First Party fraud management: A framework for the retails industry

Shah, M & Amasiatu, CV

Original citation & hyperlink:
Shah, M & Amasiatu, CV 2018, 'First Party fraud management: A framework for the retails industry' *International Journal of Retail & Distribution Management*, vol 46, no. 4, pp. 350 - 363
https://dx.doi.org/10.1108/IJRDM-10-2016-0185

DOI 10.1108/IJRDM-10-2016-0185
ESSN 0959-0552

Publisher: Sage

First Party Fraud Management: Framework for the Retail Industry

Abstract

Purpose - First Party fraud in which consumers commit fraud against retailers is a growing problem. Research in this area is very limited which means that there is almost no guidance available to mitigate this problem. Existing fraud management frameworks focus on the management of other fraud, such as identity theft or employee instigated fraud. Due to the different nature of these frauds, these frameworks do not adequately address first party fraud. Therefore we propose an adapted version of the framework which is specific to first party fraud management.

Design/methodology/approach - We conducted a systematic literature review and compared/contrasted a number of existing fraud management frameworks in related domains, and found Wilhelm's fraud management framework the most promising for adaptation and application to the first party fraud context. By modifying an existing framework according to the contextual requirements, we make the framework much more relevant to first party fraud management.

Practical implications - Our framework could help retail managers better understand and manage this growing business problem and open new streams for further research.

Originality/value - This research also makes an important contribution by proposing a framework and by helping bridge a glaring and problematic gap in existing literature and opening up new streams of research.

Keywords Fraud, e-fraud, first party fraud, consumer behaviour, framework,
holistic, retailing, retail industry

Paper type Systematic Literature Review

Introduction

The amount of losses online retail organisations suffer annually to fraud has resulted in growing attention being devoted to the management of fraud risks in organisations. Consequently, this has increased research interests in organisational ethical decision-making, organisational or workplace fraud and the preventive frameworks for such frauds (Ferrell et al., 2008; Malgwi and Rakovski, 2009; Murphy and Dacin, 2011). Although an increasing level of attention is being devoted to understanding consumer misbehaviours and/or first party frauds (Abdelhadi et al., 2014; Fullerton and Punj, 2004; Harris and Reynolds, 2004; King and Dennis, 2006; Rosenbaum et al., 2011), relatively little has been documented in literature in terms of how to manage such problems.

There is no legal definition of first party fraud as of yet. For the purpose of this research, we used the definition of (CIFAS, 2012) which states, "first party fraud as fraud committed by a customer that does not involve the use of stolen identity or third party involvement". Individuals commit such acts to obtain goods/services or to evade payment for goods/services. Within the context of exchange, consumers behave in fraudulent ways when they go against their contractual agreement and behave in ways that solely benefits them whilst resulting in a loss to their exchange partner (retailer). Expectations of behaviour are formed through rules, laws or regulations (Moschis and Cox, 1989) that regulate the exchange process. The basic rule of exchange assumes that successful exchanges are 'goal-oriented dyadic interactions' (Solomon et al., 1985) between two or more partners in which one partner (consumer) transfers cash in exchange for products/services from another partner (seller/retailer). However, recent findings suggest that this is not always the case (King and Dennis, 2003, 2006; Piron and Young, 2000; Schmidt et al., 1999; Rosenbaum et al., 2011), as consumers sometimes feign exchanges at the expense of retailers. The most common forms of first party fraud in the retail industry are: deshopping or return of used merchandise, chargeback or friendly fraud, bust out fraud, and misrepresentation of details (Amasiatu and Shah, 2014, 2015).

The prevalence of this type of fraud is startling. For example, King et al. (2007) indicated that up to 50% of returned merchandise with a mass market retailer was fraudulent with an estimated cost in the six-figure region, while Harris (2010) reported that 92 percent of their sample admitted to fraudulently returning goods after using or damaging them. Harris (2008, 2010) further identified ten facilitators of fraudulent returning, amongst them including past experience of successful fraudulent returns, positive attitude towards fraudulent returning and consumer awareness of retailers' liberal return policies, and argued that the relative ease of perpetrating first party fraud has led to the increasing societal acceptance of such frauds.

Many frauds are now carried out online. More recently, cyberspace fraud has aroused interest in the research community, with some scholars noting that online retailing may provide a potential promising avenue for the continued perpetuation and growth of first party fraud (Hjort and Lantz, 2012). The convenient and anonymous nature of the internet coupled with the availability of opportunities for misbehaviour online makes fraudulent behaviours much more attractive, making it easier for consumers to misbehave without any resultant negative affect (Reynolds and Harris, 2005). For example, it has been revealed that fraudulent chargebacks by customers is the second most costly fraud retailers face (LexisNexis, 2012), accounting for 41 percent of all fraud losses by US and Canadian retailers, estimated at $1.4 billion (CyberSource Corporation, 2012). Furthermore, a recent survey of British retailers found that over 90 percent regard online fraudulent consumer behaviour a growing threat to their businesses (Retail Fraud, 2013).

With online retailing representing the fastest growing retail distribution channel in Europe (Centre for Retail Research, 2014), first party fraud may become an even bigger challenge for businesses. However, despite evidence of the prevalence of first party fraud, no previous research has examined or developed a framework that retailers can use to manage/mitigate incidents of such behaviours. This paper is therefore an attempt to address this gap in existing research.

More recently, researchers have begun to highlight the importance of approaching fraud management from a holistic perspective. For example, Furlan and Bajec (2008) and Bishop (2004) argue that most fraud management/prevention literature has typically focused on fraud detection methods rather than the full activities in an anti-fraud framework. Bishop (2004) emphasised that whilst detection is a crucial activity in an anti-fraud framework, excessive focus on detection activities can be unprofitable for organisations as much of lost funds do not end up being recovered. This view is consistent with many other researchers, such as Durbin (2007) and Wilhelm (2004), who pointed out that superior fraud loss performance can be attained by adopting a holistic approach to fraud management and successfully integrating and balancing the activities in an anti-fraud framework (Durbin, 2007; Bishop, 2004; Wilhelm, 2004). Wilhelm (2004) and McGinley and McCall (2009) further make the case for an anti-fraud framework, arguing that fraud continues to be a growing problem for businesses despite technological advances in fraud detection. The answer, they argue, lies in an anti-fraud framework.

The aim of this research is to propose a framework that retailers can use to manage first party fraud. The large amounts lost to first party fraud and the absence of a framework in literature to manage first party fraud provides sufficient motivation for this study. Such a framework could help retailers protect their bottom lines and provide a competitive advantage in pricing for (e) retailers, rather than increasing merchandise prices to cover the losses. Using an anti-fraud framework can significantly limit fraud losses, maintain investor confidence by protecting an organisation's bottom line and protect an organisation's reputation (Durbin, 2007). Our framework, which is an extension of the existing fraud management lifecycle theory, should help retailers better understand and manage this growing business problem.

Our paper is organised as follows: first, we explain our methodological construct. Next, we review existing fraud management frameworks, and then finally, we discuss the extended framework, conclusion and future research agenda.

Methodology

The research approach adopted is a systematic review of literature. Literature search was conducted on the following databases: Business Source Premier/EBSCOhost, IEEE Digital Library, Scopus, ScienceDirect, Web of Science and Google Scholar. Our search strings consisted of the following:

1 fraud AND management AND framework
2 fraud AND holistic AND framework
3 fraud AND prevention AND framework
4 fraud AND prevention AND management
5 customer misbehaviour AND retail
6 dysfunctional customer behaviour AND retail
7 consumer fraud AND retail
8 first party fraud AND retail
9 fraudulent customer returns OR deshopping AND retail

We ensured the relevance of the articles by requiring that the fraud management articles contain at least one of the following words: 'identity fraud', 'e-fraud', 'mobile fraud', and used related words, e.g. customer/consumer to ensure relevant articles were captured. For the customer fraud literature, we ensured articles contained at least one of the following words or synonyms:

‘retail borrowing’, ‘unethical retail disposition’, ‘fraudulent returns’, ‘fraudulent consumer behaviour’ and ‘customer fraud’.

In addition, we scanned reference lists of articles, and other articles deemed to be relevant were also included. This helped in ensuring coverage of the most relevant papers. Articles that bore no relevance to the research objectives were excluded. For the fraud management literature, we excluded all articles that did not describe fraud management from a holistic view: this included articles that addressed technological solutions in one area of fraud management. We also excluded materials that did not relate to first party fraud or address any of its forms in retailing. This included articles that related only to computer-related frauds such as phishing etc, customer theft, customer rage, physical store violence, sexual harassment of employees by customers, or articles that solely related to forms of consumer misbehaviour in other industries such as tourism and hospitality.

We carefully read the article abstracts bearing in mind our inclusion and exclusion criteria, and 44 publications were found and reviewed. Of the 44 publications found, 9 publications related to fraud management in general, with 5 articles on anti-fraud frameworks. The remaining 35 publications addressed customer fraud or misbehaviour.

Fraud Management Frameworks

Here, we evaluated some fraud management frameworks from the literature to see which one would be most suitable for first party fraud management.

Furlan and Bajec (2008) Framework

Furlan and Bajec (2008) proposed a framework for health insurance fraud. Their research focused on five main concepts: process, activity, activity goal, fraud management system and fraud management system characteristic (see fig 1 below). Six fraud management activities were identified: Deterrence, Prevention, Detection, Investigation, Sanction & Redress and Monitoring.

According to the authors, deterrence of fraud starts with reducing the probability of fraud occurring by removing the elements of the fraud triangle. Next, the organisation should detect fraudulent claims early before losses are incurred. The deployment of effective fraud detection techniques should help uncover suspicious claims for investigation and sanction. Finally, constant monitoring of fraud management activities should help an organisation to continually assess and improve its counter-fraud strategy.

Furlan and Bajec (2008) claim that every fraud management activity is part of one or more business process, and that these activities have goals. There are two business processes; the first process is curative and is concerned with detecting fraud once it occurs. The activities performed within this process include detection, investigation and sanctioning. The second process is preventive and is concerned with stopping fraud from happening. The activities performed within this process include early detection, investigation, prevention and sanctioning. The authors also suggest that there are two ongoing activities: deterrence and monitoring. Deterrence decreases fraud and therefore contributes to the fraud detection activity. Whereas, monitoring focuses on assessing the efficiency of the core fraud management processes (see fig 2 below).

Furlan and Bajec (2008) identified different fraud management system/information system characteristics that enable effective and efficient support to the fraud management activities, although they noted that the system characteristics may vary across domains. The authors, however, offered no clear distinction between prevention and detection activities. Instead, they refer to 'prevention' as early detection and 'detection' as the detection of successful frauds.

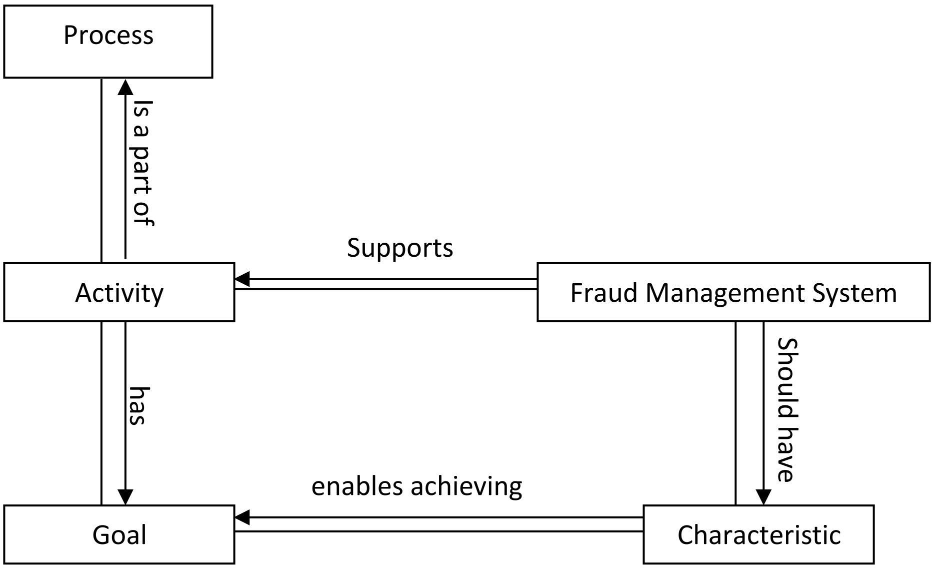
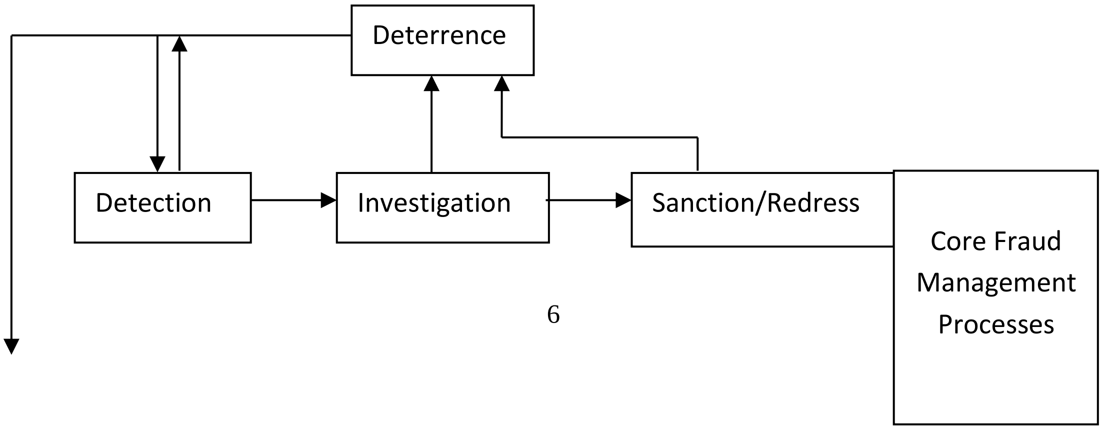


Fig 1: Furlan and Bajec (2008) research concept



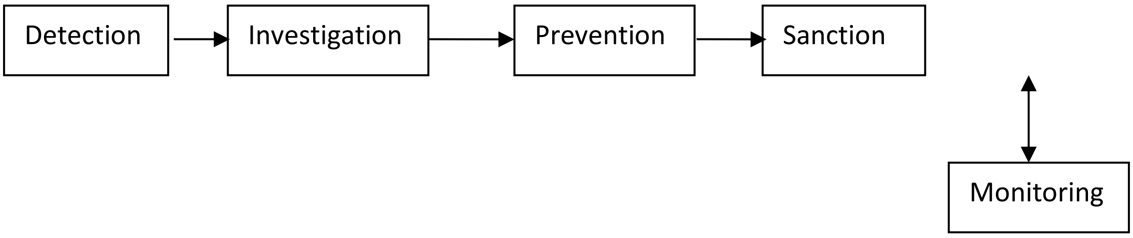


Fig 2: Fraud management activities and their relations (Furlan and Bajec (2008)

Fraud Management Lifecycle Theory by Wilhelm (2004)

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 3 below). Deterrence activities are those intended to discourage attempts at fraud. Prevention stage activities are those intended to prevent fraud from occurring or to secure an organisation against fraud. Deploying protective systems, processes and procedures that make fraud harder to commit is crucial in preventing fraud. Detection stage activities are those focused on uncovering the presence of fraud. Mitigation stage activities are those intended to reduce the extent and the amount of the associated fraud losses. The analysis stage includes performing two basic functions: identify and understand fraud losses that occur despite deterrence, prevention, detection and mitigation stage activities along with monitoring the performance of each of the other stages of the fraud management lifecycle. Policy stage activities are those intended to create and/or modify existing fraud policies to reduce the occurrence of fraud. The focus of Investigation is to gather enough evidence to stop fraudulent activity and to assist in offender prosecution/restitution, while Prosecution activity is focused on undertaking legal action against offenders.

Wilhelm (2004) subsequently applied this framework to four different industries and found the existence of all eight framework components in the industries. The author further suggests the importance of balancing the framework components, i.e. the correct allocation of resources to ensure coordinated and effective fraud response.

Wilhelm (2004) suggests that interactions between the different components do not necessarily occur in a sequential manner; rather the different components interact with each other giving rise to a web of interactions, in a network-like manner. Finally, Wilhelm (2004) argues that successful integration of Information Technology facilitates these linkages, interactions and interrelationships between the framework’s components. These interactions and interrelationships between the framework’s components ensure that the framework is flexible and adaptable.

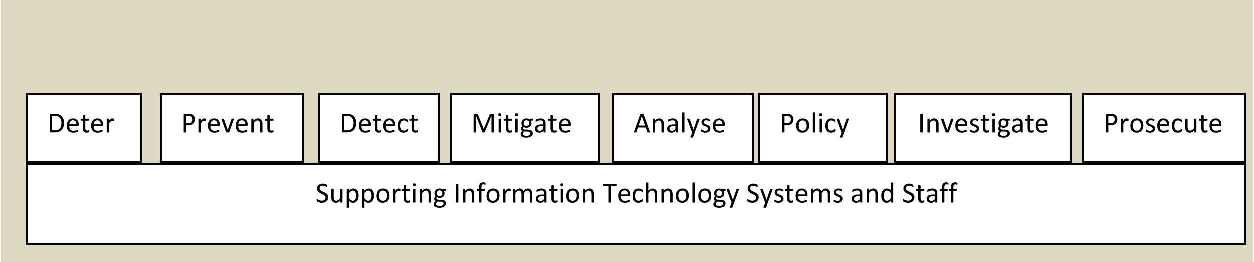
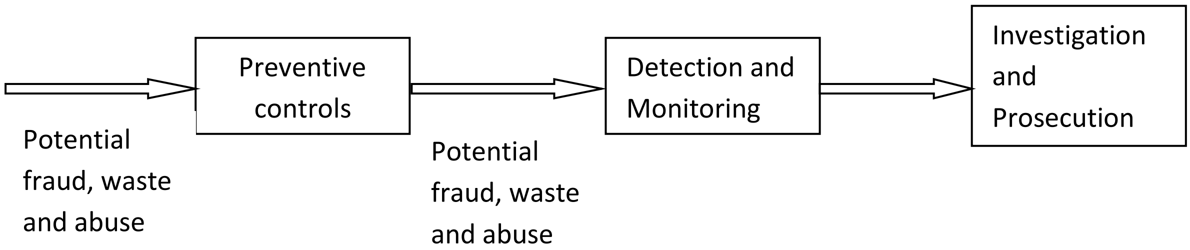


Fig 3: Linear Representation of the Fraud Management Lifecycle Theory
Source: Wilhelm (2004)

US Government Accountability Office (GAO) Framework by Kutz (2006) and Ghosh (2010) anti-ID Fraud Framework

The US Government Accountability Office Framework developed the framework for fraud prevention, detection and prosecution to minimise fraud, waste and abuse in disaster assistance programs such as the Huricane Katrina and Rita disaster relief program (Kutz, 2006). According to the framework (see figure 4), a well-designed fraud management strategy consists of 3 crucial elements: prevention, detection & monitoring, and investigations & prosecutions. The framework also suggests that weaknesses identified through detection and monitoring should be used to make improvements to the first stage of the framework - prevention. Ghosh (2010) proposed a 4-component framework (see figure 5) similar to that by the GAO, with the exception of ‘~~sanction ‘~~prosection’ and ‘monitoring’ activities. However, the Ghosh framework (2010) provides an additional component - ‘solve’ which is not in the GAO framework. The components are: Prevent, Detect, Investigate and Solve. ‘Solve’ refers to identifying a ‘fingerprint’ (historical behaviour patterns) based on past and present behaviour which can be used to predict future behaviour and to trace known fraud chains. ~~We have not chosen these frameworks because they did not meet three of our criteria: functionality, comprehensiveness and adaptability.~~


Preventive controls
Detection and Monitoring
Investigation and Prosecution
Potential fraud, waste and abuse
Potential fraud, waste and abuse

Potential
fraud, waste
and abuse

Fig 4: Framework for Prevention, Detection and Prosecution (Kutz, 2006)

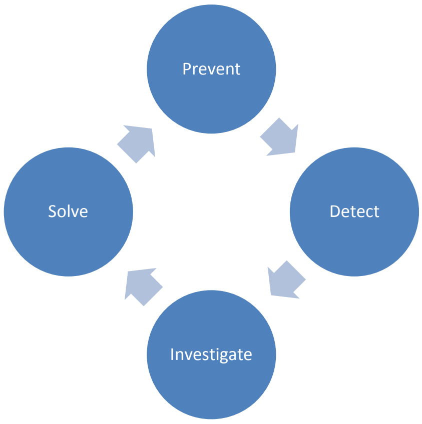
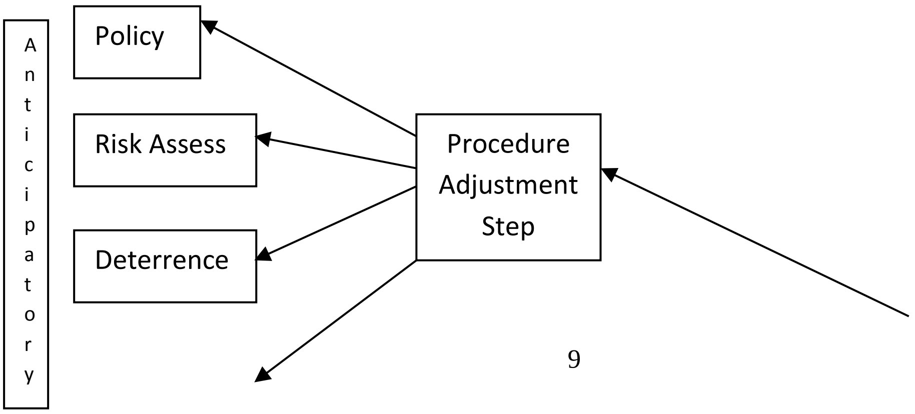


Fig 5: Anti-ID Fraud Framework (Ghosh, 2010)

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

Jamieson et al. (2007) proposed an identity fraud enterprise management framework from an organisational perspective, derived from a review of existing frameworks (see figure 6). Their framework consists of three main phases in fraud management: anticipatory, reactionary and remediation. The phases in turn consist of 13 sequential stages (policy, risk assessment, deterrence, prevention, detection, mitigation, analysis, incident management, review, investigation, prosecution, recovery and restoration). Each of the three phases in turn have both a learning step and procedure adjustment step. Jamieson et al. (2007) claimed that the purpose is to introduce innovations into the framework. ~~Although a comprehensive framework, the separation of phases and stages make the framework more suitable for implementation in bigger organisations; thereby limiting its adaptability. For this reason of complexity and limited adaptability, we have not chosen this framework.~~



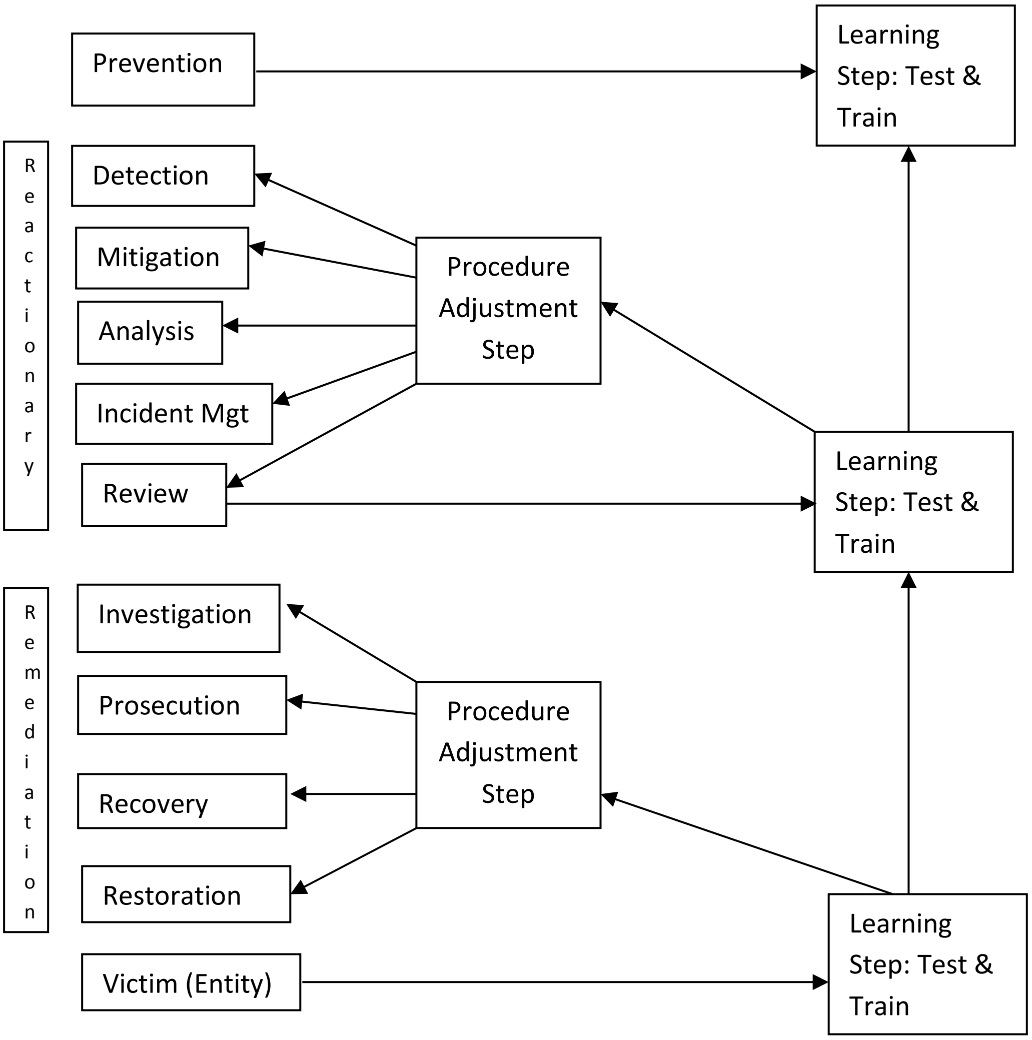


Fig 6: Identity fraud enterprise management framework (Source: Jamieson et al., 2007)

Framework Comparisons

The frameworks discussed above are summarised in the table ~~2~~ 1 below. It is clear that the frameworks share some similarities as well as differences. For example, all the frameworks reviewed feature 'prevent', 'detect' and 'investigate' components. Similarly, the 'sanction/prosecute' component features in all the frameworks apart from the Ghosh (2010) framework. The Furlan and Bajec (2008), Jamieson et al. (2007) and Wilhelm (2004) frameworks share the most similarities. However, some differences exist. For example, Furlan and Bajec (2008) specifically name a ‘monitoring’ component, while Wilhelm’s (2004) and Jamieson et al. (2007) include monitoring within the ‘analysis’ and ‘review’ stages respectively. Similarly, the ‘mitigation’ stage activity in Wilhelm’s (2004) and Jamieson et al’s (2007) frameworks are performed within the ‘detection’ stage activity in Furlan and Bajec’s (2008) framework. One possible reason for the differences could be because the frameworks were developed to manage different types of frauds and therefore reflect the nature of fraud that they manage.

Bearing in mind the aim of our research which is to ‘find a fraud management framework which can be adapted and applied in the retail context for the management of first party fraud’, we developed the following evaluation criteria:

1. **It must be functional.** In other words, it should be capable of functioning/fulfilling its objective.
2. **It must be adaptable.** In other words, it should be flexible and able to be modified for a new purpose.
3. **It must be comprehensive (but not complex), covering many stages of fraud management**. In other words, the framework should incorporate different components. Researchers, such as Furlan and Bajec, (2008) and Bishop, (2004) observe that a holistic fraud management framework involves many activities
4. **It must emphasise ongoing improvement:** In other words, performance monitoring and evaluation of the anti-fraud program (as a way of driving improvement) is crucial (Bishop, 2004; Furlan and Bajec, 2008; Pergola and Sprung, 2005).
5. **It must be empirically derived**
6. **Each of the components should have a clear focus**: In other words, it should distinguish between prevention, deterrence and detection. This is because these activities are sometimes used synonymously and can contribute to confusion within an organisation as to the focus of each of the activities. This point of view has also been supported by Wilhelm (2004).

Table 1 below shows a comparison of these frameworks using our evaluation criteria. We found that the fraud management lifecycle theory by Wilhelm (2004) provides a promising framework for first party fraud management in (e) retailing with some modifications.

Although Furlan and Bajec's (2008) framework met four of our six evaluation criteria, it was not chosen because it makes no distinction between prevention and detection stage activities, which to many other researchers (Wilhelm, 2004; Ghosh, 2010, Kutz, 2006) are clearly distinct components. In addition, this framework was only applied in the health sector, and so it is difficult to determine if it can be successfully applied to other sectors and other fraud types. On the other hand, Jamieson et al.'s (2007) framework, though comprehensive, was not chosen due to its complexity and limited adaptability. The separation of phases and stages increases the complexity of this framework, and the sequential nature of the stages may make the framework less adaptable to different sectors/work environments and fraud problems. Having a framework that is easily adaptable to different fraud challenges is key to managing fraud. Due to the complexity and adaptability issues, this framework was not chosen.

The other frameworks by Kutz (2006) and Ghosh (2010) were also not chosen because they did not meet three of our evaluation criteria: functionality, comprehensiveness and adaptability. These two frameworks were the least comprehensive of all the frameworks, although this may be because of the focus of the frauds and sectors in the studies. However, the absence of deterrence (a vital fraud management component) was in the authors' opinion a serious limitation of the frameworks for this study. Without any deterrence effort, organisations expose themselves to unnecessary fraud losses and run the risk of fire fighting fraud, which is not cost effective (Wilhelm, 2004). Ultimately, the importance of a fraud management framework lies in its applicability in different work environments and sectors; due to the limited scope and depth of the participating sectors/companies in the above mentioned four frameworks, they were not chosen. In contrast, our chosen framework by Wilhelm (2004) is comprehensive, functional, adaptable, and has been applied in different industries. It has also shown to result in significant fraud loss reduction.

<Insert Table One: A comparison of different fraud frameworks>

First Party Fraud Management Framework

Our proposed model (Figure 7 below) which is an extension of the fraud management lifecycle theory consists of 7 elements: Deterrence, Prevention, Detection, Investigation, Sanction and Redress, ~~Analysis~~ Measuring and Monitoring, and Policy. The components can, but do not necessarily, occur in a sequential manner. We briefly describe the framework stages below:

Deterrence

The importance of deterence has been highlighted in the literature as key to implementing successful anti-fraud programs (Wilhelm, 2004; Furlan and Bajec, 2008), and this is likely to be the same for first party fraud. The opportunistic nature of frauds, the cost of investigation, and the underlying motivations for engaging in them make deterrence a vital step in any anti-fraud framework, and the first step/component in our first party management framework. From the fraud triangle, there are three fraud risk factors or conditions: perceived pressure/motivation, perceived opportunity and rationalisation (Cressey, 1971). The presence of these elements in first party fraud is demonstrated below:

- Motives/Pressure: first party fraud is opportunistic in nature. Some research suggest that consumers who engage in first party fraud often cite a number of motives/reasons for engaging in the behaviour, such as: economic distress, low self-esteem (deshopping expensive clothing to support their need for acceptance), revenge motives (stemming from negative attitude towards larger businesses), anomie, differential association/peer influence, etc. (Reynolds and Harris, 2005; Rosenbaum et al., 2011; King and Dennis, 2006).
- Opportunity: the availability of opportunities for fraud, ease of committing first party fraud, low likelihood of detection, and little or no consequences for commiting first party fraud has been reported to be driving this behaviour (King and Dennis, 2003, 2006).
- Rationalisation: first party fraud offenders use rationalisation to either argue that their behaviour does not hurt anyone (and is therefore excusable), that their victim/retailer deserves the wrongdoing, or that circumstantial pressures outside their control led to their behaviour (Harris and daunt, 2011; Rosenbaum et al., 2011).

Some of the elements of the triangle such as differential association, revenge motives against larger business and presence of opportunities can be controlled (by (e) retailers) through public awareness and reduction of opportunities. For example, Fullerton and Punj, (2004) pointed out that “The educational approach uses promotional messages to persuade consumers to unlearn patterns of misconduct and to strengthen moral constraints which inhibit misbehaviour”. The benefits of public awareness about this fraud are as follows: firstly, educational campaigns targeting mainstream consumers can be used to increase social disapproval of the behaviour and alter/thwart some of the rationalisations employed by offenders to justify the behaviour. For example, denial of injury rationalisation can be thwarted by stressing the costs of such behaviour. Secondly, promotional messages can be used to communicate to the public that retailers are ethical and just organisations, as a way to thwart denial of victim (particularly those against big business committed solely for revenge). Thirdly, education can be used to communicate the disincentives and consequences of committing fraud (Cuganesan and Lacey, 2003) as well as the direct and indirect costs of fraud to both retailers and the public. The propensity to engage in fraud or crime increases when an individual's perception of the rewards of their behaviour outweighs the costs or consequences of that behaviour.

Some studies suggest that the recovery rate of fraud losses is very low (Wilhelm, 2004), and so deterring fraud from happening in the first instance should be a vital first step in managing fraud.

Prevention

The next step after deterrence has failed is to prevent fraud from occurring. ~~Prevention means~~ The activities in this stage are focused on~~-~~ preventing fraud from occurring or making fraud harder to commit, when attempted. Prevention activities directly address the opportunities that aid first party fraud. Technology plays an important role in prevention, i.e. use of address verification, credit checks, and 3-D secure authentication could make first party fraud harder to commit (Amasiatu and Shah, 2014).

The importance of promoting zero tolerance to fraud in the workplace as a key preventive measure is highlighted by Button and Brooks, (2009) and Brooks et al. (2009), who concluded that training and screening employees should be an integral part of prevention.

Staff involvement in first party fraud can present opportunities which consumers may exploit, for example, the potential for delivery men to steal parcels. It is therefore imperative that employee involvement is limited in order to minimise the opportunities for fraud. Activities to undertake in this stage may include performing background/criminal checks on employees working in areas such as delivery, warehouse, etc., to reduce the possibility of employee involvement in first party fraud. Employees should also receive training on the organisations' code of conduct and agree to comply with such standards of behaviour. Fraud awareness training should also be provided to employees specific to their duties. For example, training given to delivery personnel should alert them that their employer will not tolerate such behaviour. On the other hand, contact centre and investigating analysts should also receive training on red flags and how to detect fraudulent behaviours or opportunistic customer claims.

Detection

Detection stage activity is concerned with identifying the presence of fraud. The very nature of retailing is centred on improving customer experience, and sometimes this may come in the way of fraud prevention (Amasiatu and Shah, 2014, 2015). Employees have a role to play in detecting fraud as claims are normally received by frontline staff, so their ability to detect and stop fraudulent behaviour from continuing is crucial at this stage. Wilhelm (2004) separates these two activities into detection and mitigation stage activities; however, in the case of first party fraud, these activities can be undertaken within the same stage. For example, in the case of the return of used merchandise, returns can be denied by staff if suspected to be fraudulent or used. Information systems can support this activity by providing information to assist front line claims staff in detecting fraudulent behaviour and/or opportunistic attempts. Some researchers, such as Speights and Hilinski (2005) suggest the use of technology to track consumer return behaviour and subsequently use this to deny returns. Such a system can also be used to monitor customer claims. The authors further add that retailers can use such a system to analyse the impact of changes on the consumer, protect against fraud and abuse, and alter return policies (Speights and Hilinski, 2005). Most importantly, intelligence sharing between retailers may be vital in detecting and mitigating serial cross-organisational abuse. This has been used for the management of other fraud problems, i.e. insurance frauds.

Investigation

When suspicious behaviour has been detected, ~~investigators investigate it~~ it should be investigated to determine if it is fraudulent or not. Investigation stage activities obtain sufficient evidence to stop first party fraud and to provide support for offender sanctioning and redress. When a suspicious claim has been forwarded to an investigator, the investigators' duty is to investigate it and determine if it is fraudulent or not. Maintaining an effective relationship with law enforcement is also important. Rigorous investigations which culminate in the prosecution or sanction of fraudsters can have a deterrent effect on future behaviour. Information technology can support this stage (as well as the other framework stages) by helping manage large volumes of data and enabling investigators to spot anomalies (Furlan and Bajec, 2008).

Sanction and redress

Environmental factors (regulatory environment and the society) have an impact on fraud management (Wilhelm, 2004), and this is also true with first party fraud. In the UK, fraud is often not a police priority (Brooks et al., 2009), and first party fraud is hardly considered criminal enough for prosecution by both the public and law enforcement officials (King and Dennis, 2003), hence the need to go through the civil recovery process. Although studies suggest that retailers largely ignore these losses and often do not punish offenders (Amasiatu and Shah, 2014; King and Dennis, 2003; King et al., 2007), we argue that retailers should do more to punish offenders and obtain restitution, as a deterrent. Rather than viewing these frauds as the cost of doing business, retailers should pursue approaches such as rejecting fraudulent claims, rejecting further purchases from fraudulent offenders/accounts, as well as maintaining a closer working relationship with law enforcement officials to punish offenders and reclaim lost funds. Sanctioning and redress is a different from prosecution, in that successful prosecution does not always result in reimbursement of funds (Furlan and Bajec, 2008). Given the current landscape, we use 'sanction and redress' in our adapted framework.

Measurement and monitoring

Effective measurement and monitoring is crucial in an anti-fraud framework. Effective measurement and monitoring helps determine or assess if counter fraud efforts are meeting their ultimate objective of reducing fraud (Furlan and Bajec, 2008). The activities undertaken at this stage should involve: monitoring the performance of the other stages of the framework, understanding first party fraud losses and ongoing measurement and monitoring of first party fraud. Feedback from these assessments can be used to inform the implementation or improvement of fraud detection and prevention activities, deploy policies to address identified loopholes, as well as improve the other framework stages. Regular fraud monitoring is important because it can help an organisation quantify the benefits of an anti-fraud framework, hence it might be a better way of justifying anti-fraud investment. For example, McGinley and McCall (2009) suggest that 'quantifying the benefits of an anti-fraud strategy requires tracking metrics over time' (McGinley and McCall, 2009, p. 3). As first party frauds are under-reported and currently not receiving enough interest from businesses (Amasiatu and Shah, 2014, 2015), ongoing measurement and monitoring can help retailers better assess the performance of their overall counter-fraud strategy.

Policy

Having a comprehensive policy is key to managing fraud. Policy stage activities are focused on the creation, modification and deployment of policies to reduce first party fraud. Performance feedback from the monitoring stage is used at this stage to improve the overall anti-fraud framework. For example, performance feedback highlighting process weaknesses can be addressed by deploying/modifying policies to address identified loopholes/weaknesses. Policy stage activities are most frequently undertaken by managers.

Discussion

Although first party fraud is a growing problem in the retail sector, research in this area is still very limited, which means there is little or no guidance available for managing such problems. Our framework should help (e) retailers, many of which currently regard this frauds as a cost of doing business, manage the growing incidence of first party fraud.

Our proposed framework extends Wilhelm's (2004) framework within the domain of first party fraud management in the retail context. We chose the fraud management lifecycle theory by Wilhelm (2004) because it is comprehensive, adaptable and is functional across various industries. We further extend this framework by adapting and applying it in a different industry (retail) and context (first party fraud). The proposed framework in this paper extends the fraud management lifecycle theory not only by interpreting the framework stages in the context of retail first party fraud management, but also by the addition of the 'Sanction and redress' stage to the framework.

Raising public consciousness of the consequences of first party fraud as a deterrent measure, prevention and detection of first party frauds once deterrence has failed, investigating and sanctioning perpetrators, measuring and monitoring first party losses and the deployment or modification of policies that make first party fraud difficult to commit (Fullerton and Punj, 2004; Speights and Hilinski, 2005; King and Dennis, 2003; Wilhelm, 2004; Furlan and Bajec, 2008) should help retailers better manage their first party fraud losses.

Senior management support has been identified as key to implementing successful anti-fraud programs, and managing first party fraud is no exception (Button and Brooks, 2009; Wilhelm, 2004). Rather than viewing these frauds as the cost of doing business, the framework in this study presents a guide to help retailers devise plans for dealing with this problem. With the growth in e-commerce (making it much more difficult to detect fraudulent behaviour), we anticipate that first party problem will become an even greater threat to retail profitability if not adequately managed.

We argue particularly for the importance of deterrence as a vital component of the framework. Given the growing societal acceptance of these frauds and the lack of interest by law enforcement officials, we believe that retailers should do more to speak up and raise greater awareness of this problem, else it may be difficult to garner adequate public concern to increase social disapproval and generate interest within the law enforcement community.

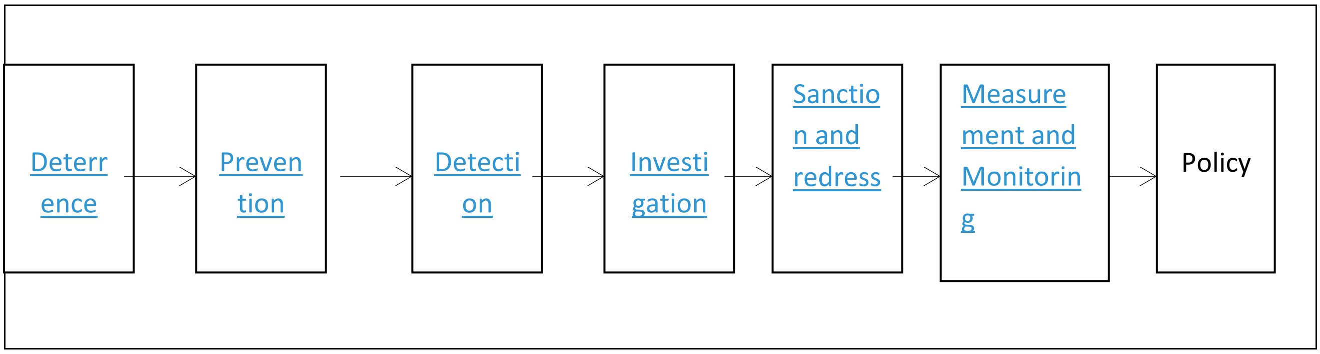


Fig 7: Framework of first party fraud management

Conclusion

Growing evidence of the frequency of first party fraud has driven the need for a fraud management framework. We reviewed five fraud management frameworks: Furlan and Bajec's (2008) framework, fraud management lifecycle theory (Wilhelm, 2004), US Government Accountability Office (GAO) framework (Kutz, 2006), Anti-ID fraud framework (Ghosh, 2010) and Identity fraud enterprise management framework (Jamieson et al., 2007). We chose and found the fraud management lifecycle theory (Wilhelm, 2004) suitable for adaptation and application to the first party fraud management context. The purpose of the framework is to address the gap in the literature on first party fraud by proposing an adapted first party fraud management framework. As with all frauds, we acknowledge that it will be difficult to completely eliminate first party fraud. However, our framework should help retail managers to better manage the prevalence of first party fraud. By extending the existing fraud management lifecycle theory, we make it more relevant to the first party fraud context. Our extended fraud management framework consists of 7 activities: Deterrence, Prevention, Detection, Investigation, Sanction and Redress, Measurement and Monitoring and Policy.

We acknowledge that our adapted framework is theoretical in nature and it would be premature to claim its applicability or usefulness in practice without testing it empirically. We propose that this framework should be tested using both quantitative (to test the gernal applicability) and qualitative (to know the depth of different aspects of framework in practice) methods.

References

Abdelhadi, A., Foster, C., Whysall, P. and Rawwas, M. (2014), "Attitudes towards shoplifting: A preliminary cross-cultural study of consumers", *Management Studies,* Vol. 2 No. 6, pp. 373-380

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 –etailing", *International Journal of Retail & Distribution Management*, Vol 42 Issue 9.

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

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.

Centre for Retail Research (2014), available at: http://www.retailresearch.org/onlineretailing.php (accessed 1/6/2014).

CIFAS (2012), "Fraudscape: Depicting the UK's fraud landscape", available at: http://www.cifas.org.uk/secure/contentPORT/uploads/documents/reports/Confidential-%20Fraudscape%202011.pdf (accessed 29 March 2012).

Cressey, D.R. (1971), *Other people's money: A study in the social psychology of embezzlement*. Glencoe: Free Press

Cuganesan, S. And Lacey, D. (2003), "Identity fraud in Australia: An evaluation of its nature, cost and extent", *Standards Australia International Limited*, Sydney.

Cybersource Corporation (2012), "13th annual online fraud report", available at: http://www.jpmorgan.com/cm/BlobServer/13th_Annual_2012_Online_Fraud_Report.pdf?blobkey=id&blobwhere=1320571432216&blobheader=application/pdf&blobheadername1=Cache-Control&blobheadervalue1=private&blobcol=urldata&blobtable=MungoBlobs(accessed 1 May 2013).

Durbin, N. R. (2007), "Building an Antifraud Framework", *Bank Accounting & Finance*, Vol. 20 Issue 1, pp. 43-46.

Ferrell, O.C., Gresham, L.G. and Fraedrich, J. (1989), "A synthesis of ethical decision models for marketing", *Journal of Macromarketing*, Vol. 9 No. 2, pp. 55-64.

Fullerton R, Punj G. (1998), "The unintended consequences of the culture of consumption: an historical– theoretical analysis of consumer misbehaviour", *Consumption Markets & Culture,* Vol. 1 No. 4, pp. 393-423.

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

Ghosh, M. (2010), "Mobile ID fraud: the downside of mobile growth", *Computer Fraud & Security,* Issue 12, pp. 8-13

Harris, L.C. (2008), "Fraudulent Return Proclivity: An empirical Analysis", *Journal of Retailing,* Vol. 84 No. 4, pp. 461-476.

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

Harris, L.C. and Daunt, K.L. (2011), "Deviant customer behaviour: A study of techniques of neutralisation", *Journal of Marketing Management*, Vol. 27 No. 7-8, pp.834-853.

Harris, L.C. and Reynolds, K.L (2004), "Jaycustomer behaviour: an exploration of types and motives in the hospitality industry", *Journal of Services Marketing,* Vol. 18 No. 5, pp. 339-357.

Hjort, K. And Lantz, B. (2012), "(R)e-tail borrowing of party dresses: an experimental study", *International Journal of Retail & Distribution Management*, Vol. 40 No. 12, pp. 997-1012.

Jamieson, R., Winchester, D. and Smith, S. (2007), "Development of a Conceptual Framework for Managing Identity Fraud", Proceedings of the 40th Hawaii International Conference on System Sciences, IEEE Computer Society, January 2007.

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

King, T. and Dennis, C. (2006), "Unethical Consumers: Deshopping behaviour using the theory of planned behaviour and accompanied de(shopping)", *International Journal of Qualitative Market Research,* Vol. 9 No. 3, pp. *282-296.*

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.

Kutz, G. D. (2006), "Framework for Fraud Prevention, Detection, and Prosecution", United states Government Accountability Office, July 12, 2006.

LexisNexis (2012), "True cost of fraud", available at: http://solutions.lexisnexis.com/forms/CE12Retail2012TRueCostofFr10206?source=RiskIDMInsights (Accessed 1 December 2012).

Malgwi, C.A. and Rakovski, C.C. (2009), "Combating academic fraud: Are students reticent about uncovering the covert?", *Journal of Academic Ethics*, Vol. 7, pp. 207-221

McGinley, R.P. and McCall, J. (2009), "The road ahead: new emphasis on prevention key to reducing fraud", *Managed Care Outlook,*Vol. 22 No. 2, Jan 15, 2009.

Moschis, G.P. and Cox, D. (1989), "Deviant consumer behaviour", *Advances in consumer research,* Vol. 16, pp. 732-737

Murphy, P.R. and Dacin, M.T. (2011), "Psychological pathways to fraud: Understanding and preventing fraud in organisations", *Journal of Business Ethics*, Vol. 101, pp. 601-618

Pergola, C.W. and Sprung, P.C. (2005), "Developing a genuine anti-fraud environment", *Risk Management*, Vol. 52 Issue 3, p.43, available at: http://38.98.118.173/Magazine/PrintTemplate.cfm?AID=2654 (accessed 8/6/2014).

Piron, F. and Young, M. (2000), "Retail borrowing: Insights and implications on returning used merchandise", *International Journal of retail & 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 (accessed 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 & Distribution Management*, Vol. 27 No. 8, pp. *290– 301*.

Solomon, M.R., Surprenant, C., Czepiel, J.A. and Gutman, E. (1985), "A role theory perspective on dyadic interactions: The service encounter", *Journal of Marketing*, Vol. 49 No. 1, pp. 99-111.

Speights, D. and Hilinski, M. (2005), "Return fraud and abuse: How to protect profits", *Retailing Issues Letter*, Vol. 17 No. 1, pp. 1-6.

Wells J. T. (2002), "Let them know someone's watching", *Journal of Accountancy*, May 2002.

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