The management of first party fraud in e-tailing: a qualitative study

Amasiatu, C. & Shah, M.

Original citation & hyperlink:
Amasiatu, C & Shah, M 2019, 'The Management of First party fraud in e-tailing: A qualitative study', International Journal of Retail & Distribution Management, vol. (In-press), pp. (In-press).
https://dx.doi.org/10.1108/IJRDM-07-2017-0142

DOI 10.1108/IJRDM-07-2017-0142
ISSN 0959-0552

Publisher: Emerald

The Management of First party fraud in e-tailing: A qualitative study

Abstract

Purpose – First party fraud in which retail consumers commit fraud against retailers is a growing problem. However, to date studies on retail crime have focused almost entirely on fraudulent consumer behaviours in physical stores. With the growth of e-commerce, the losses from this fraud is growing so there is strong need to research this problem from multiple perspectives.

Methodology – We conducted three case studies and a total of 24 semi-structured interviews with retail managers and evaluated their existing prevention-related documentation. Fraud management lifecycle theory was used to organise and discuss the findings.

Finding – We found that many retailers are treating this problem as just a cost of doing business online and have no detailed plans for dealing with this problem or any reporting to law enforcement agencies. However, they have begun working with delivery companies for delivery accuracy. Use of convenience stores as collection points is also showing early improvements.

Limitations – The small number of cases and interviews used is a limitation of this study. However, we believe that the findings are useful for advancing knowledge in this emerging research area.

Practical Implications - This study provides insight into existing management practices in this domain, and makes recommendations on how to improve the management of first party fraud. The study also makes a case for increased managerial interest and involvement in reducing first party fraud. The study also helps bridge a glaring gap in existing literature and provides useful leads for further research.

Originality/value – To our knowledge, this is the first study to evaluate the existing practices employed to manage first party fraud in e-retail.

Keywords – First Party Fraud, Retail Fraud, Consumer Fraud, Online Consumer Fraud, Consumer Misbehaviour, Retail Crime Prevention

Introduction

Advances in Information Technology have made e-commerce possible by eliminating the time and space limitations of traditional brick and mortar retailing. Whilst e-commerce provides many advantages over brick and mortar retailing, i.e. access to a global audience and convenience of shopping anytime and anywhere, it has generated new challenges/risks associated with information security, online frauds etc.

First party fraud, in which retail consumers engage in various dishonest acts in an e-commerce environment with the aim of gaining an advantage in the exchange is a growing challenge for online retailers, here referred to as e-tailers (BRC, 2013; Retail Fraud, 2013).

The most common forms of first party fraud in the retail industry are: deshopping, chargeback, bust out fraud, and misrepresentation of details (Amasiatu and Shah, 2014, 2015). Deshopping occurs when consumers purchase products with the intention to return them after use; chargeback fraud occurs when consumers deny receiving delivered goods or return different goods to those dispatched; bust out fraud occurs when consumers apply for and use retail credit facilities with the aim of not fulfilling their credit agreement e.g. when relocating abroad; misrepresentation of details occurs when consumers dishonestly misrepresent financial or personal details in order to get access to credit facilities they would otherwise not be entitled to.

A review of existing literature provides evidence to suggest that first party fraud is widespread and has profound impact on retail profitability (Amasiatu and Shah, 2014; Hinsz, 2016). For example, the British Retail Consortium estimates the cost of first party fraud in the region of £74 million or 32% of fraud costs (BRC, 2015), while an independent survey estimated the cost to be £405 million (Retail Fraud, 2013).

Despite the prevalence of first party fraud, to date studies on retail crime have focused almost entirely on fraudulent consumer behaviours within brick-and-mortar/physical stores. With the growth of e-commerce and the move towards online retailing, it is important for research in this area to continue into e-retail.

This paper is therefore aimed at bridging the gap in knowledge in this area, in response to calls for increased research in the area of fraudulent consumer behaviour in e-tailing (Amasiatu and Shah, 2014; Harris, 2010; King and Dennis, 2003).

This study also tried to explore the various practices adopted by retailers to manage first party fraud. To achieve these objectives, we conducted a total of 24 interviews with retail staff involved in the management of first party fraud across three retail organisations. In addition, we conducted a comprehensive literature search on fraud management practices with the use of various electronic databases. Guided by literature, the focus was on a holistic approach to fraud management rather than on a single fraud management activity.

Researchers such as Amasiatu and Shah (2018), Durbin (2007), Wilhelm (2004) suggest that adopting a holistic approach to fraud management can lead to superior fraud loss performance. These recommendations necessitated the need for a holistic fraud management framework to guide the data collection process. The fraud management framework by Wilhelm (2004) was used to evaluate the existing management approaches employed to deal with first party fraud.

A brief background to provide a context for this research is first presented. Next a summary of the research framework adopted is presented before the research approach and findings are discussed.

Background

First party fraud has been noted as one of the most significant challenges to online retailers, due to its prevalence and regularity (BRC, 2013; Retail Fraud, 2013: Hinsz, 2016).

Extant literature mentions various reasons for the prevalence of first party fraud. For example, King and Dennis (2003), Reynolds and Harris (2005), and King et al. (2007) provide several accounts to show that organisational policies (such as lenient no-questions asked returns policies) and limited action and/or inaction by retailers reinforce fraudulent behaviour. Furthermore, first party fraud is easy to commit and often requires little or no sophistication.

Liberal returns policies are perceived as an essential part of customer service and used as a competitive weapon in today's retail environment. In e-commerce, returns policies are considered even more imperative due to the lack of physical interaction with a product (Foscht et al. 2013). Returning products allow customers to reverse the purchase decision and provide competitive advantage to a retailer.

Prior research has shown that whilst a lenient returns policy can create a competitive advantage for a retailer, it can also expose a retailer to abuse (Peterson and Kumar, 2009). For example, deshopping fraud where consumers order and return items after they have been worn/used has been largely facilitated by e-commerce (Schmidt et al., 1999; Piron and Young, 2000; King and Dennis, 2006).

Furthermore, when goods are ordered and move through the supply chain, there are many opportunities for things to go wrong, i.e. theft/loss of parcel, damage in handling, delivery to the wrong address, etc. which increases the opportunities for abuse.

Therefore, the opportunities available to misbehave and the convenience provided by online shopping combine to make misbehaviour more attractive online.

Despite the prevalence of this behaviour, extant literature suggests that retailers do not appropriately deal with this fraud committed by their own customers for various reasons such as poor understanding of first party fraud, fear of negative impact on customer experience, etc. (Amasiatu and Shah, 2018; Fullerton and Punj, 2004; King et al., 2007). Furthermore, tackling business crime is not always high priority for law enforcement agencies and the general public have a more positive attitude towards this fraud compared to other frauds (Wilkes, 1978; Dodge et al., 1996; King and Levi, 2003), which means that there is very little deterrent effect for potential offenders and reoffenders. With the growth of e-commerce and prevalence of this fraud, assuming first party fraud to be a cost of doing business is not a sound strategy, hence any applied research such as this one could be very useful for retailers.

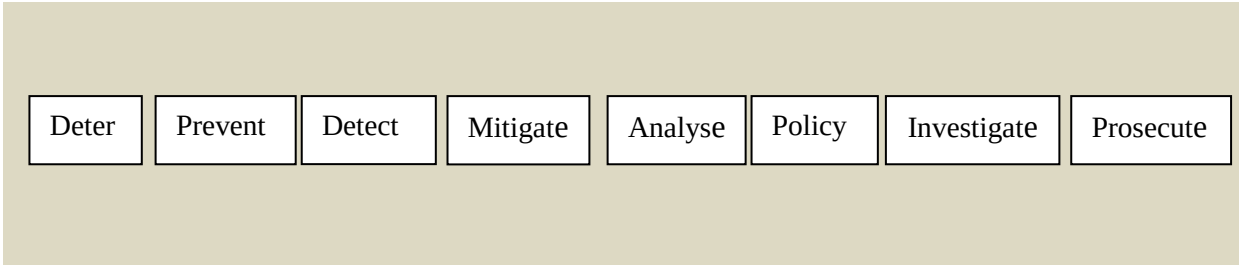
Research framework

For effective fraud management, a coherent strategy is preferred rather than a focus on isolated fraud management activities (Bishop, 2004; Button and Brooks, 2009; Durbin, 2007; Wilhelm, 2004). We reviewed literature with an aim to find a framework that is either used in first party fraud or similar context, so that that the framework can be used to evaluate the existing management approaches adopted by the retailers in this study. There are a number of fraud frameworks in the literature such as Furlan and Bajec's framework that was developed for insurance fraud, Wilhelm's fraud management lifecycle theory, Government Accountability Office (GAO) framework for disaster assistance programs, the anti-ID fraud framework and the identity fraud enterprise management framework. These frameworks contain essential elements or components

for successful fraud management. Even though these frameworks bear many similarities, the fraud management lifecycle theory was chosen for this study mainly due to its flexibility and compatibility with the retail industry and nature of fraud studied. Besides, it has been empirically tested in a number of industries, designed with the private sector in mind although flexible enough to be adapted to other sectors and has received favourable reviews and citations in a number of research papers. Nevertheless, the framework elements represent in the authors' views appropriate components for successful fraud management. The other frameworks were either too complex or too simple to be used for this study.

The fraud management lifecycle theory (Wilhelm, 2004) underpins this research so we present a brief description of it here. Wilhelm (2004) proposed the Fraud Management Lifecycle Theory consisting of eight components that drive success or failure in fraud management: Deterrence, Prevention, Detection, Mitigation, Analysis, Policy, Investigation and Prosecution (See figure 1 below). Wilhelm (2004) argues that the aim of the framework is not to present a series of sequential operations or elements, but to present the essential activities necessary for fraud management. Wilhelm (2004) subsequently applied and tested his framework in four different industries and claimed that all eight activities were present and vital for successful fraud management.

Figure 1- Linear Representation of the Fraud Management Lifecycle Theory (Source: Wilhelm, 2004)



Different elements of this framework are briefly explained next: *Deterrence defined by* Wilhelm, (2004, p. 10) as "activities designed through fear of consequences or difficulty of penetration, to turn aside, discourage, or prevent fraudulent activity from being attempted" (Wilhelm, 2004, p. 10). In this sense, activities designed to communicate the consequences or disincentives of misbehaviour have an effect on discouraging offenders or would-be offenders from misbehaviour. Applying *prevention* in the context of fraud, researchers have suggested that a number of activities are essential at this stage, such as knowing the size of the problem, internal and external collaboration, senior management or executive level involvement, training and screening of employees and fraud-proofing new policies. *Detection* is intended to reveal or detect fraudulent activity, often through the use of statistical techniques and algorithms. *Mitigation* activities are those activities that are intended to stop fraud and prevent further losses following detection. *Analysis* is concerned with carrying out a thorough analysis and understanding of successful frauds in order to determine the underlying cause of their success. *Policy* activities are those activities or actions undertaken to evaluate, or develop policies to mitigate fraud risks. *Investigation* is concerned with searching, collecting, and retaining evidence that will enable offender sanctioning, prosecution or redress. *Prosecution* activities are concerned with putting forward a case that will lead to offender punishment. The research approach and findings are discussed next.

Research Approach

We adopted a qualitative case study approach as our research objectives were mainly about understanding how retailers are managing the problem of first party fraud. Focus was on getting a detailed insight rather than surveying an entire industry so our choice of research method was made with the nature of research objectives in mind, which were:

- To understand how retailers were managing first party fraud
- To provide recommendations based on the findings from three case studies and literature review

Using the case study approach, this study investigated the approaches or methods in three selected companies. As these companies are some of the largest and most successful retailers (in terms of sales and revenue) in the UK, it was expected that there would be plans in place for managing first party fraud. The fraud management lifecycle theory (Wilhelm, 2004) was used to organise, discuss and assess the approaches used within the companies.

In order to understand how retailers managed first party fraud an appropriate interpretive research approach is needed. The case studies conducted as part of this study looked specifically at existing management practices employed by the retailers to manage first party fraud. One of the objectives of the study was to compare different cases in order to understand how retailers were managing this fraud.

We adopted a systematic approach to this study. Firstly, interview questions were formulated around the elements of the framework based on findings from the literature review. A pilot study was then conducted on 8 postgraduate students following the steps mentioned by Wengraf (2001). Participants were chosen based on their experience or

knowledge of first party fraud, and asked to look out for a number of things like repeated questions, clarity of questions among others. Comments and feedbacks were subsequently taken into consideration when revising the final interview questions.

Once the interview questions were deemed ready for use, semi-structured interviews were carried out with three retailers. To identify the case organisations, about 20 retailers were invited to be part of the study by mail, 3 of which indicated interest in the study. Semi-structured interviews were used as the data collection method. Interviews are one of the most important sources of case study information (Yin, 1994; Yin, 2014). The selection of interviewees for the study was purposive, mainly from individuals involved in managing, detecting or preventing first party fraud. This approach has been adopted in many other similar studies (for example, Brooks et. al., 2009; Bussmann and Werle, 2006). For convenience and to limit travel time for the researcher, three of the interviews were conducted over the phone. A total of 24 interviews were conducted across all three retailers: 13 interviews in the first company, 7 in the second and 4 in the third company. The number of interviews in each case was according to the availability of relevant individuals for the interview. Participating in the study was entirely voluntary and consent was sought with each respondent in advance in line with research ethics. Each interview took between 45 and 90 minutes. All interviews were recorded using digital voice recorder and later transcribed, and a manual approach of coding and analysing the data based on themes from the fraud management framework was adopted.

Description of case organisations

This section presents a summary of each of the three cases studied and the respondents in each of the companies (see table I below). In keeping with the confidentiality

agreement, the identities of the companies and respondents have been taken out and are henceforth referred to as Company 1, Company 2, and Company 3.

Table I. Description of respondents at Company 1, 2 and 3

Company 1

Company 1 is a leading multi-brand digital retailer in the UK and Ireland, selling 100s of big name brands as well as its own brand of retail goods. Following the growth of e-commerce, the company repositioned itself as a digital retailer with over 80% of its sales now carried out online.

It is a company that thrives on new ideas with the ambition to reach more people and make their brands accessible. With such ambitious goals, company 1 placed a strong emphasis on increasing sales and customer satisfaction. The study identified issues concerning the organisational goals that impacted first party fraud management, e.g. a focus on sales that was incongruent with appropriate sanctioning of offenders.

Company 2

Company 2 is one of the top supermarket chains in the UK by size, with 100s of stores in the UK. Having built up its store presence well before venturing into online retailing, the company has implemented a range of strategies to deal with store crime. However, following its transition to digital (e-commerce) retailing, new opportunities for customer abuse arose. The company attributes both third party stolen card fraud and fraudulent first party (customer) claims as their biggest online fraud losses.

Like Company 1, Company 2 placed a strong emphasis on customer service that again seemed to be detrimental to its first party fraud management capability, mainly its very generous returns policy which allows return of online orders up to 12 months after purchase which most respondents perceived to be encouraging deshopping.

Company 3

Company 3 is one of the top 5 supermarket chains in the UK by size, with well over 400 stores in the UK. The company has a robust e-commerce platform, and is one of the fastest growing online fashion retailers in the UK.

Company 3 has a well-established store presence all over the UK with a range of strategies to deal with store crime. However, new opportunities for customer abuse have arisen following the growth of e-commerce. The strength of the company's fraud initiative was that there was a fraud strategy within the business, however first party fraud was largely not considered a serious threat to profitability and so is a small line item in the budget when compared to other crimes.

Results and Discussion

A summary of frauds faced by the participating companies is given in table II. *Deshopping* refers to the return of items (for a refund) after they have been worn. *Refund fraud* occurred when customers denied receiving all or some of the items delivered to them. *Misuse of facility fraud* occurred when customers fraudulently misused credit facilities with the intention that payment will not be made or made in full. *Chargeback fraud* occurred when customers deliberately denied making orders, while *Coupon fraud* occurred when customers knowingly reused one-off vouchers/coupons as a result of system error/fault.

Table II. Comparison of first party fraud types across the three retailers (Y= present, N=absent)

Deterrence

Deterrence is considered an essential first step in the management of fraud (NHS CFSMS, 2009; Wilhelm, 2004). The aim of deterrence is to deter people from engaging

in fraud through fear of consequences. This includes raising awareness of the costs and consequences of fraud (Wilhelm, 2004).

Amongst the companies interviewed, the focus was mainly to manage fraudulent behaviour once they arose rather than deterring them pro-actively. None of the retailers pursued any educational/consumer awareness activity to highlight the costs and consequences of engaging in first party fraud. Rather, deterrence resulted from the deterrent contributions provided by the other framework/fraud management activities, as illustrated below:

> When you challenge them, some of them will stop claiming for a while…(Company 1)

> Following our investigation, we can then challenge the customer and say we have information that shows that you are lying, and that usually scares them off or stops any further contact (Company 2)

> Well, if they do it once, we will allow it but if it carries on we know there is a pattern and we take it seriously…we can deny them the claim and that stops some of them from continuing (Company 3)

Retailers believed that customer education and awareness were vital; however, this was not pursued in any of the participating companies. One of the participating retailers suggested that it was not cost effective to engage in any awareness program at least at that moment.

> Are we looking to undertake deterrence? No. Because we don't lose much from these frauds… In the bigger scale of things it's not a lot, I mean not in millions yet (Company 2)

Researchers such as King and Dennis (2003), King et al. (2007) and Rosenbaum et al. (2011) highlight the importance of education as a means of changing the motivation of offenders. The findings of the current study whilst reinforcing the extant ones also show that despite the time interval between the reported studies and this current one, retailers are still not pursuing any form of education or consumer awareness as a vital component

of their first party fraud strategy. Therefore, it can be implied from the information that deterrence as a strategy does not feature prominently in the actions undertaken by these retailers in tackling first party fraud.

Prevention

One of the most common prevention activities referred to in the interviews was staff training. Training employees to be aware of first party fraud red flags is an important step in improving fraud prevention performance. Warehouse staff and call centre staff most often were involved in the management of first party fraud, i.e. detecting deshopping (by properly inspecting returned items) and/or fraudulent claims by customers. However, these jobs were often seen as low-level jobs that attracted little training. The retailers interviewed provided mostly on-the-job training on first party fraud red flags to staff in relevant positions, however responses varied across retailers. Whilst two of the retailers agreed the training provided could be improved, they believed that the training provided was nonetheless helping to reduce their fraud losses. On the other hand, one of the retailers was less confident in the level of training provided to employees in these areas, which limited prevention capability. Knowledge limitations are likely to limit the detection of fraud.

> We have examples where customers will order like Microsoft Xbox reward points and have very sophisticatedly opened the cellophane wrapping on the product to get the reward points…and then repackage it back, a sophisticated level of repackaging where it is quite hard to the untrained eye to spot that the packaging has actually been tampered with and has been opened and used…We have trained our warehouse returns staff to the point where they can tell when the product is returned that it has been tampered with (Company 1)

> They are so many models of iPad, and if you have got someone in the warehouse that has never had an iPad before and someone's ordered the latest iPad and returned the old iPad in that box and it looks brand new, and they put a seal on it to make it look like the original one, it is very easy to get away with it…All we do is scan the barcodes of the returned item and

> check if it is the original item, but some of these customers take the barcodes off of the original model and stick it on the back of their old one, and the guy at the warehouse will scan it and if looks like the original one they just presume it is the item (Company 2)

Formal fraud awareness training was however provided to other more senior management staff, for instance:

> There is a workshop that other retailers attend that I attend every couple of months also to discuss current trends, current patterns that people have seen, give other people tips and things like that (Company 2)

> The training I have done through the company is a year course in your own time and in the evening and at the end of it you get a qualification in criminal law, so that from the law side is the qualification that I have got, and I have also got a lot of management qualifications (Company 1)

Although senior managers may know how to react to fraud, this is of little benefit if more junior employees (who are tasked with detecting first party fraud) are unable to identify it in the first place because of lack of or inadequate training or understanding.

Internal and external collaboration is also essential in preventing fraud - the more comprehensive the information a retailer can gather about an individual, the easier it is to know when the customer is lying (FSA, 2006; NHS CFSMS, 2009; Wilhelm, 2004). All three retailers believed external collaboration was important in tackling first party fraud, however we found this to be minimal.

> We currently share information with other retailers, like modus operandi via emails or phone calls. We do this bi-weekly. We do not share the details of the customers though (Company 2)

> We discuss specific jobs…say have you had an issue at this particular address or area or just in general, general chat about what fraud actions they take and what we do (Company 1)

> We currently share information with a few retailers like problems with particular addresses but we are currently working with other retailers to have a robust data sharing agreement in place to strengthen our defence (Company 3)

One obstacle to effective external collaboration that emerged was that these retailers sometimes saw fraud prevention as offering a competitive advantage, therefore information sharing could jeopardise this edge. During the interviews, some of the retailers spoke of how their superior preventative measures pushed fraud to other retailers. If competitive interests could be put aside, more comprehensive information sharing and collaboration could provide tactical advantage to retailers by providing information about offenders that can help reduce fraud.

Pre-employment screening of employees and/or contractors is also an important preventative strategy (Brooks et al. 2009; Button and Brooks, 2009). The retailers interviewed mostly regarded the job of drivers and warehouse staff as low-level jobs that required very little or no pre-employment checks, even though these employees occupy trusted positions that could expose retailers to abuse. Consumers can take advantage of a retailer's weakness such as staff theft to make fraudulent claims, and so recruiting honest staff is crucial in reducing opportunities for first party fraud, as demonstrated by this respondent.

> We have customers now claiming to have received empty boxes on high value items such as iPads and electronic items. This is because we used to have situations where empty boxes were delivered to customers, usually on low value shoes due to thefts at our depots, but never on high value items. Some customers saw the glitch in our system, and now started claiming on high value items like iPads (Company 1)

Reference checks were mostly sought and little else, and even sometimes these checks were not sought. For company 2, reference checks and/or background checks were sought for staff in these areas while company 1 carried out only reference checks. Only company 3 claimed to carry out background checks on all employees. However, respondents suggested that these checks were not always carried out.

> We are meant to carry out these checks, but we have so many colleagues and some get through without checks (Company 2)

> These drivers don't get CRB checked because it costs too much, the business doesn't consider it and it's wrong (Company 1)

More worrying is the fact that screening for agency staff was left to be the responsibility of the agency/agencies.

> We don't know if they do any checks on the drivers, we sign the contract and we expect them to adhere to it (Company 2)

> The security checks carried out on these drivers could definitely be a lot better. Sometimes on the run up to peak times, sometimes their backs are against the wall really, they have got to find all these drivers to get all these parcels out to the customer. So, I think during those peak times that the checks are not as thorough (Company 1)

Finally, the retailers interviewed employed the use of technology as well as working with delivery companies to improve delivery accuracy in order to prevent fraudulent customer claims. Some of the solutions employed include monitoring customer claims and returns using database, automated transaction risk scoring to flag up orders for manual review, delivery van tracking and end-to-end tracking of parcels, CCTV in depots and warehouses (to stop theft and reduce opportunities for fraudulent customer claims, use of collection stores as collection points, and weighing high value items prior to dispatch to reduce the opportunity for fraudulent empty box claims.

Detection

For the purpose of this study, detection activities are those intended to identify fraud during and subsequent to the completion of the fraudulent activity. Early detection and mitigation helps reduce the impact of fraud on a company (NHS CFSMS, 2009; Wilhelm, 2004).

In the wider fraud arena, detection is often done using automated statistical techniques and algorithms, however we found that the detection of first party fraud was not

completely automated and sometimes involved manual detection methods. This meant that detection and mitigation activities were often performed within the same function and team. These activities are further reported in the next stage of the fraud framework.

All retailers emphasised the importance of training front-line staff in detecting first party fraud. For example, respondents claimed that deshopping was managed in this way by having warehouse staff inspect returned items visually and sometimes through smell.

Respondents also claimed that credit applications were credit-scored to minimise losses, and that those applications not meeting set thresholds were either automatically rejected or flagged up for manual review.

The way the retailers' detected fraudulent first party claims varied considerably. Company 1 had a dedicated and specialist first party fraud team within their customer care team that detected and mitigated first party fraud claims, while other fraud cases were handled by their more generalist fraud team. On the other hand, the more generalist fraud teams in Companies 2 & 3 were tasked with the detection and mitigation of all fraud cases including first party fraud claims. However, we found that identity fraud and internal staff fraud investigations were often the priority for these more generalist fraud teams.

When first party fraud was suspected in some cases, without substantial evidence of the behaviour customers may deny their behaviour leaving the retailer in a vulnerable position. For instance:

> I had this customer that had bought a coat from us and returned it after some days, and it was clearly worn. When we checked the pocket, we found Tesco receipt in the coat with the buckle broken, so we returned it back to the customer, but the customer contacted us and then claimed the buckle was faulty when it was delivered. In the end, we had to refund her (Company 1)

> If we haven't got enough evidence we set them up; if we know someone is not good we will try and keep it to ourselves and let them carry on doing it and we catch them out (Company 2)

> We are now technologically in a place where we can prove to a customer that we have delivered the parcel or to at least have enough proof to challenge the customer if they are claiming the parcel has not been received. We believe that we have stopped the level of exploitation that we were having because if you have no signature and you have no GPS codes and you have little information available, it is hard to challenge a customer if they are claiming that the goods have not been received. So what we were finding was that we were in a position where we inevitably had to credit the customer and give the customer the benefit of the doubt (Company 1)

> There are lots of times when parcels get lost in transit and we do redeliver or refund the customer if we can't prove that it was delivered but that's why we use DPD for those higher ticket items because the risks are a lot higher with the higher items (Company 2)

Mitigation

Mitigation activities begin once a reasonable suspicion of fraudulent activity is detected. Mitigation focuses on actions that are intended to reduce the extent of fraud losses and to stop fraudulent activity from continuing (Wilhelm, 2004).

Retailers mitigated losses from deshopping by training warehouse staff to detect and reject worn, used or wrong returns. However, the extent to which they pursued this strategy differed between retailers, with some retailers adopting a more lenient position compared to others. Some of the respondents in company 2 blamed their very lenient returns policy, which in their opinion was encouraging deshopping. These respondents further suggested that they sold off a lot of the returned stock (which could have been detected and mitigated) to other retailers to re-coup some of their losses:

> Last year, we used to job off around £8000 worth of stock a week…Yes, so we are recuperating a lot of that back from selling it on so that is where we mitigate the losses in terms of getting it back because we can't put them back to stock (Company 2)

With regards to fraudulent refund claims, retailers often relied on the offender's prior history as a predictor of future behaviour. The retailers who referenced an individual's prior history had robust systems for collating information on past behaviour. Information gained from an individual's prior history was used to determine future behaviour. Respondents assert that there is a strong relationship between an offender's profile and a combination of their past behaviour and attitude.

> I had this customer who was claiming one of the items in her parcel was missing - a camera worth £579 which was in a parcel with another item of £48. She had already said to me that she opened the parcel herself and it wasn't damaged in anyway. She was adamant that the item wasn't there. So I challenged her- told her I was going to investigate it...She called back two days later and said she had found the camera…She has only just been a customer with us just under a year and she has already had £225 off us with a previous claim two months ago and she was trying to get £579 off us there … if they have been successful the first time around they try it again (Company 1)

The workings of the specialist first party fraud team in Company 1 offer useful insight into how to improve first party fraud detection and mitigation methods. This company uses similar techniques to those used in the insurance industry, such as cognitive interviewing and voice-stress analysis. A dedicated team of customer service advisers were trained on these techniques in order to detect and mitigate customer fraud. Usually open questions are asked and investigators look at behavioural cues such as signs of nervousness, stammering and contradictory statements, to determine if the customer is lying. The retailer claimed that this approach helped it significantly reduce its losses from first party fraud.

> You find that the person who is dishonest is the one who becomes more aggressive and shouts loudest…sometimes you hear them stammer…and they argue with you, trying to throw you off…
>
> If they lie, they say one story in the first call and the next time it's completely different, and I think then why did you say that the first time (Company 1)

However, we found that due to escalating caseloads, investigators prioritised cases for investigation usually based on a combination of experience/judgement, customers' claims history and monetary value, which limited the retailer's overall fraud performance.

Some of the respondents also reported that internal collaboration between their fraud teams and other departments when fraud was suspected or proven was important in mitigating fraud losses:

> "If we had any customer that has had a lot of claims on their account, we would inform our warehouse so that deliveries can be made with sufficient evidence…we can take pictures of the parcels before delivering and require signature on delivery…" (Company 1)

> "I had this customer who had several accounts with us and had made multiple claims on the accounts, the last claim was gold jewellery which she claimed she didn't receive, about £5000. I got senior managers involved and the customer was visited. I recommended shutting the account because of the many high value claims as it was becoming uneconomical…" (Company 1)

However, we found that there were often no formal channels of communication between the fraud teams and sales/order and warehouse teams. Consequently, it was not unusual for orders to be accepted and delivered to individuals with high claims histories in such a manner that sufficient evidence was not gathered prior to dispatch, thereby exposing retailers to further abuse.

This was often due to in part to the manner in which the fraud teams informed the sales teams and warehouse staff of suspicious accounts. This was usually done through internal correspondence or contact.

Consequently, we believe there is potential for the use of rule-based detection algorithms or behavioural models to improve detection and mitigation capability and provide more benefit to retailers. In addition, better integration between teams,

especially the analysis, mitigation and investigation functions can provide statistical recommendations on case prioritisations.

Investigation

Investigation is a vital component of an anti-fraud strategy (Furlan and Bajec, 2008; Wilhelm, 2004). Retailers 1 & 2 confirmed that investigations were effective based on the outcomes, i.e. successful outcomes where customers owned up when confronted. However, potential savings made could not be confirmed. Company 1 cited instances where customer investigations have uncovered the possibility of fraud and the customers owned up to their fraudulent intent.

> We had this customer that was constantly claiming not to have received ordered items. A member of our field team visited the customer with the police and we found a stockpile of products in the customer's home over £40,000 worth, some belonging to other retailers, and we notified these retailers (Company 2)

> We have had cases where customers apologised and said they didn't realise that anyone would follow-up (Company 1)

In these cases, the losses were mitigated. The way investigations were conducted varied between retailers. For example, in company 1, suspected fraudulent claims were dealt with using the experience of specially trained customer service advisers, who investigate and challenge customer claims. This approach places claims investigations with those at the front end - those closest to the customers - who were in a better position to assess and investigate the cases as efficiently as possible. These advisers received more specialist first party fraud training (compared to the rest of the customer service advisers) including the behavioural aspects of fraud. This approach was considered to yield positive results in some cases, as some customers would own up and admit that they received the parcels they were previously claiming not to have received. On the other hand, the fraud teams in Companies 2 & 3 carried out all fraud investigations

including first party fraud investigations. We found that first party fraud investigations were often the priority for these central fraud investigation teams.

With investigations, the participating companies sought further information, either from the customer or building up clear evidence of intent. For companies 1 & 2 this involved having more senior loss-prevention managers visiting customers' locations, sometimes accompanied by police, to query offenders (mostly serial offenders). As part of their investigations, all three retailers also monitored serial offenders' order activity by picking and delivering their parcels in a manner that required capturing and maintaining evidence, for example, taking pictures of parcels prior to delivery and accompanying drivers during delivery.

Analysis

The importance of regular fraud risk assessment, monitoring and analytics in the management of fraud has been highlighted in the literature (Furlan and Bajec, 2008; Wilhelm, 2004; Gee, 2009). Fraud was generally monitored and reported to fraud managers or loss prevention managers at all three retailers we studied. However, of the three retailers only company 1 claimed to have an estimate of its first party fraud losses. In addition, whereas risk analysis was carried out at all three retailers following any major first party fraud incident, company 1 carried out detailed monthly first party fraud risk analysis overseen by a working group. This working group led by senior risk managers and including representatives from the main business units and support areas, meet on a monthly basis to assess their first party fraud losses including the value, root cause, prevention controls in place. This group also appraises the effect of their fraud strategy on their overall objective of reducing first party fraud losses and uses the insights gained from their fraud analysis to implement new policies or update existing ones. It emerged that the fraud strategy adopted by this retailer had resulted in

significant first party fraud loss reduction, up to 40% reduction, in a single financial year.

> We have a steering committee that meet monthly...we produce a monthly financial information pack of where our first party fraud claims have occurred and broken down by the cause, which carrier is responsible, which area of the business is being accountable for the claim. We will then use the information to focus on where we have our worst defences and challenge those areas of the business to carry out further investigation and report back. (Company 1)

> Every investigation we do has a case report, and every case report has a correction of errors. We carry out the corrections that mitigate the actions in the future. It's about learning from our previous cases (Company 2)

Fraud-risk identification and control also featured in the review process for new products and delivery channel for all three retailers. For example, for company 1, prior to the introduction of collection points in convenience stores, trials were done to make sure the channel did not introduce more frauds. All three retailers acknowledged the importance of good analytics in the prevention of all frauds.

Policy

Policy activities focus on the creation, evaluation and communication of fraud policies to reduce the incidence of fraud. Policy activities usually take advantage of the knowledge gained from the other framework activities, and are usually undertaken by very senior managers in an organisation (Wilhelm, 2004).

We identified attempts by some of the retailers to mitigate first party fraud by revising some of their policies or even adopting new initiatives to minimise fraud losses. For example:

> We have customers now claiming to have received empty boxes on high value items such as iPads and electronic items. This is because we used to have situations where empty boxes were delivered to customers, usually on low value shoes due to thefts at our depots, but never on high value items. Some customers saw the glitch in our system, and now started claiming on

> high value items like iPads…We used to just credit their accounts, but as this grew we had to step up security around those high value items (Company 1)
>
> …That's why we now use DPD for those higher ticket items because the risks are a lot higher with the higher items (Company 2)

Respondents indicated that following increasing losses from first party fraud, their companies would no longer accept returns without the tags or labels in place or if it showed any sign of use. Retailers also mentioned the adoption of new policy initiatives such as the use of collection points in convenience stores to improve customer experience and reduce fraudulent refund claims and adoption of end-to-end tracking of high value items to minimise refund fraud losses.

Prosecution

Prosecution is defined as the process of conducting legal proceedings against an offender for crime or breach of the law, with the aim of deterrence, restitution or recovery of losses (Wilhelm, 2004; NHS CFSMS, 2009).

During the course of the research we found that prosecution was rarely pursued by any of the three participating retailers. Some of the respondents indicated that the external environment influenced their ability to undertake some activities in the fraud management lifecycle, particularly prosecution. Retailers reported experiencing mixed responses from the police when reporting fraud. The response received depended on a lot of factors such as the amount, the individual police force's ability to investigate, police knowledge of the type of fraud (third party identity fraud was thought to be more familiar to the police and easier to prove than first party fraud) and whether the company could prepare the case or referral to the police in a way that was acceptable or police-friendly. At times, respondents expressed lack of confidence in the service

they received from the police especially with regards to first party fraud compared to other crimes like shoplifting:

> What we have found is that the police will always tend to say it needs to go to action fraud because it is fraud, but nothing happens (Company 2).
>
> I mean depending on the amount, the police are also reluctant to take on any case where we are trying to claim fraud anyway; they always want to refer us to action fraud… It's a job for the police and not action fraud investigation. Sometimes you feel like you are hitting a brick wall dealing with the police (Company 1)

Despite the largely negative reception from the police, there was also evidence from company 2 to suggest a good response from the police irrespective of the type or nature of the fraud. With such mixed responses, it is difficult to draw a conclusion. However, it can be deduced that the general impression from the police with regards to first party fraud varied from 'uncooperative with a reluctance to take on first party fraud' to 'not interested in low-value fraud'.

On the reasons why the police may be reticent to take on cases of first party fraud, respondents cited lack of police resources to deal with fraud issues, with majority of the respondents in the three companies expressing the need to build up evidence and carry out investigation themselves prior to reporting to the police.

Retailers also did not pursue any civil litigation cases. When customers were found guilty of fraudulent activity, we found that financial considerations were used to determine the level of sanction imposed. For the most part, the main punishment given to offenders was to reject the fraudulent claim or blocking serial offenders temporarily from making further purchases. Depending on the amount and the weight of evidence, prosecution could be sought (although rarely in practice). The present sanctions even though had some deterrent value were regarded by most respondents as insufficient to deter fraudulent behaviour.

> When you challenge them, some of them will stop claiming for a while, they will open another account and start claiming again, mainly because there were no sanctions in the previous instance (Company 1)
>
> They don't see any negative sides to that other than they can't order with us again whereas if you did that in the store you could get put in a cell and you can get whatever repercussions from the police (Company 2)
>
> It is not effective from the point of actually stopping the behaviour, but by stopping the customer from transacting with us we are actually reducing our own losses (Company 3)

Given the results, it can be said that the combined effect of police reluctance and to some extent retail reluctance to appropriately sanction their customers (Doig and Levi, 2013; Fullerton and Punj, 2004; King et al., 2007) may be reinforcing these behaviours. A summary of the management strategies used across the three companies is reported in the table III below

Table III. Comparison of first party fraud management strategies

Conclusion and Implications

This research set out to investigate how retailers were currently managing the problem of first party fraud and how this could be improved. The fraud management lifecycle theory (Wilhelm, 2004) was used to analyse the data gathered from the collaborating companies. More broadly, this study provided insight into our understanding of the growing problem of first party fraud, existing management practices as well as presenting opportunities to build on.

This research has shown that retailers are not effectively dealing with first party fraud owing to a number of factors including: poor understanding of first-party fraud, difficulty in detecting and proving first-party fraud compared to other frauds, poor response from the police, and ineffective sanctions. When first party fraud was suspected in some cases, retailers often found it very difficult to prove conclusively.

It is evidenced from the case studies that the competitive nature of the retail sector, with its focus on customer service, mostly inhibits effective first party fraud management. Retailers want to sell as many items as possible and increase their market share and this can sometimes get in the way of crime reduction.

For the most part financial considerations were the main criteria in decisions about whether to manage first party fraud and which forms of the behaviour to prioritise over others. As one retailer rather critically noted when questioned why and whether they thought it useful to carry out risk scoring on their online orders considering that they were processing refunds in the six figure region on a weekly basis:

> It is about balancing risks and profit, but at the moment, it isn't quite profitable to go down that route. There's a lot of money involved, some customers check out multiple times, and this can be expensive (Company 2)

This retailer had decided that it was not cost-effective to manage their refund fraud losses at this stage, as it was within their risk appetite, i.e. not yet in millions. This amount is enough to make any small or medium-sized retailer go out of business.

The findings of the current study also raise important questions about how retailers are dealing with offending customers. The evidence appears to imply that retailers are largely reluctant to appropriately sanction offending customers. This, together with police reluctance in taking on first party fraud cases continues to ensure that customer fraud continues to be ingrained as a part of the culture of consumption. One retailer assumed that prosecuting their customers was going too far:

> I'm not being funny it's not about how many people you send to prison or to court but it's about recovering monies, so if they make a statement of admission we will put the value of the item back onto their account so that they owe us that money because they have the item and we will stop the account from purchasing from us until they have paid all the money or they get to a level where we might allow them to start buying again…you don't

> want to start losing money as well so it's best if you try and recover the money and keep them as a customer (Company 1).

This attitude towards first party fraud should be worrying as offenders can easily move up the fraud ladder. Retailers claimed that they have had difficulty with the police at some point when dealing with first party fraud cases; retailers face even bigger challenges in justifying police involvement with regards to first party fraud owing to the small amounts involved in this fraud. Two of the retailers noted that the police will always refer them to action fraud and nothing usually came out of it, one pointed out that the police had told them to deal with the issue as it was a commercial issue rather than a fraud issue, while another pointed out that depending on the amount the police will advise them to settle it themselves. Retailers warned that with the growth of e-commerce, first party fraud was likely to become an even greater threat, which again emphasises the importance of law enforcement keeping pace with criminal activity in e-retail in terms of investigation and sanctioning of offenders.

The findings of this study also suggest that there are many different opportunities for first party fraud in e-commerce. Indeed some of the findings demonstrate the ease of committing first party fraud, often requiring little or no sophistication. The fraud triangle is frequently used to identify the cause of crime and/or fraud (Cressey, 1973). Perceived opportunity is the result of circumstances that increases confidence in a perpetrator that they will evade detection and punishment when they commit crime. There are several factors that motivate people to commit fraud, mainly personal gain, past experience, revenge or negative attitude towards big businesses, cost-benefit consideration (perception that fraud provides more benefits than costs), peer pressure, etc. (Reynolds and Harris, 2005). Justification, the third component of the model, comprises a set of rationalisations employed be perpetrators to justify their behaviour.

Taken holistically, the findings of the study may suggest that a reluctance to appropriately punish offending customers coupled with the ease and availability of opportunities to commit first party fraud may intensify a perpetrators motivation to commit first party fraud.

The motivation behind most crime including traditional retail and e-retail crime is the same. The immediate response is the deployment of better systems but so much more can be done to prevent the behaviour in the first place. We found that retailers placed a high priority on investigating and detecting fraud, and less on deterring and punishing offenders. The importance of reinforcing positive attitudes and arousing public consciousness on the issue of first party fraud has been largely overlooked. Customer awareness programs can be used to persuade consumers to "unlearn patterns of misconduct and to strengthen moral constraints that inhibit misbehaviour." (Fullerton and Punj, 2004). With the growth of e-commerce and prevalence of this fraud, denial and assuming first party fraud as the cost of doing business is not a sound strategy, hence any applied research such as this one could be very useful for retailers. We believe that if retailers do not speak up about the problems they are facing and raise greater awareness, it may be difficult to garner enough public concern required to generate police interest in this issue.

Overall, it was found that retailers used a range of measures and processes to deal with this problem. These measures ranged from prevention, detection and mitigation, analysis, investigation, and sanctions. With regards to prevention, the retailers used a number of tools and processes to reduce the opportunities for fraudulent behaviour, such as: credit checking new applications, working with delivery companies to improve delivery accuracy using technology, use of convenience stores as collection points,

intelligence sharing with other retailers among others.

This research has shown that there are further steps retailers can take to effectively manage the problem of first party fraud. Even though all retailers agreed that they had zero tolerance for fraud, only company 1 appeared to have clear action plan to deal with the problem of first party fraud. This retailer also had good understanding of the nature and scale of most of their first party fraud losses. This action plan was born mostly when first-party fraud grew massively for this retailer, to the extent that it was a threat to their profitability. Further actions that retailers can undertake to manage first party fraud include increased staff fraud awareness training and pre-employment screening, wider intelligence sharing with retailers to reduce opportunities for fraud, measuring and monitoring first party fraud losses and putting in place adequate checks to guard against abuse of returns policies. Furthermore, we believe there is potential for the use of rule-based detection algorithms or behavioural models to improve detection and mitigation capability and provide more benefit to retailers.

The findings of this study can also help other retailers (who have little or no knowledge of how to deal with this problem) effectively manage their own first party fraud losses.

The workings of the specialist first party fraud team in Company 1 offer a useful insight into how to improve first party fraud detection methods. This company uses similar techniques to those used in the insurance industry, such as cognitive interviewing and voice-stress analysis.

Just like any other research, this research has many limitations, which need further research: First, the research findings are only based on three retailers in the UK. As a result, the researchers understand that the findings may not be representative of the whole retail domain and therefore need further investigation using empirical method

and targeting a much wider audience. However, the relevance of the findings should not be overlooked- being the first study to address this practical retail problem. Second, this study is also limited by the use of the case study method, the limited number of interviews used, non-availability of available literature and data from the companies due to confidentiality issues. Therefore, future research is encouraged using quantitative methods to test the validity of the findings across the entire retail sector.

It will be useful to find out the impact of customer awareness on changing attitudes towards this behaviour. An experiment may be carried out to test the effect of increased awareness on different samples. This may provide the needed push for retailers to consider this strategy. It will also be interesting to carry out detailed research into the reasons why consumers engage in these behaviour; targeting consumers themselves. Knowing why consumers engage in these behaviours may provide clues as to what interventions are likely to be successful. The researchers acknowledge that these are not the only dysfunctional behaviours committed against retailers, for e.g. shoplifting, etc. However, these were excluded in line with the focus of the study, the urgency of the matter (most retailers have reported not knowing how to deal with these frauds), as well as the space and time limitations of the study, hence might be considered a limitation of the current study. We suggest extending this research by conducting more case studies in other countries to learn about good practices elsewhere. An industry wide survey of practices used by other companies will also be useful in generalising the results of this study.

References

Amasiatu, C.V. and Shah, M.H. (2014), "First party fraud in e-tailing: a review of the forms and motives of fraudulent consumer behaviours in e-tailing", *International Journal of Retail and Distribution Management.* Vol. 42 No. 9, pp. 805-817

Amasiatu, C.V. and Shah. M.H. (2015) E-tailing: Strategies to reduce first party fraud, CCR Magazine, available at: www.ccrmagazine.co.uk

Amasiatu, C.V. and Shah, M.H. (2018), "First party Fraud Management: Framework For Retail Industry, doi: 10.1108/IJRDM-10-2016-0185

Bishop, T.J.F. (2004), "Preventing, Deterring and Detecting Fraud: What works and what doesn't", *Journal of Investment Compliance,* Fall 2004, pp.120-127.

British Retail Consortium (2013), "Retail crime survey 2012", available at: http://www.brc.org.uk/ePublications/BRC_Retail_Crime_Survey_2012/index.html#/4/ [cited 3 June 2013]

British Retail Consortium (2015), "Retail crime survey 2014", available at: http://www.brc.org.uk/brc_show_document.asp?id=4486&moid=8312 [cited 1 April 2015].

Brooks, G., Button, M. and Frimpong, K. (2009), "Policing fraud in the private sector: a survey of the FTSE 100 companies in the UK", *International Journal of Police Science & Management*. Vol. 11 No. 4, pp. 1-12

Bussmann, K. and Werle, M.M. (2006), "Addressing crime in companies: first findings from a global survey of economic crime", *British Journal of Criminology*. Vol. 46 No. 6, pp. 1128-1144

Button, M. and Brooks, G. (2009) ""Mind the gap", progress towards developing anti-fraud culture strategies in UK central government bodies", *Journal of Financial Crime,* Vol. 16 No. 3, pp. 229 - 244

Cressey, D. 1973 *Other People's Money: A Study in the Social Psychology of Embezzlement*. Mont-clair, NJ: Patterson Smith

Doig, A. and Levi, M. (2013), "A case of arrested development? Delivering the UK national fraud strategy within competing policing policy priorities", *Public Money and Management,* Vol. 33 No. 2, pp. 145-152

Durbin, N.R. (2007), "Building an antifraud framework", *Bank, Accounting and Finance,* Vol. 20 No. 1, pp. 43-46

Foscht, T., Ernstreiter, K., Maloles, C., Sinha, I. and Swoboda, B. (2013), "Retaining or returning? Some insights for a better understanding of return behaviour", *International Journal of Retail & Distribution Management*, Vol. 41 No. 2, pp. 113-134

FSA (2006), "Firms high-level management of fraud risk", available at: http://www.fsa.gov.uk/pubs/other/fraud_risk.pdf [Accessed 1 Septemeber 2013]

Fullerton, R.A. and Punj, G. (2004), "Repercussions of promoting an ideology of consumption: consumer misbehaviour'", *Journal of Business Research,* Vol. 57, pp.1239-1249

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

Gee, J. (2009), "Mobilising the honest majority to fight health-sector fraud", *World Health Bulletin,* Vol. 87, pp. 254-255

Harris, L.C. (2010), "Fraudulent consumer returns: exploiting retailers' return policies", *European Journal of Marketing*, Vol. 44 No. 6, pp. 730-747

Hinsz, K (2016), "First-party fraud - sifting through the noise to find and manage true risk", available at:

https://www.experian.com/blogs/insights/2016/06/first-party-fraud-sifting-through-the-noise-to-find-and-manage-true-risk/ [cited 20 February 2017]

King, T. and Dennis, C (2003), "Interviews of deshopping behaviour: an analysis of theory of planned behaviour", *International Journal of Retail and Distribution Management,* Vol. 31 No. 3, pp. 153 – 163

King, T., Dennis, C. and McHendry, J. (2007), "The management of deshopping and its effects on service: A mass market case study", *International Journal of Retail & Distribution Management*, Vol. 35 No. 9, pp. 720 – 733

NHS CFSMS (2009), "NHS CFS Performance Report 09-10", available at: http://www.nhsbsa.nhs.uk/Documents/CounterFraud/NHS_CFS_performance_report_09_10.pdf [cited 10 September 2012]

Petersen, J.A. and Kumar, V. (2009), "Are product returns a necessary evil? Antecedents and consequences", *Journal of Marketing*, Vol. 73 No. 3, pp. 35-51.

Piron, F. and Young, M. (2000), "Retail borrowing: Insights and implications on returning used merchandise", *International Journal of Retail and Distribution Management*, Vol. 28 No. 1, pp. 27-36.

Retail Fraud (2013), "The digital shoplifting survey", available at: http://www.retailfraud.com/docs/GLIT_whitepaper_002.pdf [cited 20 April 2013].

Reynolds, K. L. and Harris, L. C. (2005), "When service failure is not service failure: An exploration of the forms and motives of "illegitimate" customer complaining", *Journal of Services Marketing*, Vol. 19 No. 5, pp. 321 – 335

Rosenbaum, M.S., Kuntze, R. and Wooldridge, B.R. (2011), "Understanding unethical retail disposition practice and restraint from the consumer perspective", *Psychology & Marketing*, Vol. 28 No. 1, pp. 29-52

Schmidt, R.A., Sturrock, F., Ward, P. and Lea-Greenwood, G. (1999), "Deshopping: the art of illicit consumption", *International Journal of retail and Distribution Management*, Vol. 27 No. 8, pp. 290– 301

Wengraf, T. (2001) *Qualitative Research Interviewing.* Thousand Oaks, CA: Sage Publications Inc.

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

Yin, R. (1994) *Case Study Research: Design and Methods.* 2nd ed. Newbury Park, CA: Sage

Yin, R. (2014) *Case study design and methods*. 5th ed. Thousand Oaks, CA: Sage Publications Inc.

Table I. Description of respondents at Company 1, 2 and 3

Case Study Companies	Departments	24 Interviewees
1	Fraud Risk/Security Logistics Fraud Investigation Contact Centre	Manager (3) Manager (1) Manager (1), Investigator (1) Contact Centre staff (First level investigators) (7)
2	Loss Prevention Logistics	Manager (3) Analysts (3) Manager (1)
3	Central investigation	Investigators (4)

Table II. Comparison of first party fraud types across the three retailers (Y= present, N=absent)

Type of first party fraud	**Case company 1**	**Case company 2**	**Case company 3**
Deshopping	Y	Y	N
Refund fraud	Y	Y	Y
Fraudulent chargebacks	N	Y	Y
Misuse of facility fraud	Y	N	N
Coupon fraud	N	Y	N

Table III. Comparison of first party fraud management strategies

Approach	Company 1	Company 2	Company 3
Deterrence	No specific program aimed at deterrence. Deterrence seen as resulting from sanctions.	No specific program aimed at deterrence. Deterrence seen as resulting from sanctions.	No specific program aimed at deterrence. Deterrence seen as resulting from sanctions.
Prevention	-Fraud-proofing new concepts and systems to reduce fraud -Training staff to help prevent fraud -Staff surveillance, use of surveillance cameras in depots/warehouses -In-house automated transaction risk scoring of all orders, including use of 3-d secure authentication -Use of credit referencing agency for credit applications -Have measured their losses to first party fraud -External collaboration with few other retailers (manually)	-Fraud-proofing new concepts and systems to reduce fraud -Training staff to help prevent fraud -Staff surveillance, use of surveillance cameras in depots/warehouses -In-house automated transaction risk scoring of only general merchandise orders, including use of 3-d secure authentication -External collaboration with few other retailers (manually)	-Training staff to help prevent fraud -Staff surveillance -Automated transaction risk scoring of all orders (outsourced), including use of 3-d secure authentication -External collaboration with few other retailers (manually) -Pre-employment checks carried out on all staff

Detection	-Technology (database) used to monitor customers' claims histories - The detection of first party fraud was mostly not automated, relying on retail staff to detect and mitigate fraud losses -Deshopping usually detected by warehouse staff by visually inspecting or smelling returned merchandise - Specialist first party fraud analysts who work within the contact centre often dealt with fraudulent claims. A combination of customers' past experience and behavioural cues were used to detect and mitigate fraudulent customer claims -Suspected cases are investigated by trained staff	- The detection of first party fraud was mostly not automated, relying on retail staff to detect and mitigate fraud losses -Past behaviour used to predict fraudulent intent -Technology (database) used to collect data on customer returns which assisted generalist fraud teams in the detection and mitigation of fraudulent customer claims -Suspected cases are investigated by trained staff	- The detection of first party fraud was mostly not automated, relying on retail staff to detect and mitigate fraud losses -Past behaviour used to predict fraudulent intent -Technology used to collect data to assist in detection -Detection carried out mainly by generalist fraud team

Mitigation	Detection and Mitigation of deshopping usually carried out by warehouse staff who visually inspect and reject returned items where fraudulent activity was suspected - Specialist first party fraud analysts who work within the contact centre often dealt with fraudulent claims. A combination of customers' past experience and behavioural cues were used to detect and mitigate fraudulent customer claims Internal communication and collaboration between the fraud team and other departments in managing first party fraud losses, e.g. suspending suspicious accounts or stepping up security when packing and delivering items from suspicious accounts	Detection and Mitigation of deshopping usually carried out by warehouse staff who visually inspect and reject returned items where fraudulent activity was suspected Fraudulent customer claims handled by generalist fraud team whose major remit was on managing third party fraudulent cases	Mitigation of deshopping usually carried out by warehouse staff who visually inspect and reject returned items where fraudulent activity was suspected Fraudulent customer claims handled by generalist fraud team whose major remit was on managing third party fraudulent cases
Investigation	-Referrals are logged and individual investigator performance is assessed (number of referrals investigated) -First party fraud cases were usually investigated by specialist contact centre trace advisers -Senior loss prevention managers were sometimes accompanied by	-Investigations were mainly carried out by more generalist fraud and loss prevention team -Senior loss prevention managers were sometimes accompanied by police	-Investigations conducted by the fraud team but no house visits carried out

	police to customers' homes to interrogate serial offenders	to customers' homes to interrogate serial offenders	
Analysis	-Effective arrangements in place for collating and analyzing first party fraud losses -Dedicated working group led by senior risk managers and including representatives from the main business units and support areas meet monthly. -Detailed assessment of first party fraud losses as well as gap analysis of controls in place are discussed - Detailed analysis of successful first party fraud cases are used to update existing policies	-Detailed analysis of large-scale first party fraud losses are carried out and corrective actions put in place	-Analysis of successful first party fraud cases - Detailed analysis of successful first party fraud cases are used to update existing policies
Prosecution	-Prosecution was rarely pursued with respect with first party fraud - Retailer also rarely pursued any civil litigation cases. Fraudulent claims are rejected and offending customers asked to pay what they owe. In extreme cases, usually where there was evidence of re-offending customers could be temporarily suspended; prosecution rarely if ever sought	-Retailer's policy is to block serial offenders from purchasing with the retailer; prosecution was rarely sought -Prosecution depended on the weight of evidence, associated amount of loss, and police willingness to accept case but this	- Retailer's policy is to block serial offenders from purchasing with the retailer;

	-The level of sanction applied depended on the amount of loss and frequency of behaviour	was rarely, if ever, pursued.	