knowledge is an essential source of competitive advantage and is particularly important in online businesses due to the evolving nature of technology. Knowledge is "*a fluid mix of framed experience, values, contextual information and expert insight that provides a framework for evaluating and incorporating new experiences and information*" (Davenport and Prusak, 1998, p. 5).

In organizations, knowledge does not only exist in the mind of professional persons, but also in organizational documents, repositories, and practices. Knowledge, which resides in organizational documents and repositories, is explicit. On the other hand, the knowledge, which holds an organizational practice, is tacit. Explicit knowledge is theoretical (Polanyi, 1962), whereas tacit is practical (Polanyi, 1966; Nonaka, 1994). Explicit knowledge can be coded easily and communicated widely and quickly because of its coded nature. Tacit knowledge, on the other hand, requires knowledge holders to explain what they do and how (Tsoukas, 2011, p. 455).

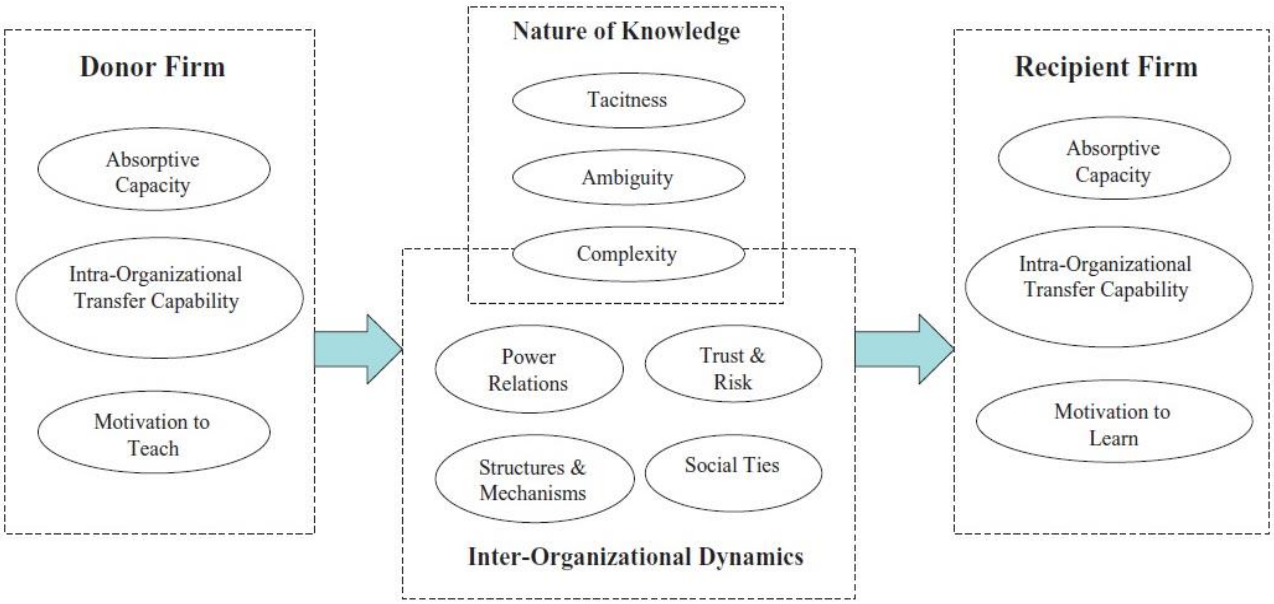
There are two major knowledge sharing processes to enhance firms know how. Firstly, intra-organizational knowledge sharing occurs when firms learn from their own employees. This type of knowledge helps organizations in acquiring internal knowledge. Secondly, firms use inter-organizational knowledge sharing relationships to explore external knowledge. Learning from an external partner has a competitive advantage because most knowledge is created outside the firm's boundary. However, this does not mean that intra-organizational knowledge sharing is less important.

Firms provide complete know-how to their employees through intra-organizational knowledge sharing practice (Jasimuddin, Connell and Klein, 2014).

This study focuses on inter-organizational knowledge sharing process because identity theft is not a problem of a single organization. The knowledge gain from a peer can be helpful to reduce security 'wheel-reinvention' (Lopez and Esteves, 2013), and mixing ideas from various actors can generate 'better solutions' (Feledi, Fenz and Lechner, 2013). Organizational innovation and performance is increased with extensive knowledge sharing among organizations various actors (Easteby-Smith, Lyles and Tsang, 2008; Mason and Leek, 2008). However, comparable goals, private scopes, necessitate a trade-off between sharing and protecting firm knowledge assets; otherwise, companies, which find themselves in learning race, behave differently (Easterby-Smith, Lyles, and Tsang, 2008). They either lock their knowledge or provide knowledge of low quality to the recipients which are wastage (Gaur *et al.*, 2011; Barney and Hesterly, 2015). Inter-organizational knowledge sharing practice, therefore, involves balancing both private and common scopes so that firms can exchange knowledge with one another fluidly.

Easterby-Smith, Lyles and Tsang's (2008) outlined factors influencing inter-organizational knowledge transfer as seen in Figure 1 to evaluate how retailers balance comparable goals. Their framework is selected based on a comparative analysis of three studies that are likely to fit the retailing organizations (Chohan, 2016).

Figure 1 - Factors Influencing Inter-organizational Knowledge Transfer



Source: Easterby-Smith, Lyles and Tsang (2008)

In Figure 1, firms' absorptive capacity, intra-organizational transfer capability and motivation to teach are identified as necessary capabilities of both donor and recipient firms to acquire external knowledge. Both firms require interactive dynamics such as power relations, trust and risk, structures and mechanisms and social ties for efficient and effective collaboration. Figure 1 also shows tacitness, ambiguity, and complexity to be relevant in the inter-organizational knowledge transfer process.

This paper focuses on interactive dynamics between organizations since these factors either facilitate or hinder knowledge sharing relationships between organizations. However, this does not mean that firms' characters and the nature of knowledge are less important. Understanding of nature of knowledge enhances knowledge comprehension (Panahi, Watson and Partridge, 2013; Nonaka and Takeuchi, 1995), while firms' characters improve knowledge utilization (Junni and Sarala, 2013; Lichtenthaler, 2009; Roberts et al., 2012).

Interactive Dynamics between Organizations

In Figure 1, the structure of the knowledge sharing process is basically a relationship between organizations such as joint ownership, partnership, and network of practice (Nonaka et al., 2014). These involve professional relationships and social ties among members of the organizations. Mechanisms are the channels through which actual knowledge is transferred from a source to a destination (van Riel and Fombrun, 2007, p. 2). It includes conferences, inter-firm reviews, onsite and online meetings (Becerra, Lunnan and Huemer, 2008). Table 1 outlines kinds of research on several inter-organizational knowledge sharing structures and mechanisms in information security management.

Table 1 - Information Security Related Knowledge Sharing Practice

Structures	Open source	Partnership	Forum Based	Virtual Community
Mechanisms	Web protégé	Complementary information system	Information Security Forum (ISF), Cifas, Gartner Inc.	LinkedIn groups - Information Security, Anti-Fraud experts
Authors	(Mace, Parkin and van Moorsel, 2010; Stahl, Parkin and van Moorsel, 2011; Feledi, Fenz and Lechner, 2013; Feledi and Fenz, 2012)	(Liu, Ji and Mookerjee, 2011; Flores, Antonsen and Ekstedt, 2014)	https://www.securityforum.org http://www.gartner.com/technology/home.jsphttps://www.cifas.org.uk	(Tamjidyamcholo et al., 2013; Tamjidyamcholo et al., 2014) See also: https://www.linkedin.com/groups/924757 https://www.linkedin.com/groups/83088

Received: 19.07.2021 – Accepted: 18.08.2021

Table 1 addresses four kinds of structures and mechanisms used by the security professionals to interact with one another. Firstly, an open-source web protégé relationship comprises users from various organizations such as government, military and commercial. Web Protégé is an ontology development software to create, upload and share ontology for collaborative editing and viewing (Stanford Centre for Biomedical Informatics, 2016). A group at the Newcastle University evaluated the impact of this open relationship on the Chief Information Security Officers (CISOs) of various companies (Mace, Parkin and van Moorsel, 2010; Stahl, Parkin and van Moorsel, 2011; Feledi, Fenz and Lechner, 2013; Feledi and Fenz, 2012). Their findings show the following: Firstly, there was little to no contribution from CISOs, and incentives were needed to encourage knowledge holders. Secondly, it offered CISOs no guiding knowledge on how to use it. Professionals, who were not adequately computer literate, found it difficult. Thirdly, the web protégé design was based on pre-defined themes such as vulnerabilities, threats, and ISO 27001. This fixed nature of software made it hard to record innovative ideas.

The second relationship (Table 1) highlights the partnership by various firms. The partnership used a signed agreement between the companies to secure a complimentary information system. Basically, two companies shared responsibility because of a shared information system. Liu, Ji and Mookerjee (2011) and Flores, Antonsen and Ekstedt (2014) evaluated this one-to-one relationship in the firms which offered security services. In Liu, Ji and Mookerjee's (2011) study, a decision made by two firms to share knowledge on information security was calculated by an investment so that contribution from each firm can be maximized. However, a complementary information system provided natural incentives because of shared responsibility. The stand-alone information system found knowledge lock-in from both firms. Similarly, Flores, Antonsen and Ekstedt (2014) investigated factors that account for behavioral information security governance in partnership. The authors explored how officials react to the establishment of information security-related knowledge sharing activities among American and Swedish organizations. Results show that competent organizations had the ability to tackle identity breaches leading to firms' lack of incentive to share their knowledge with a subordinate firm.

In Figure 1 dependency is the key to knowledge acquisition by a recipient. Power, in this context, is a force that influences outcomes (Hardy, 1994, p. 220). However, as noted above, knowledge of intense firms lack the motivation to learn from a subordinate peer. Perhaps, because it fears that a subordinate partner might not be in a position to provide them quality knowledge. Studies also noted that a fast learner subordinate might dominate the relationship by acquiring knowledge of high quality (Khanna, Gulati, and Nohria, 1998). Once the power shifts from a donor to the recipient,

the pace for collaboration was deteriorated (Easterby-Smith, Lyles and Tsang, 2008). This was highlighted in an empirical study conducted in India (Kale and Anand, 2006). Authors noticed when a foreign partner realized that there is a little more that it can acquire from local partners, their basis of collaboration was eliminated.

Similar issues were found in membership relationships. The third relationship mentioned in Table 1 highlights firms' subscriptions to information security forums such as Gartner, Cifas, and ISF. Forums are established to document the knowledge of information security officials to help detect and prevent identity theft. Participants are liable for subscription fees. Forums' relationship covered the wider industry with the audience from various countries. How the forum's relationship helps firms to address and mitigate identity theft is yet to be empirically established. Like forums, the fourth relationship shown in Table 1 is based on membership. However, rather than professional networks, firms subscribed to virtual communities on the web. Virtual communities were basically groups on LinkedIn and Facebook. Unlike forums, virtual groups, however, were subscription-free (Hsu et al., 2007). Information Security Virtual Community and Anti-Fraud Experts are common examples of LinkedIn. Firms subscribed to these groups to gain more technical knowledge, and members communicated without constraints of time and location (Hsu et al., 2007). However, researchers from various fields found a lack of active participation in the knowledge network without showing reasons what affected knowledge workers' collaboration (Tamjidyamcholo et al., 2014).

Trust, in Figure 1, is an important element in the inter-organizational knowledge sharing process. The researchers in information security management (Flores, Antonsen and Ekstedt, 2014) also realized its importance. The authors noted that the knowledge-sharing activities of security professionals should be different from other professions. Security professionals handle complex and sensitive data such as financial records and confidential information. They also employ running programming codes and clicking hyperlinks in their daily activities (Tamjidyamcholo et al., 2014). Clicking malicious hyperlinks from peers or running malicious codes could compromise computer systems of information security professionals. Consequently, the receiver of the knowledge would become a victim of the knowledge sharing process. This unique risk in learning from a partner has highlighted by Tamjidyamcholo et al., (2014, p. 21). During their data collection phase they reported, "*while we were distributing the questionnaire of this study, we received several emails informing us that they did not want to click on the survey link because of worries about a malicious link*".

Trust may create a sense of security among the collaborators that knowledge in question will be used for its original purpose as mentioned in the knowledge sharing process (Easterby-Smith, Lyles and Tsang, 2008). That the recipient will not exploit knowledge gains from the peer in personal

gain (Becerra, Lunnan and Huemer, 2008). And that the basis of collaboration will remain continued no matter what happens to the relationship status (Gaur et al., 2011; Barney and Hesterly, 2015). Trust, is, therefore, a perception that partners will behave as expected (Gaur et al., 2011; Simpson, 2013a). It is measurable by evaluating partners' ability to carry on obligations (Jiang et al., 2015). Such obligations are either formally documented by contractual governance (Gaur et al., 2011) or by observing the partner's integrity, consistency, and reliability on agreed-upon actions (Becerra, Lunnan and Huemer, 2008).

Trust, however, is not a free-hanging element, nor does it refer to the nature of a single phenomenon (Simpson, 2013b; 2013a). Researchers worldwide assess its various forms in inter-organizational knowledge-sharing practice. For instance, Jiang et al., (2015) evaluated two forms of trust in the success of the inter-organizational knowledge sharing process, namely goodwill and competence. Authors found that competence trust was associated with intangible resources sharing [e.g., tacit] while the goodwill trust was concerned with tangible resources sharing [e.g., explicit]. Goodwill trust was emotional and was grounded in relational settings between collaborators to support one another (Roy, Sivakumar, and Wilkindon, 2004), while the competence trust was rational that predicts if the partner possesses sufficient resources to be exchanged (Malhotra and Lumineau, 2011). A higher level of goodwill trust overcomes negative thinking about partners' unexpected behavior (Noorderhaven, 2004), while the competence trust was able to reduce fears from partner's lack of invaluable knowledge resources (Sengun and Wasti, 2007).

Concluding studies, it was observed that security professionals lack to contribute their knowledge in the four major knowledge networks such as open-source, dyad, forum-based and virtual groups on the web. The discussed framework brings our attention to various elements that either facilitate or hinder the inter-organizational knowledge sharing process. The review however clearly shows a lack of evaluation of these factors in the retailing firms for an in-depth analysis. Such an analysis might help to examine how inter-organizational identity theft prevention knowledge sharing practice can help retailers to address and mitigate identity theft, and what makes retailers reluctant during collaboration. Both questions are important because the examination of the former question may help firms in realizing what works for them in the fraud prevention process. Similarly, evaluation of factors, which make retailers reluctant during collaboration, may help them in assessing solutions for more optimal lines of communication with one another. Therefore, this study as designed below is an attempt to explore these two questions in the retailing industry in light of interactive dynamics discussed above.

3. Methodology

UK Retailing - The Field of Study

Online retailing is the fastest growing business in entire Europe. UK retailing however is considered as Europe's leading online shopping economy (Khan, 2015). UK retailing is the world's third-largest e-commerce industry (Statista, 2018). It is also fourth-most victimized channel after the United States, Australia, and Canada in identity theft and related crimes (Trustwave, 2013, p. 9). UK retailers consider information security as a priority because of highest victimization rate. Nearly 82 percent of identity crimes were committed in the UK via online mechanism (Cifas, 2015), and six million identity frauds happened only in England and Wales (Office for the National Statistics, 2016). The design of this study, therefore, focused on firms that reside in the UK since they are in a better position to provide useful insights.

Qualitative inquiry (e.g., case study, ethnography) can be contextualized in various ways, such as social settings, professional settings of the organizations, or in this case, a retailing industry in the fraud prevention process (Silverman, 2005). A single case is likely to generate in-depth investigation (Mason and Leek, 2008, p. 779) and is appropriate design in the relational setting of the organizations (Becerra, Lunnan and Huemer, 2008). A single case can help theory building and is able to contribute a field that lacks empirical investigation (Peltokorpi, Nonaka and Kodama, 2007). Therefore, it is considered in the UK retailing organizations because they were appropriate knowledge networks in the fraud prevention process.

This paper includes data from three firms (ShoppingCo, PaymentCo and NetworkingCo) because of their relational view with one another. Names of the companies and participants were anonymized to ensure confidentiality and pseudonyms (e.g., Jon, Jackson, Sophie and Ben) were assigned to participants to hide their original identities. Description of the companies given in the next section and their relational setting are outlined in Figure 2.

Study Sample

The sample of this study was purposive because it considered the suitability of the research site (Miles, Huberman and Saldana, 2014; Newman, 2005). However, convincing participants was the biggest challenge, due to the complexity of the topic, operational engagement of the participants, and managerial concerns. The following comment from a participant of this study shows how critical the data of the fraud prevention process was and how difficult was it to convince participants in this line

of inquiry "*Apology I was a bit wag, because, I had not been actually given background or any detail. As you can appreciate the sensitivity we do as a department. But that's fine. Do what you need to do*" [ShoppingCo.Debra]. Concerning these challenges, we used Saunders, Thornhill and Lewis's (2015, p. 378) advise approaching the managers (persons in-charge). One page description of the project, which dictated how topic was related to participants' current role and responsibility, was attached with invitation letter. This is because managers are more likely to agree if the study topic is interesting (Easterby-Smith, Thorpe, and Jackson, 2012).

In ShoppingCo, we approached the head of security operations and recorded 18 audiotapes from April 2014 to May 2015. Jon's team in collaboration with police department performed covert security operations to track identity thieves. Jon snowballed us to his three field-based security managers Bram, Sam and Greg. They were responsible for producing legal shreds of evidence to present to the court. Jon's team had three computer-based analysts, Lyn, Ronny and Adie who supported field-based officers in online evidence. Thus, in Jon's team, seven members were interviewed. Jon snowballed us to fraud department where interviews were conducted with Debra and Mandy, the fraud prevention managers. They provided their three fraud prevention advisers, Drew, Fran and Bella for further exploration. Insights from Carl, the head of physical security department were also collected. Freddy, in ShoppingCo was manager for training information security staff. His insights were also useful. Celia was a member from the compliance department who audited third parties how they keep ShoppingCo's information systems. And Pat was from IT department to check how internal members used an internal information system. Therefore, they were also interviewed. Field visit with ShoppingCo was concluded with two practical briefings. In the first briefing, the use of cutting-edge technology was discussed how it prevented identity theft. A group, which performed covert security operations, concluded field visit in ShoppingCo by showing an onsite example of covert security operations. Mostly, managers and related senior officials were able to communicate with peers in other firms. Informants in these positions provided rich information for nearly 2 hours of audiotape recordings. Some security officials (e.g., Lyn, Pat and Celia) shown lack of collaboration with peers in other firms, therefore, they hardly interviewed about an hour, as they were unable to comment on inter-organizational knowledge-sharing practice.

Access to PaymentCo and NetworkingCo was gained through LinkedIn social networking site. In PaymentCo, we conducted three interviews from February 2015 to April 2015; each ranged 2 hours of audiotape recording. PaymentCo also provided two internal documents that show how external knowledge explored at conferences was turned into useful form to benefit the company. Jackson was the first interviewee in PaymentCo at senior management position in fraud and risk

department. We then interviewed compliance manager, Pon, and ended data collection in PaymentCo due to accessibility reasons and explored final insights from Fredrick, the director of card services.

NetworkingCo provided two informants and two internal reviews, which were internally communicated with member firms. Sophie was a deputy head for financial crimes, and Ben was a financial crime intelligence manager. We interviewed only two officials in this company on same day in May 2015, each with 2 hours of audiotape recording. The nature of the company was sufficiently discussed and informants provided useful insights on how inter-organizational identity theft prevention knowledge relationship provided timely and useful information to the firms, and what difficulties were faced by the informants during collaboration.

Interview Protocol

Table 2 is a sample of interview protocol. We based on semi-structured interview design because of its benefit on structured and unstructured design. Unstructured interview talk has no limits, while the structured interview cannot help in getting new insights because of fixed nature of themes (Saunders, Thornhill and Lewis, 2015). A combination of two allowed us in exploring data within interactive dynamics of the organizations and the research questions mentioned above. We also keep ourselves open to new emerging relationships addressed by the informants such as police and retailers' relationship in the fraud prevention process (see Figure 2).

Table 2 outlines questions, sources, and rationale behind an inquiry. We considered interview design to cover one-to-one interaction with participants because of its benefit over a group interview. A group interview was able to save time, however, it was unable to facilitate exploration of participants' perceptions, understandings and experiences (Ryan, Coughlan and Cronin, 2009, p. 309). The participants might not be able to talk freely in front of their colleagues. Additionally, we might not be able to get number of participants under one roof since retailing was the busy industry.

We initiated interviews with simple questions to provide interviewees comfortable environment. These questions focused on their roles and responsibilities. However, this is not included in the sample questions (Table 2). We used various synonymous and tried to apply business-oriented terminologies to help respondents' understanding. For instance, rather than knowledge, we used best practice, skill and expertise.

Interview protocol design considered inter-organizational dynamic components mentioned in Figure 1. The first set of questions as can see from Table 2 concentrates inter-organizational knowledge sharing relationships. Thereby we evaluated nature of knowledge networks used by

informants to exchange knowledge with one another. This set of questions assisted us in exploring kind of structures and mechanisms used. This set of questions also supported exploration of trust and risk implicitly when we asked participants how often they use the network and why. Then trust and risk of the companies were explored as highlights second set of questions. We inquired from participants whether they use sensitive information during collaboration, or they need permission from their line managers before exchange any detail with their partners. A final set of questions addresses power and powerlessness of the informants with conclusion of addressed barriers and solutions.

Table 2 - Sample of Interview Instruments

Questions	**Rationale**	**Source**
Have you been provided membership with any professional community such as ISF or IT-ISAC security forums? How useful do you think these forums are to enhance your fraud prevention skills? Are you registered on any other virtual community to extract current trends on identity theft such as information system security association, LinkedIn security group, and society of information risk analysts? How often do you share your knowledge through email, SharePoint, blogs, video conferencing and why? Do you share any white paper, industry specific magazine, or newsletter with each other? Do you use interpersonal interaction, social gathering, organized meetings, presentations, reports to exchange knowledge and why?	To explore nature of networks in exchange relationship	(Liu, Ji and Mookerjee, 2011; Tamjidyamcholo *et al.*, 2014)
Would you consider any information that you share with other organization to be sensitive? Do you need permission from your line manager before you share anything with other organizations? Do you trust the knowledge shared by your peer is useful?	To assess level of trust and associated risks in the knowledge network	(Majchrzak and Jarvenpaa, 2004; Easterby-Smith, Lyles and Tsang, 2008; Becerra, Lunnan and Huemer, 2008)
How do you feel about your overall experience of knowledge sharing process? Would you like to have more open lines of communication with people in other organizations? What factors might prevent this from happening? Is there anything that you can do to overcome those barriers?	To assess their own view of situation and their feelings of power (powerlessness) about the knowledge sharing process	Authors

Data Analysis

A total of 23 interviews and 13 internal documents were collected from ShoppingCo, PaymentCo, and NetworkingCo. We used Nvivo-10 software package to support analysis process. Nvivo-10 provided audiotape transcription facility and automated code generation. We added data to Nvivo-10 project and themes were created by following outlined interactive dynamics discussed in Table 2 in assigning codes. However, codes cannot be used as if they are end results (Yin, 2009). A minimum condition of a case study based research depends on verbatim records (Yin, 2009) such as considering how text speaks (Smythe et al., 2008, p. 1389). This in-depth analysis allowed us in identifying new emerging themes including police-retailers' relationship (see Figure 2). Therefore, new codes were also assigned to repetitive patterns of emerging themes. Transcript summaries, reflective diaries and self-memos were used to help interpretation (Saunders, Thornhill and Lewis, 2015). For more refined results, we also sent an analysis of the data to firms to confirm whether their insights were evaluated accurately. A final reporting of results followed research questions how inter-organizational identity theft prevention knowledge relationship can help retailers to address and mitigate identity theft, and what makes retailers reluctant during collaboration. We have also added the emerging elements such as police-retailers' collaboration in combating identity theft.

4. Case and its Findings

Background of the Case

Retailing industry in the United Kingdom has undergone significant changes over past decade from a conventional method of trading to online sale. Most retailers were reluctant to use Internet technologies and have been using the traditional style of "bricks and mortar" outlets (Marciniak and Bruce, 2004, p. 368). However, this conventional method still exists; online retailing is growing rapidly as an easier means of supporting business activities (MarketLine, 2015). Statista (2018) has shown a dramatic increase in online shoppers. It identifies eighty percent of Internet users who shopped online. Consumers welcome online shopping because of reduction in prices due to reduced cost of high-street stores. Additionally, they were able to shop anywhere, anytime without being constraints of timing and location.

Due to consumers' vast preference of online shopping, most conventional retailers in the UK are using online mechanisms to supplement their traditional ways of trading, and ShoppingCo is one among them. ShoppingCo, mentioned in Figure 2, is a knowledge-intensive firm due to nature of its

work. Its multi-brand retail outlets engaged 4000 to 5000 staff members. It offered customers incentives through its scheme of buy now and pay latter. This credit sale affected it extensively making it vulnerable to identity thieves. Similarly, PaymentCo, group incorporation, sold online payment systems to companies like ShoppingCo and both share risk together. However, inclusion of NetworkingCo in this study was based on the nature of its work. It was not a retailer as such, because it did not sell products. Rather, it facilitated retailers with fraud prevention knowledge to overcome identity theft. It is also working in collaboration with various retailers and law enforcement agencies. Hence, NetworkingCo was able to see dynamics of various retailing organizations and law enforcement departments in the fraud prevention process.

Figure 2 - Inter-organizational Fraud Prevention Process in the Retailing Organizations

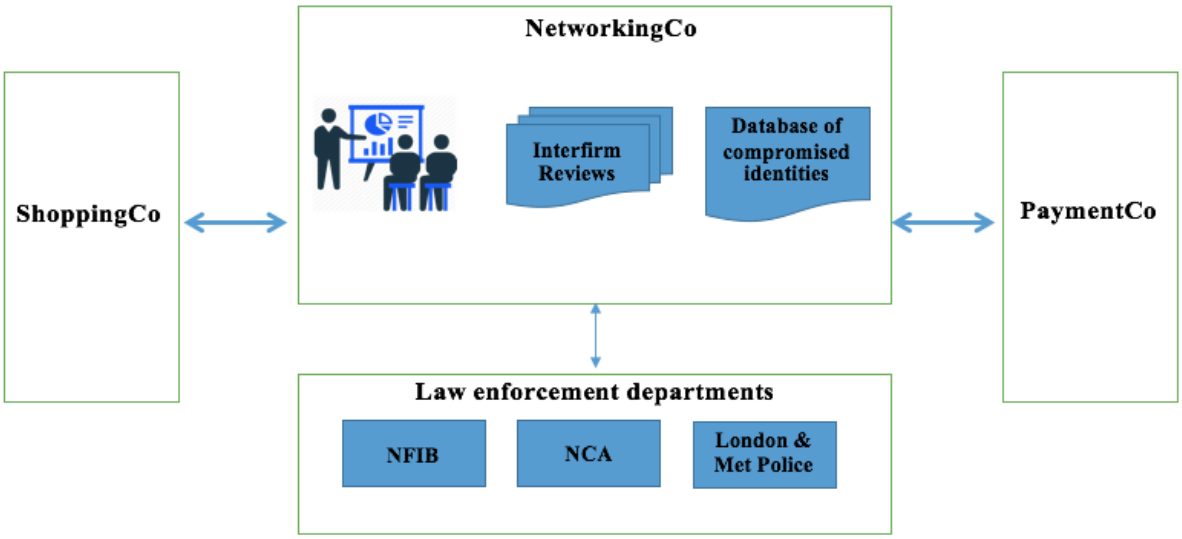


Figure 2 summarizes relationships explored from UK retail companies. ShoppingCo and PaymentCo connect with each other through NetworkingCo for fraud prevention knowledge. They also had a direct relationship with one another. ShoppingCo, a core retailer, which sold products and services directly to the end customers, bought selling system from PaymentCo. However, PaymentCo was an intermediate retailer which connects retailers and the banks to fulfill online transaction. Jackson [PaymentCo] highlights this relationship and shared risk from identity theft as follows "*We set up payment pages for the merchants. When a shopper goes to the website and says okay I like that pair of shoe and checks-out. That checkout then takes them to the payment page. They would then know the card details. PaymentCo process the information and sends it to the shopper's Card Company or bank. The card company would come back to PaymentCo to confirm, and [if we] say yes*

we know them, they are then authorized. If it is not [authorized], we will then send this information back to the shoe retailer. Now say for example this shoe retailer was having financial problems. They could not fulfil the orders. [Or] They could not ship the goods, and then the person who placed the order will contact the card company and request the chargeback. Now if there is not enough money on retailers' accounts, then PaymentCo could essentially bare that loss. So, say for example there are hundred transactions for the one hundred pounds - there is potential loss."

During analysis, we have discovered various other emerging relationships of retailing organizations such as retailers' relationship with law enforcement agencies (e.g., National Fraud Intelligence Bureau (NFIB), National Crime Agency (NCA), London and Metropolitan Police. Therefore, their relationships were also considered in the findings. First we will discuss how inter-organizational identity theft prevention knowledge relationships can help retailers to address and mitigate identity theft and then will examine what factors hinder their collaboration. In the last we will highlight an unknown side of prevention collaboration, the police and retailers' relationship in combating identity theft. Gap in their collaboration, and enhancement of their lines communication will be discussed.

How Inter-organizational Identity Theft Prevention Knowledge Relationships Help Retailers to Address and Mitigate Identity Theft?

Despite strong relationship with one another, retailers failed to communicate directly for fraud prevention knowledge. They used NetworkingCo as an intermediate channel to exchange knowledge as can see in Figure 2. We have evaluated three inter-organizational knowledge-sharing practices of the retailing industry via NetworkingCo. Firstly, a comprehensive database of compromised identities shared centrally by the member firms to spread know-who. They were able to flag fraudulent person by checking prior compromised cases. They were also able to store their own fraudulent orders. This practice secured retailers products worth million pounds, and Bella [ShoppingCo] reveals usefulness of this interaction with member organizations as "*We have dealing with other members of NetworkingCo, the members of the bank security [for instance] calls us, querying about the information that we have loaded onto NetworkingCo's [database regarding] why we have filed that person and then they will deal with their customer*". This database of compromised identities provides retailers an opportunity to interact with one another and exchange information on fraudulent cases. Based on information from supplied from partner, other retailers were able to make decision whether to pass an order or not. Thus, they were able to address and mitigate an identity theft.

Secondly, NetworkingCo circulates quarterly inter-firm reviews to spread knowledge about why a fraud was committed. This mechanism allowed other firms to apply proactive measures when they identify similar kind of flag in their orders. What happened was a member of staff e.g., Ben [NetworkingCo] collects information from several law enforcement departments (e.g., NFIB, NCA, and London and Metropolitan police force). From those details are then used to produce an inter-organizational review. Reviews are then shared with all member organizations, so that they can proactively prevent identity theft. Ben [NetworkingCo] highlights this process and its importance as follows "*I have got an operational lead for NetworkingCo's engagement with Law Enforcement departments. And the purpose of that is to try and obtain intelligence, basically on how fraudsters do what they do and why. So, that we can turn it into something useful form that members can use to prevent frauds*". NetworkingCo's reviews (e.g., NetworkingCo.Doc1, 2014; NetworkingCo.Doc2, 2015) were examples of their quarterly inter-organizational reports.

Like NetworkingCo, PaymentCo also reported use of inter-organizational reviews. However, this time they create their own knowledge to share with internal members rather than using mixed up knowledge created over forums. Jackson [PaymentCo] produced "Retrieval Request Report" (e.g., PaymentCo.Doc1, 2014) which was an example of his documented experience of what he learned at "Merchant Risk Council". It was a conference basically organized by a forum like NetworkingCo where he participated as an attendee and documented his experience so that other members of his organization who were not able to go there could use it.

Thirdly, NetworkingCo hosts several events a year where retailers can exchange experiential knowledge with one another face-to-face. It organizes several conferences and inter-organizational meetings, quarterly and annually. Debra [ShoppingCo] showing her keen interest in NetworkingCo conferences emphasized that "*There were lots of common themes that have been discussed. How other organizations are tackling elements of what they are seeing. It was like an opportunity to see what other areas and issues they are facing and what can be done differently*". Similar kind of opinion was extracted from another participant who recommended inclusion of these events on regular basis as "*I do personally recommend these meetings quite often. I think they do add value. It puts things in perspectives. So, the issues that we are facing, obviously other organizations are facing similar things. And anything technical they are doing that we can learn from them, it does help*." [ShoppingCo.Mandy]. Both Debra and Mandy support implicitly Lopez and Esteves's (2013) reduction to security 'wheel re-invention' by highlighting importance of practices their peers are applying. The respondents emphasized their keen interest on peers' different ways of dealing identity theft. In consistent with Mitchel et al., (2014, p. 2198), these statements support the view that

organizations with comparable goals were able to provide them useful technical knowledge for an efficient fraud prevention process.

NetworkingCo divides conferences and meetings into two major groups such as business sector working parties and fraud-intelligence. Former was sector-specific, while the latter was cross sector. Former is an opportunity for firms who are offering same kinds of goods and services to discuss same set of frauds. However, in the latter approach, it gives chance to the member organizations to interact with a wider audience. We asked participants what kind of benefits they have found in cross sector interaction since it was based on wider audience. Greg [ShoppingCo] commented, "*The conferences or the meetings that I go to, sometime it has nothing to do with retail frauds. So, if I'm listening to somebody from the mortgage company talking about how somebody was defrauding the mortgage system by living in a second house instead of rented out to somebody to get a more favorable mortgage. That is never going to impact on our retail business... However, when I hear the CompetitorCo have had somebody's credit cards been hit by certain credit card numbers, that's really important*". This statement discusses two distinct elements. First, it confirms Cohen and Levinthal's (1990) prior knowledge relatedness increases recipients' learning intent. Second, however, does this not emphasize that cross-sector meetings were useless?

Sector specific conferences increased value of the knowledge in information security professionals because of similar experiences. Why retailers used cross-sector meeting at NetworkingCo was because they can access wider audience. Figure 2 shows that NetworkingCo invites public sector organizations and members from law enforcement agencies. They can access them on these meetings. Retailers' relationship with law enforcements, especially with police department is considered which highlights why they need to access them on conferences. We will come back to this relationship.

What Makes Retailers Reluctant during Collaboration?

We have mentioned barrier to inter-organizational knowledge sharing process in three major relationships that retailers used frequently. First, a NetworkingCo relationship, as mentioned above, was an effective communication for inter-organizational knowledge sharing process. However, despite its usage, NetworkingCo also faced many challenges from member firms and reciprocity was the major issue. We will discuss this in detail. Then, we will highlight what hinders dyad relationship in exchange of inter-organizational knowledge that may help them to prevent identity theft. We will

conclude barriers to inter-organizational knowledge sharing process by highlighting retailers' lack of trust on virtual groups on the web.

Knowledge Power as Barrier

Even though fraud was common issue, retailers found reluctant to open their doors of collaboration to other firms due to lack of general trust. Trust was not a major issue in the NetworkingCo relationship, however, reciprocity was. Quality of knowledge was regulated by contractual governance and grading system. Lack of reciprocity was explicitly evident by a participant who stated that "*I appreciate what you really concern is, if we have information intelligence, we should pass that intelligence to other businesses. However, people guard their data and hide their data protection. All our data goes into NetworkingCo's [database]… A lot of other businesses also use NetworkingCo. However, very little comes out from other sides*" [ShoppingCo.Jon]. This statement implicitly weakens donor's motivation due to unequal contribution from the partners. This statement is an inquiry from researchers that why should I share my knowledge with the firm that is hiding its practice from my company.

Reciprocity concern was also found in other participants implicitly who feared that a subordinate partner might not be in position to provide them quality knowledge. Sam [Shopping.Co] stated by laughing at a subordinate firm "*In the security world if there are many groups like ShoppingCo, more security department like ShoppingCo, it will be very easy to start having a proper collaboration. There is another company similar to ours. They have only one man who covers the whole country [Laughs]*" [ShoppingCo.Sam]. This statement supports Easterby-Smith, Lyles and Tsang's (2008) argument that a firm, which perceives itself in highest rank, will behave differently. ShoppingCo perceived itself a competent organization. Consequently, it offered negative reactions to the knowledge sharing activities. While PaymentCo offered, a positive response to knowledge sharing activities because it did not considered itself in learning race in the fraud prevention process as "*You all are essentially working towards a same goal. You are trying to stop fraudsters out there, and fraudulent merchants. Any exchange of detail is helpful, because the reality is that, if fraudsters could hit PaymentCo, they can hit ShoppingCo too. I think there is no point of hiding information when it comes to fraud*." [PaymentCo. Jackson]

NetworkingCo was a reputable organization in the UK, especially in fraud prevention knowledge. They regulate trust through contractual governance. When a new retailer wants to be their member, it must follow undersigned obligations. Competence trust was regulated by a mechanism

which evaluates knowledge supplied by the member firms. For instance, on a question, how they deal issues of reciprocity from member organizations, Sophie [NetworkingCo] by giving example of a grading mechanism highlighted that "*It is used to be a process where they [the retailers] would be graded between sort of accomplished down service improvement. Or if we found that a member putting NetworkingCo and other organizations at risk by not having sufficient evidence to record the case to the database, then they will be considered as unsatisfactory of some description, and they would be immediately measured to put in place, to make sure they will then be brought up to an acceptable standard*". This statement shows that they evaluate their members on evidences they supply. Thus, they were able to handle reciprocity issues.

Sensitive and Confidential Data as Barrier

This paper extracted widespread responses from participants about what makes them reluctant during collaboration via a dyad relationship. Use of sensitive and confidential data was one reason why retailers are not keen to share information. The study result also show that potential vulnerability from partner's action hindered donor's motivation in information sharing. Group which used sensitive and confidential information in the firm highlighted that "*The big stumbling block is that of data protection and protection of customers' details*" [ShoppingCo.Sam]. Similar concern was found at PaymentCo implicitly when a respondent highlighted hiding use of personal information of the retailers they deal with on regular basis during collaborations as follows "*When you are talking about fraud you could not give away information about the merchants, but you could talk about trends and you could talk about issues.*" [PaymentCo.Jackson]

Another participant who highlighted reputational risk argued, "*There is nothing going to be personal about it. But what we would not do is to make ourselves foolish either. There is reputational damage to take into consideration. You cannot go into open meetings with all your woes on the table. It will only be shared at official level and will only be shared with an association that is deemed safe*" [ShoppingCo.Freddy]. Individual members failed to comment on this question because they either had little or no active participation to interact with peers in other firms. Respondents highlighted lack of time "*I do not have time to follow up. Our business is usually quite intense. We have a lot of work to do in a short period... Our day is totally taken with business as usual*" [ShoppingCo.Pat], and availability of in-house training sessions "*You get training sessions in here all the time. If a new tool comes in, you get trained on it. So, you don't need to do anything else*" [ShoppingCo.Bella].

Virtual Identity on the Web as Barrier

Retailers have shown a complete lack of trust on virtual groups on web such as LinkedIn and Facebook. During literature review, it was observed that knowledge collaborators had lack of active participation from information security staff on information security group and anti-fraud expert group (Tamjidyamcholo et al., 2013; Tamjidyamcholo et al., 2014). To uncover what makes them reluctant on these groups we asked participants about their opinion of its use. Freddy [ShoppingCo] highlighted that "*I have never known anyone been declined from their membership. There are certain fraudsters and organized criminal wings sitting on these forums to listen to the best practice and procedures to get around it*". Through this statement, we can assume that people in information security, by their attitude, norms and investigative work, becomes detective. This nature consequently, makes them hard to trust people on the virtual groups. Since, fraudsters can impersonate other people to hide their identities; they might attack these groups by subscription.

However, regardless of the preference of the network, few participants shown trust on Twitter site for technical knowledge as highlights this statement "*I think twitter is quite useful tool for this type of industry. I do follow quite a few people in there, and they are purely risk based and fraud based people. I would be looking at that on daily basis to find what happens in the industry. In fact, I had an experience that somebody I follow on twitter was talking about certain experiences and the subject was interesting, then I certainly click on the link*." [PaymentCo.Jackson]"

Police and Retailers' Relationship in Combating Identity Theft

Participants revealed explicitly by stating that dyad was not suitable knowledge sharing relationship to establish inter-organizational knowledge sharing process. They highlighted this by demanding use of police unit as their intermediate communicator "*The way forward is not Retail Company talking to Retail Company. The way forward is retail company is telling the police; the police are sharing it with other businesses. It should not be retail to retail*" [ShoppingCo.Greg].

Levering relationships from police was key theme emerged from our data. Majority of participants reported use of police unit. Preference of police force by the retailers to exchange knowledge with one another was twofold: First it had pattern to measure quality of identity cases. Police have identified what they have required to get involved in covert security operations in collaboration with retailers. Secondly, they can create a good reputation by showing them good evidences. Retailers may get more priority access from them in dealing their cases when they show

them their knowledge power. This was highlighted as follows "*Now the beauty of the Metropolitan Police is that they are the biggest force in the country. They have forty-three boroughs. They are splitting to forty-three sections. They have done a report which is telling everyone in Metropolitan Police on how to investigate Business Crimes. And they mention our company in it. So, we are quite well within Metropolitan police. It refers ShoppingCo's to other companies. So that's how far we are into them. The city of London Police is responsible for fraud investigation in the whole UK except Scotland. Now similarly they have done the document, which they have circulated outside the metropolitan police to the other police forces. And when Bram [field-based security managers] goes to knock on police doors for assistance. They actually know [us] that we are involved because of those documents from two forces. So how much and how bad sharing of information is, and within businesses it is not good at all.*" [ShoppingCo.Jon]. Regardless, of the preference, however, does this not dictate that police unit was also a less preferred channel due to unnecessarily disclosing of companies' names. This statement shows that firms want to share knowledge with one another anonymously.

Police and retailers' interests converge in sense that police want to arrest fraudsters, and retailers want to recover assets lost 'in transit'. Despite this common interest, why retailers have potential interest to access police. To answer this specific question we chose NetworkingCo because of its engagement with retailers and law enforcement agencies. We asked NetworkingCo whether is there any communicational gap in their collaboration. Ben [NetworkingCo], an intermediate communicator between the two categories, replied that "*Budgets and resources falling across police forces, [and] financial crimes are generally low and historically not a key interest for police. If you ask most police officers why have they joined the police? Most of them would say to deal with fraud, to arrest a murderer, and arrest the burglar. Police prioritize on things like drug, robbery and the violence crime that actually harm individuals. Whereas financial crimes are basically more than a theft, a lot of it appear as identity theft, and that's not really a glamorous sort of work police will get involved with*".

This statement clearly shows police department's lack motivation to deal identity theft. In identity frauds, fraudsters are not easily identifiable because they impersonate others. Why retailers want have interest to access police department was because as civilian organizations, retailers are unable take legal actions against identity thieves. They need police support in prosecution process. This was supported by the documents explored at ShoppingCo as "*As [a] civilian organization, we have no physical rights to search anyone under law*" [ShoppingCo.Freddy]. "*The retailer must NOT, in any circumstance, insert technical equipment [e.g. a tracker devices] into the parcel, without the*

expressed knowledge and/or authority of police. To do so would constitute a breach in RIPA1 and contravene the MPS [Metropolitan Police Service] Directed Surveillance Policy" (ShoppingCo.Doc4, 2014).

Because of lack of power to capture and prosecute the fraudsters, retailers need a collective intelligence from various law enforcement agencies including the police department. Retailers use various mechanisms to access police and NetworkingCo was one among them. Ben [NetworkingCo] by highlighting retailers eagerness for acquiring intelligence from various sources comments on ShoppingCo as follows "*The way fraud reporting [mechanism] now works is, you have NetworkingCo as one organization which will take fraud reports for prevention purposes and pass them to police for intelligence and potential enforcement outcomes. And you have 'Action Fraud' which is the central reporting mechanism. ShopppingCo is using both routes for reporting cases*". National Fraud Intelligence Bureau's 'Action Fraud' was a direct mechanism to report identity cases, whereas NetworkingCo was used as an intermediate channel. Despite these mechanisms, retailers demand enhancement of more opportunities to access police department, because during collecting evidences of identity frauds, retailers are unlikely to collect effective evidences, because fraudsters impersonate others.

To overcome this prevention collaboration gap, businesses have started training frontline officials in police force on how fraudsters commit identity frauds. This was evident by a document explored from ShoppingCo as "*ShoppingCo have been at the forefront of educating local police boroughs as to how easy a clear up an operation of this type is. This has been done by face to face meetings with borough commanders, lectures at the BRC [British Retail Consortium], at a Met Police business SPOC conference and meetings with representatives of MOPAC [Mayor's Office for Policing and Crime]. This has helped to prove we as a business are competent with our evidential packages and procedures. We will always try to assist Police when investigating one of our crimes*" (ShoppingCo.Doc4, 2014). This statement at one hand, points out those retailers wants to maximize police interest in tackling identity crimes by giving them fraud related knowledge. On the other hand, it shows that retailers try to show their competency power to police force, perhaps for their attention in tackling business frauds. What costed retailers to arrange these trainings, Greg [ShoppingCo] by highlighting impact of cost on public responded, "*I don't think the people will appreciate the cost of fraud. You are paying a little bit of your money for the goods to be stolen elsewhere. Identity fraud investigation should be treated as crime, because it does affect people. It is not just taking the money*

[1]Detail on RIPA can be found on http://www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf

from big company created to look forward". These lines clearly show that retailers spend time and energy on reducing identity frauds. However, its impact was incurred on the public at a large. Identity theft is major issue and need support from nations at a large.

Retail fraud directly or indirectly impacts public in increased prizes on products. But if the retailers are able to spot a fraudster by evaluating effective evidential material then they can apply civil recovery. They can recover on every single entity and every process to capture and prosecute the fraudsters which is true loss figure. It was not just the item stolen. Freddy [ShoppingCo] highlights about civil recovery and its benefit to the retailing industry as "*No one in ShoppingCo applies for compensation or court cost. We apply for civil recovery. We use a company, called Nottingham court civil recovery. I spend on my investigation, my observatory, hotels and all that add together, and HR, and my colleagues, and admin, fraud prevention, all those people that were involved to get the prosecution is added to the cost of the item that were stolen. That's true loss figure representation. I suppose it's not just the item stolen*".

5. Conclusions

Research Implications

This paper presents a framework for inter-organizational fraud prevention process in the retailing organizations and outlines how retailers' relationships with various stakeholders can help them to address and mitigate identity theft. In particular, we have addressed role of online fraud forum and law enforcement department in the fraud prevention process inconsistent with the retailing industry. Thus, our paper has implications on these three categories discussed below.

Firstly, our findings have significance on the retailing industry because it was the most victimized channel in identity theft and related crimes. Researchers worldwide broadly assumed that an increased knowledge sharing practice can contributes to organizational performance (Easterby-Smith, Lyles and Tsang, 2008; Becerra, Lunnan and Huemer; Van Wijik, Jensen and Lyles, 2008). Our findings support this assumption by showing an example from the UK retailing industry. Retailers' exchanged skills, expertise, and fraud prevention information was able to address and mitigate identity theft. Through our findings, we have elaborated on how fraud prevention process works in the retailing organizations, and what factors are most critical in the prevention collaboration process to reduce impact of identity theft. We have addressed role of various stakeholders and the knowledge networks that are essential in the fraud prevention process. In particular, how networking forum and law enforcement agencies were able to reduce retailers' identity related loss was discussed.

Similar organizations might be in position to consider where to start having a proper collaboration in the fraud prevention process.

Secondly, researchers explicitly lack to pay attention to how fraud forum could reduce identity frauds. Our findings suggest that online forums can explicitly, as knowledge gatekeeper, was able to address and mitigate identity theft. This paper is established on NetworkingCo, a reputable forum in the UK in fraud prevention knowledge. How it provided retailers timely and accurate information in the fraud prevention process was discussed. Additionally, we have outlined barriers that this forum faced during collaboration and addressed solutions that can be applied to overcome such hindrances. For instance, in the networking forum there was a reciprocity concern. Our findings addressed that knowledge grading analysis can overcome such barriers.

Lastly, the major finding of this study was a prevention collaboration barrier in the police and retailers' relationship, and its solution. Role of these two categories is important in the fraud prevention process because their interests converge. Fraudsters cannot be captured or prosecuted if these two categories failed to collaborate. We have highlighted how retailers train police officials to enhance their optimal interests in retailing frauds. Since fraudsters impersonate others, they were unlikely to be identified easily. Because of this police failed to pay attention on retailing frauds. Police on other hand focused issues that have immediate results such as robbery. We have highlighted that more open lines of communication between two categories can open their doors of collaboration. In particular, we have highlighted role of conferences and organized meetings to bring these two categories closer. However, training police officials on issues such as how fraudsters were able to breach security issues could explicitly increase their potential interest in financial crimes.

6. Limitations and Future Suggestions

We have addressed an unknown side of prevention collaboration, the police and retailers' relationship in identity fraud prevention process, and a gap in their collaboration. However, this relationship was established on insights from NetworkingCo, ShoppingCo and PaymentCo. None of these was from law enforcement. NetworkingCo was a fraud forum and the last two were the retailers. We have failed to inquire police unit in this line of inquiry which is a clear limitation of our study. In our findings we have suggested that police can be used in exchange relationship for retailers' fraud prevention knowledge. May be police officials having no interest in data sharing kind of work for retailers? This study could not extract opinion from them. Therefore, requires further investigation on

this aspect. Another study may add to our theory by investigating role of law enforcement agencies in this line of inquiry.

References

Ahmad, A., Bosua, R. and Scheepers, R. (2014). 'Protecting organizational competitive advantage: A knowledge leakage perspective'. *Computers & Security, 42* (2014), pp. 27-39.

Barney, J.B. and Hesterly, W.S. (2015). *Strategic management and competitive advantage: Concepts, Boston, Pearson.*

Becerra, M., Lunnan, R. and Huemer, L. (2008). 'Trustworthiness, Risk, and the Transfer of Tacit and Explicit Knowledge between Alliance Partners'. *Journal of Management Studies, 45*(4), pp. 691-713.

Chohan, R. (2016). *'An evaluation of inter-organisational identity theft knowledge sharing practice in the UK retail sector',* PhD thesis published by University of Central Lancashire.

Cifas (2015). *Identity Crime, London, UK, Cifas - The UKs Fraud Prevention Service.*

Cohen, W. M. and Levinthal, D. A. (1990). 'Absorptive capacity: a new perspective on learning and innovation'. *Administrative Science Quarterly,* 35(1), pp. 128-152.

Davenport, T. H. and Prusak, L. (1998). *Working knowledge: how organizations manage what they know, Boston, MA, Harvard Business School Press.*

Doherty, N. F., Ellis-Chadwick, F. and Hart, C. A. (1999). 'Cyber retailing in the UK: the potential of the Internet as a retail channel'. *International Journal of Retail & Distribution Management, 27*(1), pp. 22-36.

Easterby-Smith, M., Thorpe, R. and Jackson, P. (2012). *Management Research, Los Angels, London, New Delhi, Singapore, Washington DC, SAGE.*

Easterby-Smith, M., Lyles, M. and Tsang, E. W. (2008). 'Inter-organizational knowledge transfer: Current themes and future prospects'. *Journal of Management Studies, 45*(4), pp. 677-690.

Feledi, D. and Fenz, S. (2012). 'Challenges of Web-based Information Security Knowledge Sharing'. *In Proceedings of the Seventh International Conference on Availability, Reliability and Security (ARES) Prague, Czech Republic, 20-24 August.*

Feledi, D., Fenz, S. and Lechner, L. (2013). 'Toward web-based information security knowledge sharing'. *Information Security Technical Report, 17*(4), pp. 199-209.

Flores, W. R., Antonsen, E. and Ekstedt, M. (2014). 'Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture'. *Computers & Security, 43*(0), pp. 90-110.

Gaur, A. S., Mukherjee, D., Gaur, S. S. and Schmid, F. (2011). 'Environmental and Firm Level Influences on Inter-Organizational Trust and SME Performance'. *Journal of Management Studies,* 48(8), pp. 1752-1781.

Hardy, C. (1994). *Managing strategic action: mobilizing change: concepts, readings, and cases, Sage Publications Ltd.*

Hsu, M., Ju, T. L., Yen, C. and Chang, C. (2007). 'Knowledge sharing behavior in virtual communities: The relationship between trust, self-efficacy, and outcome expectations'. *International journal of human-computer studies, 65*(2), pp. 153-169.

Jasimuddin, S. M., Connell, C. and Klein, J. H. (2014). 'A decision tree conceptualization of choice of knowledge transfer mechanism: the views of software development specialists in a multinational company'. *Journal of Knowledge Management, 18*(1), pp. 194-215.

Junni, P. and Sarala, R. M. (2013). 'The Role of Absorptive Capacity in Acquisition Knowledge Transfer'. *Thunderbird International Business Review, 55*(4), pp. 419-438.

Khan, A. (2015). 'Bitcoin–payment method or fraud prevention tool?'. *Computer Fraud & Security,* 2015 (5), pp. 16-19.

Lichtenthaler, U. (2009). 'Absorptive capacity, environmental turbulence, and the complementarity of organizational learning processes'. *Academy of Management Journal, 52*(4), pp. 822-846.

Liu, D., Ji, Y. and Mookerjee, V. (2011). 'Knowledge sharing and investment decisions in information security'. *Decision Support Systems, 52*(1), pp. 95-107.

Lopez, V. W. B. and Esteves, J. (2013). 'Acquiring external knowledge to avoid wheel re-invention'. *Journal of Knowledge Management, 17*(1), pp. 87-105.

Mace, J., Parkin, S. and van Moorsel, A. (2010). *A Collaborative Ontology Development Tool for Information Security, UK, Newcastle University.*

Malhotra, D., & Lumineau, F. (2011). Trust and collaboration in the aftermath of conflict: The effects of contract structure. *Academy of Management Journal, 54*(5), 981–998.

Majchrzak, A. and Jarvenpaa, S. L. (2004). 'Information security in cross-enterprise collaborative knowledge work'. *Emergence: Complexity & Organization, 6*(4), pp. 40-50.

Mason, K. J. and Leek, S. (2008). 'Learning to build a supply network: an exploration of dynamic business models'. *Journal of Management Studies, 45*(4), pp. 774-799.

Miles, M. B., Huberman, A. M. and Saldana, J. (2014). *Qualitative Data Analysis: A Methods Sourcebook, California, Sage Publications.*

Mitchel, R., Boyle, B., Burgess, J., and McNeil, K. (2014). 'You Can't Make a Good Wine without a Few Beers": Gatekeepers and knowledge flow in industrial districts'. *Journal of Business Research, 67*(2014), pp. 2198-2206

NetworkingCo.Doc1. (2014). *Confidential Datum - Internal Newsletter to Authors.*

NetworkingCo.Doc2. (2015). *Officials Interactive Datum - Internal Newsletter to Authors.*

Newman, G.R. and McNally, M.M. (2005). *'Identity theft literature review'.* US Department of Justice.

Newman, W. L. (ed.) 2005. *Social research methods, London, Pearson.*

Noorderhaven, N. G. (2004). *Hermeneutic methodology and international business research.* In R. Marschan-Piekkari, & C. Welch (Eds.), Handbook of qualitative research methods for international business (pp. 84–104). Cheltenham, U.K., & Northampton, MA: Edward Elgar.

Nonaka, I., Kodama, M., Hirose, A. and Kohlbacher, F. (2014). 'Dynamic fractal organizations for promoting knowledge-based transformation–A new paradigm for organizational theory'. *European Management Journal, 32*(1), pp. 137-146.

Nonaka, I. and Takeuchi, H. (1995). *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation, New York Oxford, Oxford university press.*

Nonaka, I. (1994). *'A Dynamic Theory of Organizational Knowledge Creation'*. Organization Science, 5 (1), pp. 14-37.

Office for the National Statistics (2016). Crime in England and Wales: year ending. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmar2016.

Panahi, S., Watson, J. and Partridge, H. (2013). 'Towards tacit knowledge sharing over social web tools'. *Journal of Knowledge Management, 17* (3), pp. 379-397.

PaymentCo.Doc1. (2014). Retrieval Request Report: A documented experience from Merchant Risk Council Congress to Authors.

Peltokorpi, V., Nonaka, I., and Kodama, M. (2007) 'NTT DoCoMo's Launch of I-Mode in the Japanese Mobile Phone Market: A Knowledge Creation Perspective' *Journal of Management Studies, 44* (1), pp. 52-72.

Polanyi, M. (1962). *Personal knowledge, Chicago, The University of Chicago Press.*

Polanyi, M. (1966). *The Tacit Dimension, USA, The Doubleday Broadway Publishing Group.*

Rabolt, J. N. and Miler, K. J. (eds) 2009. *Concepts and cases in Retail and Merchandise Management, New York, Fairchild Books.*

Rannenberg, K., Royer, D. and Deuker, A. (eds) 2009. *Future of Identity in the information society, Berlin Heidelberg, Springer.*

Roberts, N., Galluch, S. P., Dinger, M., and Grover, V. (2012). *'Absorptive capacity and information systems research: review, synthesis, and directions for future research'.* MIS Quarterly theory and review36 (2), pp. 625-648.

Roy, S., Sivakumar, K., & Wilkinson, I.F. (2004). Innovation generation in supply chain relationships: A conceptual model and research propositions. *Journal of the Academy of Marketing Science, 32*(1), 61–79.

Ryan, F., Coughlan, M. and Cronin, P. (2009). 'Interviewing in qualitative research: The one-to- one interview'. *International Journal of Therapy and Rehabilitation, 16* (6), pp. 309-314.

Sanchez, R. (2005). 'Knowledge Management and Organizational Learning'. *Fundamental Concepts for Theory and Practice.*

Saunders, M., Thornhill, A. and Lewis, P. (eds) 2015. *Research methods for business students,* Harlow, Pearson.

Sengun, A. E., & Wasti, S. N. (2007). Trust, control, and risk: A test of Das and Teng's conceptual framework for pharmaceutical buyer–supplier relationships. *Group & Organization Management, 32*(4), 430–464.

Shaw, D. (2016). "Nearly six million fraud and cybercrimes last year, ONS says", http://www.bbc.com/news/uk-36854413.

ShoppingCo.Doc4. (2014). *Fraud prevention strategy, teams, responsibilities. A talk*. London Crime Scott, emailed to Author.

Simpson, T. W. (2013a). *'Testimony, Trust, and Authority, by Benjamin McMyler. Knowledge on Trust, by Paul Faulkner'.* Mind, 122 (485), pp. 305-311.

Simpson, T. W. (2013b). *'Trustworthiness and Moral Character'.* Ethical theory and moral practice, 16 (3), pp. 543-557.

Simpson, T. W. (2011). 'e-Trust and reputation'. *Ethics and information technology,* 13 (1), pp. 29-38.

Smythe, E. A., Ironside, P. M., Sims, S. L., Swenson, M. M. and Spence, D. G. (2008). 'Doing Heideggerian hermeneutic research: A discussion paper'. *International journal of nursing studies, 45*(9), pp. 1389-1397.

Stahl, F., Parkin, E. S. and van Moorsel, A. (2011). Cooperative Information Security Knowledge: Content Validation and incentives to contribute, Newcastle upon Tyne, Newcastle University.

Stanford Centre for Biomedical Informatics (2016). Protégé. http://protege.stanford.edu/products.php#web-protege. Accessed: 01/03 2016.

Statista (2018). "E-commerce in the UK - Statistics & Facts". https://www.statista.com/topics/2333/e-commerce-in-the-united-kingdom.

Styhre, A. (2011). Knowledge Sharing in Professions: Roles and Identity in Expert Communities, USA, Gower Publishing Ltd.

Tamjidyamcholo, A., Baba, M. S. B., Shuib, N. L. M. and Rohani, V. A. (2014). 'Evaluation model for knowledge sharing in information security professional virtual community'. *Computers & Security, 43,* pp. 19-34.

Tamjidyamcholo, A., Bin Baba, M. S., Tamjid, H. and Gholipour, R. (2013). 'Information security – Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language'. *Computers & Education, 68* (0), pp. 223-232.

Trustwave (2013).Trustwave 2013 Global Security Report. http://www2.trustwave.com/rs/trustwave/images/Trustwave_GSR_ExecutiveSummary_4page_Final_Digital.pdf. Accessed: 20 November 2013.

Tsoukas, H. (2011). *'How should we understand tacit knowledge? A phenomenological view'.* In: Easterby-Smith, M. and Lyles, M. A. (eds.) Handbook of Organisational learning and knowledge management, pp. 453-476. Chichester, UK, John Wiley and Sons.

van Riel, C. B. and Fombrun, C. J. (2007). Essentials of corporate communication: Implementing practices for effective reputation management, Routledge.

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

Yin, R. K. (2009). Case Study Research: Design and Methods, USA, SAGE Publication, Inc.